BMC Client Management 12.6

Date: 2017-07-31 23:58
URL: https://docs.bmc.com/docs/x/P0n9Kw

Contents

This space contains information about the BMC Client Management 12.6 release.

BMC Client Management automates client management helping organizations control costs, maintain compliance, and reduce data and financial risks. From device acquisition to disposal, BMC Client Management provides an accurate view of software installations, ensures device adherence to organizational and industry policies, and supports systems and software currency.

You can browse through the topics, search for specific information, add comments, and view comments from other users. PDFs of the content can be found on the PDFs page. A BMC support ID is required for commenting and downloading PDFs.

What's new

> **Note**
>
> For information about enhancements available with BMC Client Management 12.6, see the 12.6 enhancements page.
>
> For information about release notes available with BMC Client Management 12.6, see the Release notes and notices page.

Where to start

For planning information and general information about the application, see the Planning topics and Getting started topics.

To learn more about using Client Management, see the topics listed below:

- New users with a Cloud installation: Installing OnDemand, Working with BMC Client Management console
- New users with an on site installation: Installing onsite, Working with BMC Client Management console
- Existing users: Upgrading

Other resources

BMC Communities

If you are interested in joining discussions with peers and experts on BMC Client Management, you might also like to visit the BMC Client Management User Community.

Proactive Notifications

If you would like to receive email notifications directing you to new Release Notes, Technical Bulletins and Flashes available online, along with links to additional information for the selected product, you can sign up for Proactive Notification Subscriptions. You need a BMC Support ID to participate.

Help for online technical documentation

For help on searching, adding comments, following topics, and exporting the Client Management documentation, see Help for BMC Client Management Online Documentation.

Help and Localized Help

English and localized PDFs are provided for on the PDFs page.

Release notes and notices

This section provides information about what is new or changed in this space, including urgent issues, documentation updates, service packs, and patches.

The following release notes include information about BMC Client Management 12.6. Several enhancements were added to BMC Client Management 12.6 and several defects were addressed.

Date	Title	Summary
27 July	12.6 release	The major improvements and new features in BMC Client Management 12.6 are the following: • Browser-based remote control of devices managed by BMC Client Management • Roll out agents through account credentials that are centrally managed by BMC Client Management • Automatically generate incidents in Remedy with Smart IT by defining events in BMC Client Management • Customizing company logo for end-user dialogs • Customizing company logo for style-based reports • Customizing the acknowledgment dialogs associated with Remote Control Access and Direct Access • Improved patch management in BMC Client Management • License applications that are purchased through the Apple Volume Purchase Program for BMC Client Management users • BMC Client Management integration with Remedy SSO allows technicians to sign on to BMC Client Management browser-based console with Remedy credentials • Updated Security Products Inventory types and Virtual Infrastructure Management • Ensure GUIDs generated for BMC Client Management devices are not duplicated • Visible column separators in BMC Client Management console

12.6 enhancements

This section contains information about enhancements in version 12.6 of the BMC Client Management product.

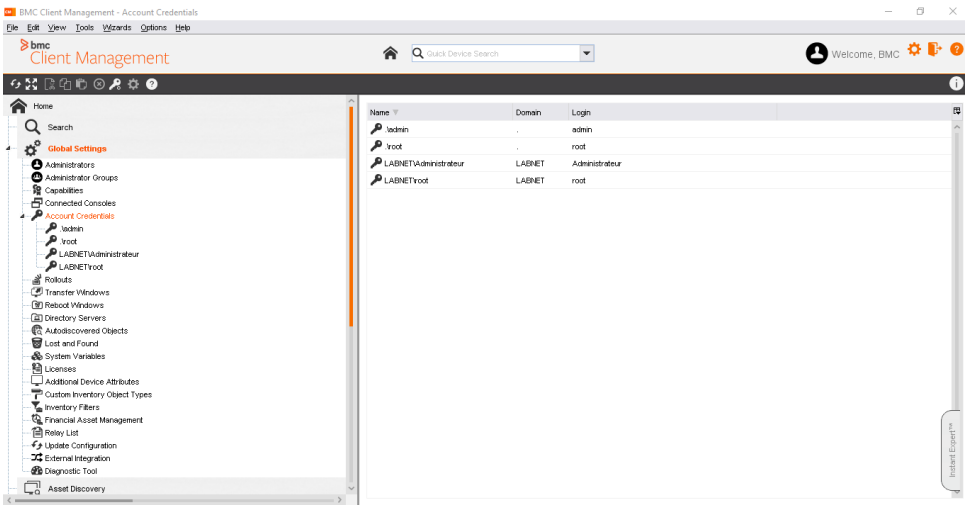
Centralized management of account credentials for rolling out BMC Client Management agents

Before BMC Client Management version 12.6, administrators had to authenticate their credentials on each asset while rolling out BMC Client Management agents. Any changes to administrator credentials did not automatically apply to the associated rollouts. It became time-consuming and repetitive to enter authentication credentials on each asset.

From BMC Client Management version 12.6 onwards, administrators can centrally manage account credentials and associate it to rollouts. BMC Client Management automatically applies any changes to an account credential to all the associated rollouts. This mechanism efficiently manages rollouts.

The BMC Client Management console provides a new node, **Account Credentials**, that enables administrators to centrally manage account credentials for all the roll outs.

The following screenshot shows the overview of account credentials in your IT infrastructure:



For more information, refer to Managing administrator credentials centrally for rolling out BMC Client Management agents.

Remotely controlling devices through a web browser

In addition to the classic remote control feature through the BMC Client Management console, 12.6 release enables remote control of devices through a web browser. It does not need you to install the BMC Client Management java console to remote control devices. You can remote control devices from anywhere through a web browser using a compatible browser on a compatible operating system. As a BMC Client Management administrator, you can configure the remote control settings that will be used by the help desk technician.

For more information, refer to Remotely controlling a device through a web browser.

Integrating Remedy with Smart IT product with BMC Client Management

Integrating Remedy with Smart IT with BMC Client Management enables administrators to automate incident generation in Remedy with Smart IT based on events defined in BMC Client Management.

For more information, refer to Remedy with Smart IT product integration with BMC Client Management.

Integrating BMC Remedy SSO with BMC Client Management

Integrating BMC Client Management with BMC Remedy SSO enables Remedy with Smart IT technicians to remote control BMC Client Management managed endpoints through the BMC Client Management browser-based console.

For more information on configuring Remedy SSO with BMC Client Management:

- Managing Remedy SSO parameters
- Integrating with BMC Remedy Single Sign-On

Customizing the end-user dialogs to provide a personalized experience

From BMC Client Management version 12.6 onwards, you can directly customize dialog boxes that provide product updates or acknowledgments to an end user directly through the BMC Client Management console. It enables you to deliver a personalized experience for end users.

You can customize the end-user dialogs for the following features:

- Remote Control Access and Direct Access
- Operational rules

- Patch management

For more information on customizing the dialogs that are sent to devices which are to be remotely controlled or directly controlled, or where operational rules, patches are to be installed, see

Customizing the end-user dialogs to provide a personalized experience

Customizing company logo for end-user dialogs

From BMC Client Management version 12.6 onwards, administrators can customize logo for end-user dialogs boxes:

1. On the BMC Client Management console, go to **Global Settings** > **System Variables** > **Customization**.
2. Click **Browse** to select a logo.
3. Select a logo in PNG or JPG format.
4. You can crop a part of the image or select a specific part of the image and click **OK**.
5. On the **Customization** tab, click **Apply**.

After you customize the logo, all dialog boxes will display the customized logo.

For more information, refer to Managing company logo.

Customizing company logo for style-based reports

Before BMC Client Management version 12.6, administrators could customize logos by storing logos on the master server and browsing them from the BMC Client Management console. But, an administrator could not add and customize new logos directly from the BMC Client Management console.

From BMC Client Management version 12.6 onwards, administrators can customize logo for style-based reports directly from the BMC Client Management console. This enhancement is not applicable for template-based reports.

> When an administrator generates a report, BMC Client Management generates the report with the default logo. The default logo can be replaced with a customized logo, which is displayed in future reports.

To customize logo on style-based reports:

1. On the BMC Client Management console, go to **Global Settings** > **System Variables** > **Reports**.
2. Click **Browse** to select a logo.
3. Select a logo in PNG or JPG format.
4. You can crop a part of the image or select a specific part of the image and click **OK**.

5. On the **Reports** tab, click **Apply**.

After you customize the logo, any newly generated style-based reports will display the customized logo.

For more information, refer to Managing report settings.

Ensuring GUIDs generated for BMC Client Management devices are not duplicated

For eliminating duplicate Global Unique Identifiers (GUIDs) associated to devices, BMC Client Management has enhanced its GUID generation mechanism. The new mechanism uses all the device attributes to generate a GUID, irrespective of whether an attribute is enabled or not in the BMC Client Management console.

BMC Client Management considers the attributes enabled in the console when an agent has to be re-installed on a device. BMC Client Management performs an attribute match to determine whether a device exists with at least one attribute match in the master database. If an attribute match is found, BMC Client Management persists the existing GUID for that device. This ensures that GUIDs are not duplicated in the master database and there are no communication issues between the master database and the agents.

Before BMC Client Management version 12.6, BMC Client Management used to generate unique IDs for devices by using the attribute value defined in the BMC Client Management console. The GUIDs were duplicated because was due to identical attributes on different systems. Thus it caused communication issues between the master database and the agents.

What's changed

From BMC Client Management 12.6 onwards, BMC Client Management uses all the attributes of a device to generate GUIDs, irrespective of whether an attribute is enabled or not.

For more information, refer to Managing BMC Client Management agent connection behavior.

Does an upgrade change existing GUIDs

Existing device GUIDs will not be changed after BMC Client Management is upgraded from version 11.7 or later to version 12.6.

How does BMC Client Management manage GUIDs when you deploy an OS (OSD) using the BMC Client Management console

When you deploy an OS image on systems using BMC Client Management, it ensures that each OS deployment is assigned a unique GUID. It ensures GUID uniqueness, by removing any existing GUID information from the `Identity.ini` file that is captured by the SYSPREP utility.

How to manage GUIDs when you deploy an OS using third-party tools

Before you use third-party tools to deploy OS images, ensure that the captured OS image that you will use to deploy the OS image on other systems is clean of any GUID information. To ensure that the captured OS image is clean of GUID information, remove any GUID information from the `ini` file.

If you do not remove the existing GUID from the `Identity.ini` file before you deploy the ghost OS image, then the same GUID will be deployed on all the other systems causing duplicate GUIDs recorded by the master database.

Improved patch management mechanism

From BMC Client Management version 12.6 onwards, the patch management mechanism is upgraded to provide a more efficient patch management experience. The update is seamless with a fresh product install or during an upgrade.

Microsoft Office patching

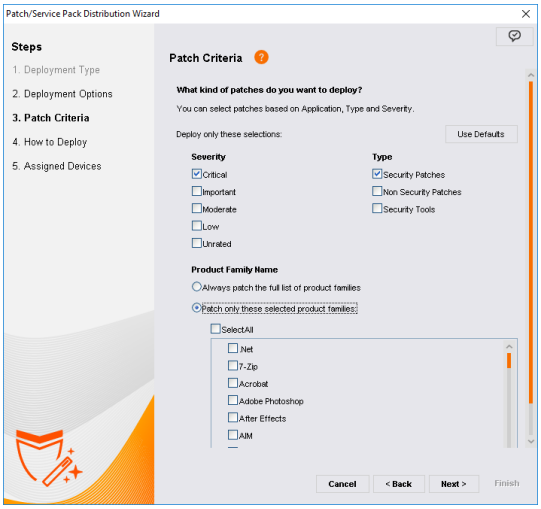
The upgrade patch management mechanism does not support patching individual Microsoft Office products. It only supports patching the entire Microsoft Office suite.

-
  - In the **Patch/Service Pack Distribution** Wizard, the **Office Options** step is not available in the wizard, which enabled selecting individual Office products. The upgraded patch management mechanism only patches the complete Microsoft Office suite. SDK 9.2 only deploys the patches that support full file. In BMC Client Management 12.5, the **Office Options** step was part of the wizard.
  - SDK 9.2 also supports Office 365 patching for devices with an internet connection.
  - Columns that list the patch versions are not shown in the wizard.

To view the updated console:

1. Go to **Patch Management**.

2. On the menu bar, click **Wizards** > **Patch/Service Pack Distribution Wizard**.



For more information on distributing patches/service packs, refer to Patch Service Pack Distribution Wizard.

Product family representation

In the **Patch Criteria** step, the **Product Name** list an updated list, where some product families list all individual products.

The updated product listing is beneficial because you can pick and choose the products you want to patch rather than patch the entire product family.

Product Family Names (BMC Client Management 12.5)	**Product Family Names (BMC Client Management 12.6)**
Adobe	Acrobat, Reader, AIR, After Effects, Bridge, Creative Cloud, Digital Editions, Distiller, Dreamweaver, Elements, Fireworks, Flash Builder, Flash Professional, Illustrator, InDesign, Shockwave, Adobe Photoshop
Wireshark Foundation	Wireshark
Windows Small Business	Windows Small
Windows Live Messenger	Windows Messenger
Windows Journal Viewer	Journal Viewer
Windows Defender	Defender

Product Family Names (BMC Client Management 12.5)	Product Family Names (BMC Client Management 12.6)
RealVNC Free Edition	VNC, VNC Connect
VMware	VMwareHorizon View Client, VMware Player, VMware Tools, VMware Workstation
Visual Basic for Applications	Visual Basic
Visual Studio	Visual FoxPro, Visual C++, Visual Basic, Visual Studio
Sun Java	Java, Java Virtual Machine
Step By Step Interactive Training	Microsoft Step By Step
Real Player	RealPlayer
Rarlab	WinRAR
PDF-XChange	PDF-XChange
Oracle OpenOffice.Org	OpenOffice
Opera Software ASA	Opera
Nullsoft	Winamp
Microsoft Windows Media Services	Windows Media Services
Microsoft Silverlight	Silverlight
Microsoft Office	Office
Microsoft Exchange	Exchange Server
MDAC Components	MDAC
IIS	Internet Information Server
Hewlett-Packard	HP System Management

Product Family Names (BMC Client Management 12.5)	Product Family Names (BMC Client Management 12.6)
Google	Google Desktop, Google Earth, Chrome, Picasa, Drive, Google Talk
FrontPage Server Extensions	Front Page
Foxit Corporation	Foxit PhantomPDF, Foxit Reader
Forefront Client Security	Forefront
EMC	Mozy
Citrix	Citrix GoToMeeting, Citrix Password Manager, Citrix Receiver, Citrix Single Sign-On, Delivery Controller, Group Policy Management, MetaFrame XP, Online Plugin, Presentation Server, Provisioning Services, Virtual Delivery Agent, XenApp, XenDesktop
Blackberry	BlackBerry Desktop Manager, BlackBerry Server
Autodesk	AutoCAD, DWG TrueView
Zimbra	Zimbra Desktop
AT&T	Global Network Client
Apple	QuickTime, iCloud, Safari, iTunes
Apache	Apache, Tomcat
AOL Inc	AIM

For more information on selecting specific products to patch, refer to Patch Criteria.

Updates to Security Products Inventory types and Virtual Infrastructure Management

After upgrading to or freshly installing BMC Client Management 12.6, the Security Products Inventory types and Virtual Infrastructure Management are updated in BMC Client Management.

For more information on updates to BMC Client Management, refer to Updates to Security Products Inventory and Virtual Infrastructure Management.

Managing application using Apple's Volume Purchase Program

License applications that are purchased through Apple's Volume Purchase Program for BMC Client Management users.

For more information, refer to Managing applications purchased through the Apple Volume Purchase Program.

Visible column separators in BMC Client Management console

In the BMC Client Management console, you can add color between columns to make the columns visible.

To add a color, go to the **Preferences** window, in the **Color of separators between columns** setting, choose a color and click **OK** to apply the settings.

Known and corrected issues

Use this section to learn about the issues that are corrected in the BMC Client Management 12.6. The following sections are provided:

- Known issues
- Corrected issues

Known issues

The following items are known issues or constraints with BMC Client Management version 12.6:

Issue Number	Issue Description
DRZKZ-1260	The Module Setup Operational Rule Steps that use non-standard default values might cause performance issues. **Workaround**: Use the standard operational rule steps when setting up modules.
DRZKZ-1257	From the BMC Client Management browser-based console, when a thumbnail is refreshed the current remote control session might temporarily hang.
DRZKZ-1279	SCAP package validation fails with Java Runtime Environment (JRE) 1.9 **Workaround**: Uninstall JRE 1.9 and to install Java JRE 1.8.131
DRZKZ-1283	After upgrading the BMC Client Management master server to version 12.6, any MDM server that is running a version earlier to 12.6 cannot be used to send commands to mobile devices. **Workaround**: Ensure that MDM managers are upgraded to BMC Client Management version 12.6.
DRZKZ-1026	The BMC Client Management Master agent service is not stopped properly.
DRZKZ-1097	After you deploy a BMC Client Management agent on a macOS or a Windows computer that has VMware Server running, the VMware shared virtual machines are not detected and displayed in BMC Client Management.

Corrected issues

The following items were addressed in BMC Client Management version 12.6 (build). Issues requiring more details include a hyperlink to the Knowledge Base article.

Issue Number	Issue Description
PM11115	The `Mtxagent` crashes on communication management process.
DRZKZ-511	Operational rules advertisement to macOS systems causes high CPU usage.
DRZKZ-572	Each time the BMC Client Management agent looks up the system for '**Darwin**' version, it causes memory leaks in macOS X computers.
PM11049	Free space in macOSx computers are not detected.
PM11083	The `mtxagent.log` files are written with `Devices XXX has not the last version of config file` messages.
PM10958	Laptops are incorrectly discovered and reported as workstations.
PM11061	The `HostAccessCheckAddress` action sometimes needs several seconds or minutes to be executed.
PM11102	In some cases, the client devices might no longer communicate after the GUID scheme has changed.
PM11130	The `AsynchronousActions` module performs unauthorized actions to the super master.
DRZKZ-581	It takes too much time to integrate actions in the `AsynchronousActions.sqlite` database.
PM11139	After BMC Client Management 12.5 hotfix 1, an error is generated while stopping the `Mtxagent.exe` on an Windows XP computer.
PM11097	Serial information cannot be stored if the information is greater than 64 characters.
PM10761	The agent does not always show up in the systray because the `mtxproxyservice` does not always initialize properly.
PM11012	The user synchronization process on the active directory generates duplicate users.
PM10774	As a user the `Execute program` does not work with UNC install path.
PM11066	Clients behind a NAT using GUID Scheme 004 (MAC Address) generate duplicate GUID values.
PM11074	The Windows Security logs are filling up with `event ID 4703-Authorization Policy Change` on Windows 10 client machines.
DRZKZ-576	The Windows SysTray icon does not appear or it takes an additional 18 seconds for the icon to appear.
PM11122	Office 365 is not detected by the `Software Catalog Inventory` module.
PM11100	Synchronizing a User Group from a Directory Server may randomly alter device records.
PM11113	SQL Execution Error when a device group is browsed from Software Inventory.
DRZKZ-579	Cannot import Windows 10 drivers in BMC Client Management.
PM11007	An `Access denied. Please verify your access rights.` message appears when the administrator does not have the View capability on administrators.
DRZKZ-562	Missing patch inventory is not appearing in the console after upgrading to BMC Client Management 12.5.
PM11143	Agent may download patch repeatedly.

Issue Number	Issue Description
DRZKZ-599	Some constraints are missing are missing after upgrading from 11.7 to 12.5.
DRZKZ-600	The connected user might not be detected if `mtxproxy` starts before Internet Explorer. As a result, the user cannot be auto connected to MyApps.
DRZKZ-558	On the Operating System Deployment (OSD) node, the `Synchronize` and `Stop Synchronization` links does not allow the selection of a child repository when the selection is invoked from the Primary OSD Manager.
DRZKZ-667	Operational Rules - Showing Deprecated machines.
DRZKZ-605	The Mtxagent.exe crashes on Master device when advance search is complete.
DRZKZ-831	Rule Dependency is not respected in case of rule assignment.
DRZKZ-903	Changed assignment dates are not replicated to the members of the device group that is assigned.
DRZKZ-940	Executing the `List of Windows Services` step causes heavy memory usage on some agents.
DRZKZ-969	The Remote Control driver is not loaded from time to time on Windows XP SP3.
DRZKZ-666	Integration with Remedy with Smart IT.
DRZKZ-638	The master crashes after the following log, `Moving legacy EventLogs files` from the Vision64 database.
PM10989	Asset Discovery may not collect connectivity from all SNMP devices.
PM10208	FileStore SQL error displays the following error, `cannot start a transaction within a transaction.`
DRZKZ-735	Asset Discovery may not collect connectivity inventories.
DRZKZ-724	SNMP discovers switches however these switches are not visible under Asset Discovery > Discovered Devices.
DRZKZ-740	The UpdateManager is not able to address file to some Mac devices.
DRZKZ-752	Sometimes it is not possible to add an OSD manager, error popup appears.
DRZKZ-566	The master agent crashes after a deadlock detected.
DRZKZ-722	Add web services to stop or reassign a discovery scan.
DRZKZ-723	Modify web services to get the number of devices belonging to a target list.
	Deactivated patch groups activate during automatic patch synchronization at 11:00 PM.

Issue Number	Issue Description
DRZKZ-725	
DRZKZ-742	Report not using the proper label.
DRZKZ-746	Published reports do not show embedded charts if the chart is on the first sub report.
DRZKZ-749	Asset discovery scans fail to connect to VMware hosts using SSH.
DRZKZ-756	When a device is offline a pop-up message during Remote Control or Audit Now operations does not appear with proper text.
DRZKZ-757	Patches status hangs in Patch Group.
DRZKZ-758	Asset Discovery is slow, hangs from time to name and upload IP addresses in place of Hostname in some cases.
DRZKZ-759	BMC Client Management 12.0 to 12.5 upgrade fails to delete attributes in `ObjectTypeAttrs` table.
DRZKZ-816	Inventories cannot be updated after BMC Client Management is upgraded to v12.5.
DRZKZ-830	Host is unreachable when the hostname is used instead of IP address.
DRZKZ-834	When one or more IPv6 addresses are scanned with Asset Discovery, the last IP is not scanned.
DRZKZ-837	You get an error while creating an OSD Project when OSD manager and Image Repository are on Domain controller.
DRZKZ-847	To have hardware inventories for VMWare ESX servers.
DRZKZ-858	Moving to the latest version of OpenSSL.
DRZKZ-883	NMAP scan hangs. It seems NMAP does not provide output.
DRZKZ-899	Problems with some patches showing 0 device count when there are devices requiring that patch.
DRZKZ-927	BMC Client Management 12.5 OsDeployment.ini does not reference `./data/OsDeployment/sql /dbupgrade_1210_1250.sql`
DRZKZ-928	Online mode USB do not rename hostname properly and offline mode fails to check local unattended file.
DRZKZ-1011	The patch KB is not completely processed since the update 2.0.2.2159 from Shavlik.
PM8372	The Synchronize all Devices option does not work as expected.

Issue Number	Issue Description
PM4158	The advanced search based on a date that is filtered by `greater than` or `lower than`' parameters does not return good results.
PM4199	When viewing the last report results, the timestamp shown in the dialog box is incorrect.
PM8159	Assigning a free query to a device group may generate SQL errors if the populator is not an administrator.
PM10374	SMB credentials are not updated when a new password is entered.
PM10737	The agent web interface displays an untrusted certificate warning in Firefox after a certificate is imported.
PM10389	The new `ini` configuration file that function as a restorator does not restore more than one file.
PM8303	After the release of Footprints Asset Core 11.5, from the Operational Rule Assignment window, double-clicking on a bar chart does not show the list of devices with that status anymore.
PM7298	The Number of Critical Missing Patches field in the Patch Detection node does not account for hidden patches.
PM9605	The Packagebuilder.bat file is not generated if the `Standard.xml` file contains unaccepted characters.
PM11052	The master list cannot be parsed if a download link contains an "&" in it.
PM8252	Trying to insert a patch in PatchJobHistory using an invalid PatchJobId results in Error `ORA-02291`.
PM11089	Operating System Deployment (OSD): Windows edition value is not set up to deploy the Windows 10 image.
PM10809	Operating System Deployment (OSD): Windows edition value is lost after editing an OSD Image.
PM11079	Dynamic device groups are not populated when there is a ; character at the end of the free query that populates that group.
PM11079	If a query that populates dynamic device groups has a special character ; at the end of the free query, these dynamic device groups are not populated in the BMC Client Management console.
PM10960	The Set Agent Parameter step does not modify the AvertisePopup parameter.
PM11025	The Operating System Deployment (OSD) Project build did not pick up a DISM error.
PM5043	The Sysprep utility that is executed through AMP does not display expected behavior, as described by Microsoft. The rear limit is reached sooner than expected.
PM7034	Changes done to the Administrator Login field in the unattended information section for an Operating System Deployment (OSD) target are not taken into consideration when deployment.
PM5230	When rolling out a relay, the MaxThreads value must be set to 200.
PM7636	The syntax, `${}`, returns an environment variable only on a Windows system.
PM3433	The `Collect Ini` file value step does not get data in an expected format.
PM4067	Applications with blank version information cannot be added to software license titles.
PM10938	Comments added to rules are not displayed in MyApps tooltips anymore in BMC Client Management 12.1.
PM10982	Changing the status for Licensed Software for a device changes status for all devices.
PM10952	For Direct Access, the value of `Path` set in the registry is empty.
PM10937	When running a query for the Internet Browser Version in Security Product Management, entering values of 10, 11 or 12 get converted into a month.

Issue Number	Issue Description
PM10977	Incorrect information in tooltip: `When do you want this rule to be run on` device?
PM6946	CSV import fails if any string values contain a comma.
PM3362	Request for copy and paste operations to be logged in the `mtxagent_audit.log`.
PM10835	Cannot see the Field Mapping section when importing Software License Management data.
PM7639	From the Advanced Search node, changing object type dims the search button even though the search value is valid.
PM7683	The Advanced Registry Management step does not create multiline registry values.
PM10261	Collecting data through the Registry Value step does not manage Default data.
PM8932	Linux devices generate hardware inventory data containing line breaks.
PM11060	During report generation, when `TO_CHAR` is used in `GROUP BY` field on an Oracle 12 database, the database generates the `ORA-00979` error.
DRZKZ-618	Provide WMI ability to query remote Windows from Linux computer.
DRZKZ-617	Some LDAP Organizational Units are not browsing from BMC Client Management master server.
DRZKZ-450	In some cases, the Asset Discovery module can replace valid data with null (blank) data.
DRZKZ-660	A Java exception occurs when an administrator with limited rights tries to display 'Assigned objects' node when assigning a rule to a device.
DRZKZ-661	Console bookmarks for device groups cannot be deleted.
DRZKZ-644	All registry value name is not getting captured from the registry if you use the Extracts Operational Rule on Windows registry.
DRZKZ-680	Operational rules which are assigned to parent device groups are not always assigned to devices that become members of a sub-group of this parent device group.
DRZKZ-726	Nothing happens when trying to save viewing PDF format.
DRZKZ-736	When you must work in the 'Run as Administrator' mode, the Execute program fails on Windows 10.
DRZKZ-743	Our agent is vulnerable to click-jacking which is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information.
DRZKZ-1000	XML Parsing Error in Reports when software name contains an ampersand, `&`, character.
DRZKZ-995	When you rename an Operational Rule by changing the case, the following popup ‘`the object already exists` is displayed.
DRZKZ-1132	Complete package import and export, not just the XML files.

Issue Number	Issue Description
DRZKZ-1079	Ability to perform a real-time file analysis using the regular expression step.
DRZKZ-1176	Deleting a patch from the download in progress queue deletes all the published packages from the master installation folder.
DRZKZ-1171	File Analysis through RegEx does not store data in `CustomInventory`.xml if the `Maximum number of entries to preserve` parameter is set to 0.
DRZKZ-1133	Ability to select Package folder in Package Factory when using wizard.
DRZKZ-974	Unable to clear the User Login field for Execute Program as User.
DRZKZ-495	Devices with duplicate GUID values in their `Identity.ini` files are not handled properly.
DRZKZ-598	When you rename a Driver by Model directory in the console, the Drivers streams are deleted.
DRZKZ-647	A BMC Client Management SaaS Web administrator is unable to properly parse a Remedyforce Client Management Premium license file.
DRZKZ-929	A Network Boot listener may return the following error: “EnsureTunnel: failed to open a tunnel for reference device for family 'OSD_...".
DRZKZ-578	A method is needed to deliver SSL certificate needed by Remedyforce Client Management Premium or Premium Plus for importing into Trusted 3rd Party CA stores.
DRZKZ-571	If you manually create a device, you can set different static admin rights for that device from the rights set for the device group.
DRZKZ-587	When you create a Patch Group by setting the "No Reboot" option and assign devices to this patch group. After patch installation, a reboot is required for installation to be complete, but BMC Client Management displays "`Installation In Progress until manually rebooted`" message.
DRZKZ-561	OS Deployment: The Drivers by Model panel in the console might not populate with driver details.
DRZKZ-828	Remedyforce Client Management SaaS master servers are not properly patched when the cumulative update is applied using the SaaS Admin Web Console.
DRZKZ-1169	When the BMC Client Management console is running an `V64DbAdminCheckLoginrequest` a request is sent every 5 minutes to the log files.
DRZKZ-1239	The BMC Client Management agent stopped working on New Linux Kernel Build `3.10.0-514.21.2.el7.x86_64`.
DRZKZ-574	Outbound email configured on Port 25 on a hosted box is blocked for Remedyforce Client Management Premium users.
DRZKZ-1247	The assigned value for Remote control acknowledgement changes from “`Required`” to "`Inherit`" and the assigned value for Direct Access Acknowledgement changes from “`Not required`” to “`Inherit`”.
DRZKZ-1235	When you install patch `INTEL-SA-00075` it installs an `Intel SCS` utility which is incorrectly extracted to the `C:\Program` directory. Windows does not allow the patch to be installed in this directory and displays a pop-up message to rename the folder where the patch must be extracted.

Issue Number	Issue Description
DRZKZ-1233	The Execute Program As User step fails to install applications as an administrator when the device runs on Windows 8.1 (x64).
DRZKZ-1234	The Execute Program As User step fails to install applications on Windows 8.1.
DRZKZ-924	An operational rule that executes the Execute Program step does not install Zenworksplugin.
DRZKZ-827	The `Run Program As User` step fails if the program needs to be executed as an administrator.
DRZKZ-871	In some cases, Hardware Inventory may not be populated where an inventory attribute exceeds 256 characters.
DRZKZ-748	Cannot upgrade BMC Client Management if SQL server 2012 is installed with SP2 or SP3.

Getting started

This section provides a high-level overview of the BMC Client Management product.

The following table provides links to relevant topics based on your goal:

Goal	Instructions
If you are a CIO or an Architect of an organization:	
Understand the benefits and business value of BMC Client Management	• About BMC Client Management
Review product features	• Orientation
Review product architecture and components	• Architecture
Understand product capabilities	• Product capabilities • Inventory management • Patch management • Compliance management • Deployments • Remote management
If you are a System Administrator:	
Install BMC Client Management on premises	• Installing onsite
Install BMC Client Management in a cloud environment	

Goal	Instructions
	• Installing OnDemand
Upgrade the product to a new version	• Upgrading

About BMC Client Management

BMC Client Management is an advanced systems management software that provides a reliable way to monitor all systems on a network. It isolates the exact point of failure when problems occur and makes it possible for network and system difficulties to be resolved quickly. BMC Client Management is a client-server system made up of several different computer programs. It contains a database which is integrated with the master server, a graphical user interface to access the data in the database, and the agents installed on the clients providing the data for the database.

BMC Client Management automates client management helping organizations control costs, maintain compliance, and reduce data and financial risks. From device acquisition to disposal, BMC Client Management provides an accurate view of software installations, ensures device adherence to organizational and industry policies, and supports systems and software currency.

BMC Client Management allows you to streamline and automate client management with a comprehensive set of capabilities that enable you to discover, configure, manage, and secure all of your IT end points:

- Pass software audits with ease
- Reduce data vulnerabilities and financial risk through automated software patching
- Know what you have - confidently discover all your clients and edge devices
- Intelligently manage your software entitlements - don't over deploy and don't over spend
- Enjoy turnkey integration with multiple BMC service desk solutions

BMC Client Management allows you to manage IT clients from receipt to retirement. You can easily automate processes and effectively manage the full range of IT assets while also delivering-and communicating-overall business value. BMC Client Management is composed of five modules, which can be purchased individually or as the complete suite, either on site or in the cloud:

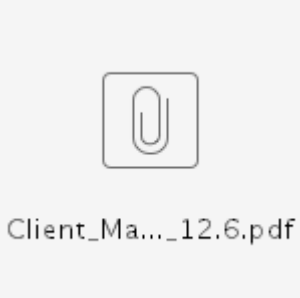
- Inventory : Automate inventory tracking to help guide investment decisions, reduce manual processes, and maintain compliance. Reduce costly audit failures by understanding software license usage and the associated financial liabilities.
- Patch : Centrally assess, manage, deploy, and report on patches to ensure that systems are secure and that the integrity of your business is never compromised
- Deploy : Easily deploy, migrate, and patch software to ensure that all systems are secure and up-to-date.

- Compliance : Reduce the hassle associated with monitoring IT assets and defining policies, and provide auditors with records of compliance levels from a centralized console. Reduce PC energy consumption and track ROI and TCO. Define and enforce usage policies, including what content is available for upload and download, and keep track of events and activity across all assets.
- Remote : Identify and resolve PC issues without leaving your desk.

The key benefits of BMC Client Management are:

- Centrally manage client assets
- Reduce discovery, configuration and deployment of client devices
- Intelligently optimize software license management
- Reduce risk of audit failure
- Make informed, financially sound decisions
- Reduce exposure and financial risk by automatically resolving known vulnerabilities
- Deliver actionable data through reporting and dashboards
- Provide self-service for software downloads, common actions and quick links with MyApps
- Easily establish return on investment (ROI) and total cost of ownership (TCO) with granular power management settings

See the Client Management datasheet.



Orientation

BMC Client Management automates client management helping organizations control costs, maintain compliance, and reduce data and financial risks. From device acquisition to disposal, BMC Client Management provides an accurate view of software installations , ensures device adherence to organizational and industry policies, and supports systems and software currency.

BMC Client Management is composed of five modules, which can be used individually or as the complete suite, also the product can be installed either on site or in the cloud.

Quick overview

As businesses continue to grow and merge, IT organizations continually find themselves facing the increasingly difficult task of a accurately managing their technology assets, including client devices.

- Inventory your IT assets - know what you own and exactly how those assets are being used
- Ensure that your devices are secure and compliant with your IT policies
- Easily deploy, update, and patch operating systems and applications
- Remotely access all of your devices (even those not connected via VPN)
- Provide one-click desktop access to role-specific, preapproved software and other relevant data
- Integrate client data with your BMC IT Service Desk

Product features

BMC Client Management is a client/server system made up of several different computer programs. It contains a database that is integrated with the master server, a graphical user interface to access the data in the database and agents installed on the clients, providing the data for the database. The product provides the following features:

- Discovery and inventory: Automate inventory tracking to help guide investment decisions, reduce manual processes, and maintain compliance for physical and virtual devices
- OS and application deployment: Centralize and automate system deployment or migration - with no configuration - for minimal disruption
- Software license management: Reduce costly audit failures by understanding software license usage and the associated financial liabilities
- Patch management: Centrally assess, manage, deploy, and report on patches to ensure that systems are secure and that the integrity of your business is never compromised
- Event management: Extend monitoring and custom alerting capabilities to proactively track, manage, and automate remediation when key infrastructure events occur
- Financial asset management: Make informed decisions to optimize spending and eliminate compliance penalties
- Policy compliance: Reduce the hassle associated with monitoring IT assets and defining policies, and provide auditors with records of compliance levels from a centralized console; leverage SCAP templates certified by National Institute of Standards and Technology (NIST)
- Device security: View, control, monitor, and update all major anti-virus and anti-spyware software from a single source
- Remote management: Securely manage routine desktop management tasks and enable administrators to detect, diagnose, and resolve PC issues without leaving their desk
- Power management: Lower energy bills and reduce the environmental footprint associated with PC energy consumption
- Device management: Centrally define and enforce your device usage policies, control upload and download activity, log peripheral device events for proactive response, and audit any unwanted activity
- MyApps: Put preapproved software and access requests in the hands of the end user without going to any websites or submitting Help desk forms

Product Documentation

Ready-made documentation is available for download on the PDFs and videos page.

Architecture

BMC Client Management is a client/server system made up of several different computer programs. It contains a database with is integrated with the master server, a graphical user interface to access the data in the database and the agents installed on the clients providing the data for the database.

A highly scalable and flexible architecture ensures effective client systems management no matter how complex the enterprise infrastructure. BMC Client Management can scale from 150 to more than 200,000 heterogeneous client systems on geographically distributed locations. It provides a reliable way to monitor the status of all systems on a network and isolates the exact point of failure when problems occur to make it easy for network or systems difficulties to be resolved quickly.

The following topics are provided:

- Types of architecture
- BMC Client Management components

Types of architecture

The BMC Client Management is available with the following different types of architecture:

- On-site architecture
- Cloud architecture
- Supermaster architecture

BMC Client Management components

The architecture of the BMC Client Management software is made up of the following components:

- Master Server
- Relay
- Console
- Client

Master Server

The master server or administration server is the main server in the network topology which contains the database. It is responsible for answering requests from the console and executing the appropriate database communication. It receives and stores all information and data sent by the client agents and sends requests for additional information when necessary through the first-level relays. The master server database is an object model database system in which each network or

system component is modelled by corresponding model objects. It operates in real time and reacts to changes in the real network and systems components by updating and changing the corresponding objects in the database. The BMC Client Management console connects to the master to display the collected data on the screen.

Relay

A relay or intermediate server is used to balance the network and resource load. Relays are present at multiple levels depending on the network topology to forward the down-going data /actions to their own lower level. They also collect up-going data/actions which they forward to their upper level based on a predefined schedule allocation. Each relay records a list of transactions and is configured for a number of retries before abandoning and informing the next higher level on error. Relays are basically clients with the extra feature of forwarding data in both upstream and downstream directions for software distribution and other operations to execute.

Console

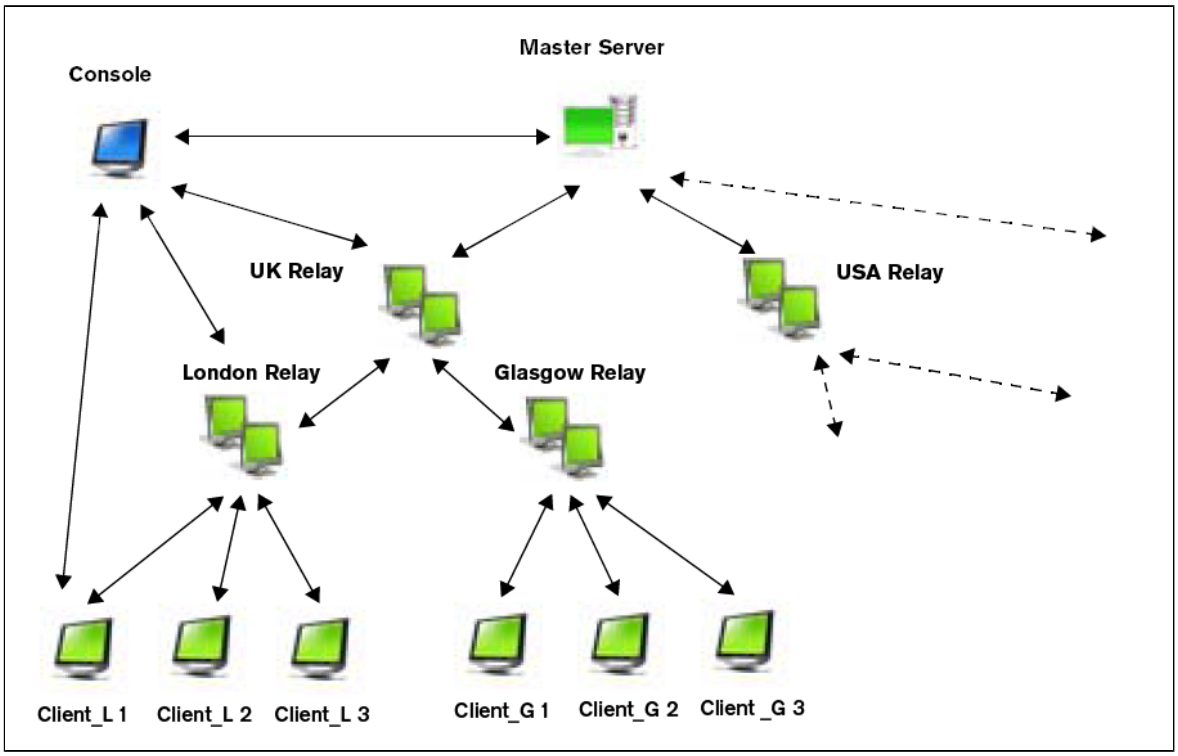
The BMC Client Management console is the graphical user interface to the management system and its database. It is a Java application through which you may visualise all data collected in the database and execute any type of action on the objects in the database, such as create and delete objects, modify specific data of an object, execute reports and operational rules or remotely access a client to make modifications on the remote client's registry.

Client

The BMC Client Management client agent is installed on each client and operates completely independent of the master server, sending information either at regularly defined intervals or when polled by the master or any other module through its respective relay, such as reporting their connection status. Agents receive data/actions from and forward data to their upper level based on a pre-defined schedule allocation. They provide monitoring of and reporting on a very large number of parameters. The nature of these parameters depends on the operating system of the client on which the agent is installed, that is, if it is a Windows client, a Linux client or a Mac client.

On-site architecture

Our dependence on computers within the workplace is clear. Present on every desktop and commonplace for all business travellers, we have come to depend on easy and reliable workstation access to deliver the applications, tools, and communication mechanisms that improve our performance. In recent years most organisations have invested heavily on enterprise software systems and the number of workstations (both fixed and laptop) can be counted in the thousands and tens of thousands. While these workstations have driven higher performance and productivity, the number of systems, their complexity and diversity, their geographic distribution, and the need for regular upgrades and maintenance, have outpaced the capacity of most IT support departments.



Preparing your architecture

Before you can launch the installation and rollout process you should create an architectural schema of your network, that is, define amongst others the points listed following. After you have followed the example installations and operations in this booklet you will certainly find more questions to be answered before you can make the complete installation of your network.

The architecture will obviously look very differently depending on the size of your company, that is, is it a small company, with everybody, that is the whole system, being located in the same building, is it a company operating on several sites within one country or even one continent, or is it a company with sites and locations all around the world:

- Define, if your database will be on the master server. If you have a large network we recommend you use different machines.
- Define the basic architecture of you network. There are three different types:
  - A smaller number of relays which are each managing a large number of clients. This scenario asks for quite powerful relays to guarantee a performant operation.
  - A larger number of relays managing a smaller number of clients each. In this case the master server needs to be very powerful and your network must have a good and fast performance.
  - Super master architecture
- Define the relays on your remote sites, we recommend you use one relay per site, a site being in this case a physically independent entity like a building,

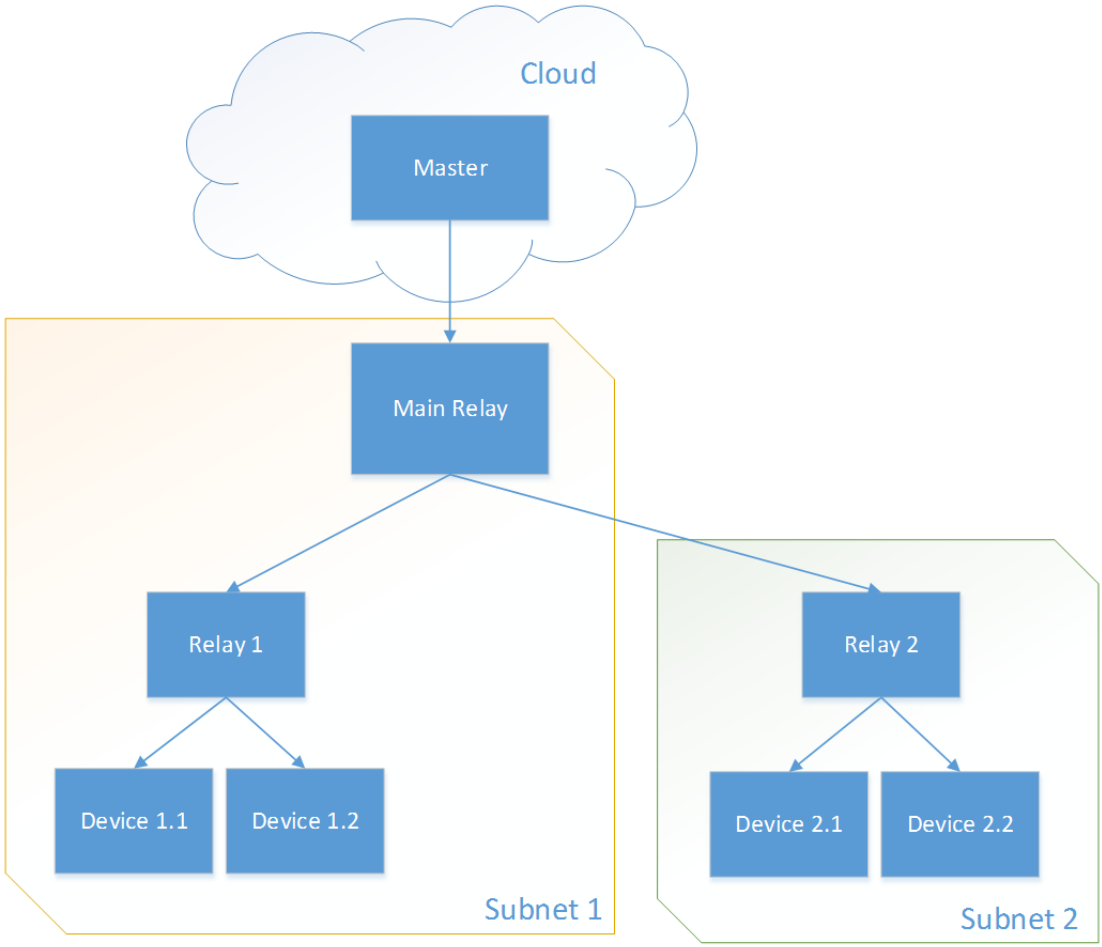
- Define the maximum number of clients per relay: this number may vary depending if the relay is a dedicated relay, meaning it will only be used as a relay and does not serve for any other tasks, or if it is not dedicated, i.e. a normal client in your network. For a dedicated relay we would recommend a maximum number of 2000 clients and for a normal one, not more than 500. Also, for a site relay we would always recommend to use a dedicated relay.
- Plan for growth for at least one year ahead, preferably for two years. This will avoid costly reconfiguration later on.

The points listed here are not an exhaustive list of all the questions appearing when you create your BMC Client Management architecture, they are supposed to give you an entry point in the complexity of this task, as well as the recommendations made. They are only intended as guidelines. If you have any question or are in doubt please contact the BMC Software support.

Cloud architecture

Standard architecture is a master with several relays and then more relays or clients directly below. Numbers depend on the size of the infrastructure and the performance. In a SaaS environment this type of architecture might lead to issues, as Client Management has several bandwidth consuming functionalities, such as patching or deploying of operating systems and applications. BMC,

therefore recommends to have only one *first-level* or *master relay* in your network directly below the master, which is located in the cloud. This master relay then takes over all the roles the master is assigned by default and thus limit network traffic between the customer network and the cloud.



Supermaster architecture

A super master in BMC Client Management is limited in its functionality and the objects it provides in the console via its database, as it only consolidates and reports on the data provided by the site masters, which will execute all network management tasks in their part of the organization's infrastructure. The super master stores the inventory data uploaded by the "normal" master servers at the different locations of the organization, and then may generate reports on these.

Depending on the configuration of the site masters, part or all of the following types of inventory data may consolidated in the super master's database, the data will be uploaded by the site masters right after it was integrated in the local database:

- Device information (name, IP address, domain name, etc.) from the list of autodiscovered devices
- All available types of inventory

The super master itself is completely autonomous. It may create its own configurations for a number of specific objects, such as:

- Objects that are required for reporting: queries, device groups, patch groups, and reports
- Device settings such as when a client is lost

Product capabilities

Our dependence on computers within the workplace is clear. Present on every desktop and commonplace for all business travellers, we have come to depend on easy and reliable workstation access to deliver the applications, tools, and communication mechanisms that improve our performance. In recent years most organisations have invested heavily on enterprise software systems and the number of workstations (both fixed and laptop) can be counted in the thousands and tens of thousands. While these workstations have driven higher performance and productivity, the number of systems, their complexity and diversity, their geographic distribution, and the need for regular upgrades and maintenance, have outpaced the capacity of most IT support departments.

With BMC Client Management , IT managers are able to automate client management functions thereby driving IT efficiency, reducing operating costs, and ensuring end-user productivity. It provides a completely integrated solution permitting IT departments to understand, plan, automate, control and secure their client systems. By offering a solution that automates CSM, yet is easy to use, administer and deploy, BMC Client Management provides a crucial means for driving IT efficiency, reducing management costs, and ensuring end-user productivity.

This section provides a high-level overview of the BMC Client Management product capabilities:

- Inventory management
- Patch management
- Compliance management
- Deployments
- Remote management
- Mobile device management

Inventory management

Tracking inventory is more than just gathering a list of all computers, software applications, servers, and operating system settings. To make more effective business decisions, companies need a way to easily identify and understand their entire IT asset portfolio. The alternative - manually tracking assets - often results in wasted time, redundant purchases, increased support costs, and compliance risks.

BMC Client Management Inventory is part of a fully integrated line of IT service and asset management solutions. Each product automates and streamlines a specific IT challenge to help you reduce costs and improve service levels. Built from the ground up as a modular, yet integrated system, this family of technologies provides a single, unified solution to simplify a diverse set of complex client lifecycle and service management needs.

The main features of inventory management are:

- Inventory - Maintain control with a comprehensive inventory of hardware assets across the entire organization; auto-deploy and update BMC FootPrints agent; Manage changes to hardware or software configurations, enforce change control policies, and maintain detailed inventory history
- Software license management - Show proof of entitlements and know what software licenses are being used
- Financial asset management - Achieve complete cradle-to-grave asset management workflow by receiving assets, tracking financial data, retiring assets, and reporting on depreciation
- Virtual infrastructure management - Discover virtual hosts and guests, and change the stop /pause/start state to perform maintenance or troubleshoot issues
- Security inventory - Collect specific data on key security settings with ease, including installed / update status for anti-virus and anti-spyware, as well as firewall configuration or shared resources
- Self-healing - Maintain the integrity of an application with routine checks that automatically correct an application even after events that compromise the core files
- Agent/agentless discovery - Support both agent and agentless discovery of assets and provide detailed configuration information
- Data import - Perform customized data imports, such as assets and user fields from external sources
- Next-generation and multi-OS support - Support discovery of network devices for Windows, MacOS, Linux®, VMware workstations, servers, laptops, and network devices; core agent support for Redhat 6, MacOS X Lion, and Windows 2008 R2, Windows 7 and 8, and Microsoft SQLServer2012 and 2014
- Windows-embedded client support - Discover, deploy, troubleshoot, assess, and update Windows-embedded devices through a single management console
- Audit now - Update the summary asset data in near real-time (summary asset data provides quick navigation to hardware, software, and security information)
- MyApps - Puts pre-approved software and access requests in the hands of the end user. It's the app store for the desktop - IT can advertise available software applications, advanced actions and quick links for the end-users to access on their schedule, not IT's.

Patch management

Security threats to your applications and operating systems have never been more pervasive. Ensuring your organization's computers are properly patched with the latest releases from an ever-growing list of vendors is time-consuming and difficult. Mistakes and delays in the patch process can be extremely costly to the business.

BMC Client Management Patch powered by Shavlik®, automatically scans your environment and identifies which devices are missing which patches. It also provides administrators with options for quick deployment of critical fixes to ensure compliance and reduce the risk of a security breach or incident, including the option to set once and automate the ongoing patching for operating systems and applications across the environment. Administrators can easily track the progress of patch updates in real time and can utilize built-in wizards to quickly define pre- and post-installation parameters to control how deployment occurs. BMC FootPrints Patch Manager tracks and provides patch management options for Microsoft operating systems, Exchange, SQL, and Citrix, as well as a wide range of other third-party applications.

The main features of patch management are:

- Service Anywhere - Secure and patch local devices or machines across the internet without the need for a VPN
- Automatic bulletin updates - Configure downloads and updates to the vulnerability and patch bulletins catalog
- Set-it-and-forget-it patching - Determine your deployment options, patch criteria, and how you want to deploy patch updates over time - automatically or upon review and approval - with the built-in wizard
- Missing patches view - View a list of missing patches per device with their severity level
- Wake-on-LAN - Distribute patches and other related maintenance tasks automatically, outside of business hours, by waking PCs, deploying patches, and shutting down machines once updates are complete
- Support for Microsoft and non-Microsoft solutions - Deploy patches for such products as Citrix, Exchange, SQL, Mozilla Firefox, Adobe, Apple iTunes, WinZip, and more including MacOS devices
- Dynamic groups - Easily target groups of devices for updates based on patching requirements and computer attributes
- Status tracker - Monitor the patching process in real-time and receive detailed information regarding any errors or anomalies so you can take immediate corrective measures

Compliance management

Enforcing compliance policies and assessing assets is difficult and time-consuming. To complicate matters, compliance standards are often interpreted differently from one auditor to another. As a result, compliance can quickly become a moving target. Reduce your compliance risk with the most comprehensive asset inventory and PC lifecycle management solution on the market today - and automate policy compliance across Windows, Mac, and Linux® environments.

With BMC Client Management Compliance, along with BMC Client Management Inventory, and Patch, you can quickly evaluate and remediate corporate, regulatory, and industry compliance requirements with a single database and console.

The main features of compliance management are:

- Intelligent software recognition - Assess licensable software units, choose what you want to manage, add licenses, and track usage with software inventory normalization for consistency
- Automated patching - Keep desktop and server software current with fully-automated, wizard configurable, set-it-and-forget-it patch management
- Security software "manager of managers" - View, control, monitor, and update all major anti-virus and anti-spyware software from a single source; apply definition updates and security settings; deploy out-of-the-box compliance templates and customizable alerts
- Compliance management - Define policies based on your vendors' licensing agreements and other regulatory standards with essential tools, reports, and templates for PCI, ISO 27001, ISO 27002, NIST, and Microsoft hardening guides
- Compliance check - Visually identify your compliance status with new dashboards and drill-down functionality
- Software metering -Track the actual usage of any given application and redeploy unused software licenses to other users
- Dynamic groups - Identify, group, and remediate those devices that do not adhere to defined compliance policies
- Agent/agentless - Support both agent and agentless discovery of assets with detailed configuration information
- Multi-OS support - Support the discovery of software licenses on network devices for Windows, MacOS, Linux, and VMware, including workstations, servers, laptops, mobile machines, and network devices, such as printers

Deployments

Constantly evolving technology introduces multiple updates for multiple applications deployed to any given number of machines in your IT environment. Keeping systems configured with the latest upgrades becomes a time-consuming and often expensive process. Most IT organizations are constantly searching for the most effective way to automate this task across their Windows, Mac, and Linux® environments.

BMC Client Management - Deploy gives you the reliable and comprehensive control you need to ensure successful software deployments in heterogeneous environments, as well as OS deployments for Windows environments, from a single, centralized console - without disruption to your end users.

The main features of deployments are:

- Multi-casting and bandwidth management - Conserve network bandwidth by simultaneously sending data to multiple clients while minimizing interference
- BMC Client Management agent deployment and updates - Auto-deploy and update the BMC Client Management agent to newly discovered machines
- MyApps - Deploy pre-approved software directly from the desktop without submitting a request or waiting for a technician to install the software - self-service for the end-user and reduced impact to IT resources
- Checkpoint restart - Ensure that portable devices, such as laptops, receive a complete installation regardless of the size of deployment or number of network disconnections
- Wake-on-LAN - Successfully update workstations regardless of power state
- Easy packaging - Deploy software and configuration changes for Microsoft, MacOS, UNIX®, and Linux systems, as well as custom applications
- Remote install - Remotely install Windows OS, including formatting/partitioning hard drives
- Customized planning - Streamline software distribution planning efforts by grouping software with similar characteristics
- Hardware compatibility - Maintain a comprehensive list of hardware assets to ensure that the software being rolled out is supported
- Application kiosk - Access a web-based catalog of approved software for self-service installs following migration
- Report now - Provide reports on application update details
- Service anywhere - Access a machine without the use of a VPN to perform desktop management tasks, such as inventory, patch management, and software deployment

Remote management

Respond as quickly and effectively in the virtual workplace as you do in corporate headquarters. Meet different customers' needs, while providing a differentiated quality of service and reducing capital and operational costs.

BMC Client Management remote management provides IT managers with the means to manage assets and provide consistent desktop support. IT managers can respond as quickly and effectively in the virtual workplace as they do in the corporate headquarters. As a result, they can meet different customers' needs, while providing a differentiated quality of service and reducing capital and operating costs.

The main features of remote management are:

- Remote support - Remotely view and control users' PCs and quickly resolve desktop issues from afar
- Service Anywhere - Extend the reach of IT to include not only telecommuters and remote office locations, but also travelling workers and contractors who are not logged on to the network via VPN and are traversing firewalls
- Team Viewing - Multiple agents can remote into and view the same desktop or server simultaneously to review and determine cause of issues and appropriate solutions
- Intel vPro integration - Enable administrators to access computers even if the PC is off or the operating system is down
- Security options - Ensure privacy during all remote sessions with encrypted communications, authenticated sessions, and user confirmations prior to network connection
- Power user mode - Perform command-line executions, file transfers, clipboard management, and target device restart
- Audit trail - Maintain central audit file of remote control sessions and end-user acknowledgements
- Direct device access - Consolidate many common device actions, such as wake-up, check connectivity, reboot, shutdown, configuration summary, transfer file, remote control, file system, registry, services, process management, and Windows events, and allow administrators to perform any of these options for after-hours adjustments or troubleshooting
- Operating Systems support - Remote into a MacOS or a Windows device

Mobile device management

Mobile phones and tablets are widely used by enterprises to help their employees stay connected to business data round-the-clock. Business data includes corporate emails, meetings, corporate contacts, as well as other documents and files stored in the local or removable storage of a mobile device. Like all other devices in the IT infrastructure, it is necessary to manage configurations, applications, and security for mobile devices. BMC Client Management supports mobile device management for iOS mobile devices.

> **Note**
>
> In BMC Client Management, any mobile device (with or without calling feature) is referred as a *mobile device*.

After one-time enrollment, the IT administrators can manage the mobile devices from the BMC Client Management console.

Mobile device management key features

The following are the key features of mobile device management:

- Collect inventories, run queries, and generate reports to meet organizational and statutory compliance requirements
- Keep track of the licensed software usage and the financial information of a mobile device during its lifecycle
- Control the configurations of the managed mobile
  For example, you can create configuration profiles that can be set to all managed mobile devices in your organization. You could restrict mobile camera usage; or you could allow camera usage, but prevent it from recording videos.
- Create a list of applications and install them on mobile devices
  Using mobile commands, you can install applications on the managed mobile devices. Even if the user manually removes the application, setting the `Repeat Frequency` option to run the command daily ensures the application will be installed automatically the next day.
- Control mobile device security using direct commands - Lock Mobile Device, Wipe Mobile Device, and Clear Passcode
  If the device is stolen, you can wipe it remotely (reset to factory settings). If the device is misplaced, you can lock it remotely so that unauthorized users cannot access the sensitive business data. If the user forgets the passcode, you can remotely clear the passcode to ensure uninterrupted data access.

Mobile device management key benefits

The following are the key benefits of mobile device management:

- Saves time by providing an ability to see and manage all mobile devices from a single interface instead of using another solution to manage mobile devices, including for reports and queries
- Improves security through the ability to remotely erase or lock a mobile device, clear passcodes, install configuration profiles, and manage compliance by regularly updatting the information about device (basics), certificates, restrictions, and security
- Improves productivity and end user satisfaction by providing the ability to install, update, and remove applications for mobile users
- Reduce the cost of compliance by automating the inventory and track the financial information of the device durinig its lifecycle

Related topics

Configuring mobile device management

Managing mobile devices

Planning

This section helps you to get started with the planning of your installation and setting up BMC Client Management.

The following table provides links to relevant topics based on your goal:

Goal	Instructions
Review the system requirements	• System requirements • Onsite installation - hardware requirements • Onsite installation - software requirements • OnDemand installation - hardware requirements • OnDemand installation - software requirements
Understand what configurations are supported BMC Client Management	• Supported configurations
Understand licensable attributes and its purposes	• License entitlements
Know the default network ports	• Network ports
Understand sizing guidelines and general hardware recommendations for supported database	• Database best practices • Oracle 12c recommendations • PostgreSQL recommendations • SQL Server recommendations

System requirements

Depending on the architecture, the the hardware and software requirements must be met before installing BMC Client Management components:

BMC Client Management Onsite

- Onsite installation - hardware requirements
- Onsite installation - software requirements

BMC Client Management OnDemand

- OnDemand installation - hardware requirements
- OnDemand installation - software requirements

Onsite installation - hardware requirements

The following sections provide a quick overview of the minimum hardware requirements for the different components of BMC Client Management . For more detailed information and specific database recommendations refer to Database best practices.

Hardware requirements for the master, database, and relays

This table lists the recommended hardware per node count. It is important to understand that this document generalizes the hardware recommendations and the hardware requirements can be more or less for any given environment. When running in virtual environments, CPU, RAM, and NIC utilization on the host system can impact performance. Dedicated physical CPU, RAM, and NIC cards can improve performance.

Evaluation or <500 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	Dedicated relay should not be required [1]	Dedicated database should not be required
Core	2		
Speed	2 GHz		
Cache	2 MB		
RAM	4 GB		
Estimated size	50 Gb		

<20,000 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	1	2
Core	4	4	4
Speed	2 GHz	2 GHz	2 GHz
Cache	8 MB	8 MB	8 MB
RAM	8 GB	8 GB	16 GB
Disk size for Client Management data storage	65GB free space, 15k RPM or faster drives [5]	60GB [5]	20GB [6]

<50,000 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	1	2
Core	4	4	4
Speed	2 GHz	2 GHz	3 GHz
Cache	8 MB	8 MB	12 MB
RAM	16 GB	8 GB	24 GB
Disk size for Client Management data storage	73GB free space, 15k RPM or faster drives [5]	60GB [5]	50GB [6]

<100,000 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	1	2
Core	4	4	8
Speed	2 GHz	2 GHz	3 GHz
Cache	8 MB	8 MB	20 MB
RAM	16 GB	8 GB	48 GB
Disk size for Client Management data storage	85 GB free space, 15k RPM or faster drives [5]	60 GB [5]	100 GB [6]

<150,000 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	1	2
Core	4	4	8
Speed	2 GHz	2 GHz	3 GHz
Cache	8 MB	8 MB	20 MB
RAM	16 GB	8 GB	72 GB
Disk size for Client Management data storage	98 GB free space, 15k RPM or faster drives [5]	60 GB [5]	150 GB [6,7]

<200,000 nodes

	Master server	Each relay [2,3]	Dedicated database [4]
CPU	1	1	2
Core	4	4	8
Speed	2 GHz	2 GHz	3 GHz
Cache	8 MB	8 MB	20 MB
RAM	16 GB	8 GB	96 GB
Disk size for Client Management data storage	110 GB free space, 15k RPM or faster drives [5]	60 GB [5]	200 GB [6,7]

1. Required disk space varies based on size of deployed packages, patches and service packs.
2. Number of relays required varies based upon network topology and other environmental factors.

3. These estimations are for infrastructures in which a Windows relay has a maximum of 2000 child nodes or a Linux relay has 5000 child nodes. If your infrastructure requires more nodes per relay contact BMC support for specific sizing.
4. Check with the database vendor to identify any hardware limitations based upon the version in use. Your licensed database version cannot utilize all hardware resources, for example, Microsoft SQL Express, Microsoft SQL Workgroup, Oracle Express.
5. The amount of required disk space is estimated for usage over 3 years if all space consuming functionalities are used. Individual estimations are as follows: patch management 18 GB, software distribution 30 GB, operating system distribution 5 GB per image, other (temporary files, reports, and so on) 10 GB.
6. This is the estimated disk size for storing only Client Management generated data. For detailed information on the required database size and best practices see Database best practices .
7. BMC recommends and Oracle or PostgreSQL database on Linux for better performance, but an SQL Server database is also possible to use SQL Server.

Hardware requirements for the console

Computers on which the console is to be launched require at least 2 GB RAM.

Onsite installation - software requirements

This topic contains the following software requirements:

- Master, relays, and clients
- BMC Client Management master database server
- BMC Client Management console
- Supported directory servers
- Supported browsers
- Supported email servers and platforms

Master, relays, and clients

The BMC Client Management master requires the Oracle Java Runtime Environment (JRE) version 1.8 or later (provided with the installation program for Windows installations).

Operating Systems	Master server [1,2,3,5,6]	Relays [1,2,3,4,5,6]	Clients [1,2,3,4,5,6]
Windows			
Windows Server 2016	✔	✔	✔
Windows Server 2008 SP2 (32/64 bit)	✔	✔	✔
Windows Server 2008 R2 SP1	✔	✔	✔
Windows Server 2012	✔	✔	✔
Windows Server 2012 R2	✔	✔	✔

Operating Systems	Master server [1,2,3,5,6]	Relays [1,2,3,4,5,6]	Clients [1,2,3,4,5,6]
Windows Server 2016	✓	✓	✓
Windows XP SP2 (64 bit)	✗	✗	✗
Windows XP SP3 (32 bit)	✗	✗	✗
Windows XP Embedded SP3 (32/64 bit)	✗	✗	✗
Windows Vista with SP1 (32/64 bit)	✗	✗	✓
Windows 7 (32/64 bit)	⚠	✓	✓
Windows 7 Embedded (32/64 bit)	✗	✓	✓
Windows 8 (32/64 bit)	⚠	✓	✓
Windows 8.1 (32/64 bit)	⚠	✓	✓
Windows 8.1 Embedded (32/64 bit)	✗	✓	✓
Windows 10 (32/64 bit)	✗	✓	✓
Linux			
Red Hat Enterprise 6 and 7	✓	✓	✓
Suse 12	✗	✓	✓
Suse 13	✓	✓	✓
CentOS 6 and 7	✓	✓	✓
Debian 7, 8	✓	✓	✓
Ubuntu LTS 14.04	✓	✓	✓
Ubuntu LTS 16.04	✓	✓	✓
Mac			
Mac OS X v10.5 (Leopard)	✗	✗	✓
Mac OS X v10.6 (Snow Leopard)	✗	✗	✓
Mac OS X v10.7 (Lion)	✗	✗	✓
Intel Based Mac OS: v10.8 (Mountain Lion)	✗	✗	✓
Intel Based Mac OS: v10.9 (Mavericks)	✗	✗	✓
Intel Based Mac OS: v10.10 (Yosemite)	✗	✓	✓
Intel Based Mac OS: v10.11 (El Capitan)	✗	✓	✓

Operating Systems	Master server [1,2,3,5,6]	Relays [1,2,3,4,5,6]	Clients [1,2,3,4,5,6]
Intel Based, Mac OS: v10.12 (Sierra)	✗	✓	✓

Legend:

✓ : Fully supported.

⚠ : Supported for evaluation and proof of concept only, not recommended for production environment.

✗ : Not supported.

1. Minimum requirements do not include the total requirements for the server operating system or any other application (that is, MS SQL, MS IIS, antivirus, and so on) installed on the same server.
2. If several Client Management components (that is, Client Management Master Server, database, or web server application) are installed together on a common server, the minimum requirements for each server component must be combined, and note 1 also applies.
3. Actual requirements and product functionality might vary based on your system configuration and operating system.
4. Recommendation: at least 512 Kbps connectivity from audited computer to Client Management relay.
5. Itanium 64-bit processes are not supported.
6. Windows XP is not supported.

⚠ BMC Client Management 12.6 does not support Windows XP, but it is possible to install agents on devices running Windows XP. However, there are known issues when BMC Client Management 12.6 is installed on devices running Windows XP.

On Windows XP x64 SP2 the following issues are known:

- Patch Inventory is not available
- Security Products Inventory is not available

BMC Client Management master database server

Platform	Supported versions
Microsoft SQL Server (Express, Standard and Enterprise editions (Windows masters only)	• Microsoft SQL Server 2008 (32/64 bit) • Microsoft SQL Server 2008 R2 (32/64 bit) • Microsoft SQL Server 2012 (32/64 bit) • Microsoft SQL Server 2014 (32/64 bit) • Microsoft SQL Server 2016 (32/64 bit)

Platform	Supported versions
Oracle RDBMS	• Oracle 11g: 11.2.0.2 (with 10.2.0.4/5 or 11.2.0.2 client), 11.2.0.3 • Oracle 12c: 12.1.0.2.0
PostgreSQL (Linux masters only)	• PostgreSQL 8.4 and above • PostgreSQL 9.5

For more information, see Database best practices.

BMC Client Management console

The BMC Client Management console requires the Java Runtime Environment (JRE) version 1.8 and later (version 1.8 update 40 is provided with the installation program).

Supported directory servers

Component	Supported Platforms
Microsoft Active Directory	Microsoft Active Directory Services (ADS) 2008 R2, 2012, 2012 R2, and 2016
Lotus Domino	Lotus Domino 9.0
Novell eDirectory	Novell eDirectory 8.8
LDAP	

Supported browsers

The BMC Client Management user interface, specifically, the MyApps application kiosk, requires one of the following browsers:

Browser	Notes
Google Chrome (version 43 and later)	Requires the LocalLink Add-on to be installed if intranet shares are to be advertised in MyApps.
Microsoft Internet Explorer 10 and 11	
Microsoft Edge (version 20 and later)	
Mozilla Firefox (version 38 and later)	Requires the LocalLink Add-on to be installed if intranet shares are to be advertised in MyApps.
Apple Safari (versions 6 and later)	Does not support direct links to intranet shares in MyApps.

Supported email servers and platforms

Component	Supported Platforms
Email Servers with support for SMTP	• BMC Client Management requires SMTP for sending email notifications • Secure SMTP (SSL)

Component	Supported Platforms
	• Authenticated SMTP

OnDemand installation - hardware requirements

Hardware requirements for the relays

This table lists the recommended hardware per node count. It is important to understand that this document generalizes the hardware recommendations. The hardware requirements can be more or less for any given environment.

When running in virtual environments, CPU, RAM, and NIC utilization on the host system can impact performance. Dedicated physical CPU, RAM, and NIC cards can improve performance.

Evaluation

Parameter	Value
CPU	1
Core	2
Speed	2 GHz
Cache	2 MB
RAM	4 GB
Estimated size	50 GB

Production

Parameter	Value
CPU	1
Core	4
Speed	2 GHz
Cache	8 MB
RAM	8 GB
Disk size	60 GB These estimations are for infrastructures in which for best performance, a Windows relay has a maximum of 2000 child nodes or a Linux relay has a maximum of 5000 child nodes. If your infrastructure requires more nodes per relay, contact BMC support for specific sizing. If the master relay takes over all space consuming master functionalities, the amount of required disk space is estimated for usage over 3 years. Individual disk size estimations are as follows, which must to be added to the relay that has the respective functionality: • Patch management: 18 GB • Software distribution: 30 GB • Operating system distribution: 5 GB per image • Other (temporary files, reports, and so on) 10 GB

Parameter	Value

Hardware requirements for the console

Computers on which the console is to be launched require at least 2 GB RAM.

OnDemand installation - software requirements

This topic contains the following software requirements:

- Relays and clients
- BMC Client Management console
- Supported directory servers
- Supported browsers
- Supported browsers for browser-based console
- Supported email servers and platforms

Relays and clients

Platform	Supported versions [1,2,3,4,5, 6]
Windows operating system	• Windows Server 2016 • Windows Server 2008 SP2 (32/64 bit) • Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Windows 7 (32/64 bit) • Windows 7 Embedded (32/64 bit) • Windows 8 (32/64 bit) • Windows 8.1 (32/64 bit) • Windows 8.1 Embedded • Windows 10 (32/64 bit)
Linux operating system	• Linux RHEL 6 and 7 • SUSE 12 and 13 • CentOS 6 and 7 • Debian 7.0 and 8.0 • Ubuntu LTS (14.04, 16.04)
Mac operating system	• Intel Based Mac OS: v10.5 (Leopard) • Intel Based Mac OS v10.6 (Snow Leopard) • Intel Based Mac OS: v10.7 (Lion) • Intel Based Mac OS v10.8 (Mountain Lion) • Intel Based Mac OS v10.9 (Mavericks) • Intel Based Mac OS X v10.10 (Yosemite) • Intel Based Mac OS X v10.11 (El Capitan) • Intel Based Mac OS X v10.12 (Sierra)

1. Minimum requirements do not include the total requirements for the server operating system or any other application (that is, MS SQL, MS IIS,antivirus, and so on) installed on the same server.
2. If several Client Management components (that is, Client Management Master Server, database, or web server application) are installed together on a common server, the minimum requirements for each server component must be combined, and note 1 also applies.
3. Actual requirements and product functionality might vary based on your system configuration and operating system.
4. Recommendation: at least 512 Kbps connectivity from audited computer to Client Management Relay.
5. Itanium 64-bit processes are not supported.
6. Windows XP 32- and 64-bit is not supported. Production installations should always use a server operating system.

BMC Client Management console

The BMC Client Management console requires the Java Runtime Environment (JRE) version 1.7 update 55 or later (version 1.8 update 40 is provided with the installation program.)

Supported directory servers

Component	Supported Platforms
Microsoft Active Directory	Microsoft Active Directory Services (ADS) 2008 R2, 2012, 2012 R2, 2016
Lotus Domino	Lotus Domino 8.0, 8.5, 9.0
Novell eDirectory	Novell eDirectory 8.7, 8.8
LDAP	

Supported browsers

The BMC Client Management user interface, specifically, the MyApps application kiosk, requires one of the following browsers:

Browser	Notes
Google Chrome (latest version)	Requires the LocalLink Add-on to be installed if intranet shares are to be advertised in MyApps.
Microsoft Internet Explorer (version 11)	Microsoft Internet Explorer version 8 does not support HTML5. Any charts that are part of the agent interface cannot be displayed in this browser version.
Microsoft Edge (latest version)	
Mozilla Firefox (latest version)	Requires the LocalLink Add-on to be installed if intranet shares are to be advertised in MyApps.
Apple Safari (versions 6, 7, 8, 9, 10)	Does not support direct links to intranet shares in MyApps.

Supported browsers for browser-based console

The browser-based console is not available with a BMC Client Management version earlier to version 11.5.

Browser	Notes
Google Chrome (latest version)	(optional) Requires SSL certificate to be installed
Internet Explorer 11	Microsoft Internet Explorer version 8 does not support HTML5.
Edge, Current version	
Firefox, Current version	
Safari (version 9, 10)	Requires SSL certificate to be installed

Supported email servers and platforms

Component	Supported Platforms
Email Servers with support for SMTP	• BMC Client Management requires SMTP for sending email notifications • Secure SMTP (SSL) • Authenticated SMTP

Supported configurations

This topic provides information about different configurations supported by BMC Client Management 12.5.

- Supported core functions
- Supported virtualization
- Supported bare metal hypervisors (virtual infrastructure element)
- Supported languages

Supported core functions

Depending on the operating systems of your client, BMC Client Management supports the following core functions:

Core Functions	Windows	Mac	Linux	iOS
Discovery/Inventory	✓	✓	✓	✓
Applications Usage (Self-healing and Blocking)	✓	✗	✓ 2	✗
Software Deployment	✓	✓	✓	✓ 3
OS Deployment	✓ 1	✗	✗	✗
Patch Management	✓	✗ 5	✗	✗

Core Functions	Windows	Mac	Linux	iOS
Remote Control	✓	✓	✗	✗
Direct Access	✓	✓	✓	✓ 4
USB & Port Security	✓	✗	✗	✗
Power Management	✓	✓	✓	✗

1. The operating system for OSD must be listed in the supported Windows Operating Systems for the master server. For more information on the supported operating systems for master server, see Master, relays, and clients.
2. Self-healing is only available on Windows operating systems.
3. Install and remove mobile applications.
4. Direct commands for locking, unlocking, and wiping the mobile device.
5. Patch systems running Mac OS by using the operational rules functionality. For more information, see:
   - Applying a patch to BMC Client Management
   - Patch Management steps

Supported virtualization

Component	Supported Platforms [1]
Virtual Platform Support	BMC Client Management (Client Management) was proven by BMC Software customers to function properly in virtualized data centers that use VMware® ESXi™, VMware® Infrastructure™ and Microsoft Hyper-V Core Server 2008 R2. Client Management is only supported in these environments if the product is installed on an approved OS platform, web server, and database. Client Management might work properly on other virtualization products, but BMC Software has not tested them and verified that functionality. BMC Software has no documented statistics regarding the performance of Client Management in these environments since the mix of outside vendors' applications and hardware can have a direct impact on overall performance.Additionally, should BMC Software believe that the virtualization layer is the root cause of an incident the customer is required to contact the appropriate virtualization layer support provider to resolve the virtualization issue. Note, that BMC server components are not supported on VMware Server™ or VMware Workstation using the GSX engine in a production environment since it is not designed for hardware optimization.

1. The OSD Manager (functional agent module/role) is not supported on a virtual platform. It must be designated/reside on a physical host due to TFTP constraints with virtualization.

Supported bare metal hypervisors (virtual infrastructure element)

Inventory Manager can discover bare metal hypervisors and detect their configuration and attached virtual machine, and it allows for management of those virtual machines. This functionality is supported on:

Component	Supported Platforms
VMWare	vSphere, ESX and ESXi1 [1] v3.5 and 4.x
Microsoft	Hyper-V 2008

1. The VMWare licensing policy limits the free version of VMware ESXi to read-only access by the VMWare vSphere SDK. To enable full functionality (that is, active management such as start/stop Virtual Machines) on a VMware ESXi host, the host must be licensed with vSphere Essentials.

Supported languages

BMC Client Management console is available in the following languages:

- US English
- French
- German
- Japanese
- Spanish
- Brazilian Portuguese

License entitlements

BMC Client Management has several licensable attributes. Each of these is enabled or disabled based on the installed license file. The below table covers each major attribute and its purpose.

You can access attribute information in the product under the **Global Settings > Licenses** node.

Attribute Name	Module	Description
BMC Client Management Agents	**All**	The total number of agents that can be deployed within an environment.
Compliance Management	Compliance Manager	The is the number of devices which are assigned to compliance rules.
Power Management	Compliance Manager	This is the allowed number devices which have uploaded a power management events to the server. This information is only collected via an agent.
Windows Device Management	Compliance Manager	The is the number of devices which are assigned to device management rules.
Software Catalog	Compliance Manager	This is the allowed number devices which have uploaded a normalized software inventory to the server. This value could be decremented by agent based, or agent-less audits of a device.
	Compliance Manager	

Attribute Name	Module	Description
Software Catalog Updates		This is the date when the automated software catalog updates will cease to download and be imported into the system (This subscription is typically co-terminus with the support expiration date).
Security Configuration Updates	Compliance Manager	This is the date when the automated security configuration updates will cease to download and be imported into the system (This subscription is typically co-terminus with the support expiration date).
Software Distribution	Deployment Manager	The is the number of devices which are assigned to software packages.
Operating System Deployment	Deployment Manager	This is the number of devices which the system is entitled to deploy operating systems to.
Inventory	Inventory Manager	This is the allowed number devices which have uploaded an inventory to the server. This value could be decremented by agent based, or agent-less audits of a device.
Application Management	Inventory Manager	The is the number of devices which are assigned to application lists for either monitoring, prohibiting or self healing an application.
Patch Management	Patch Manager	This is the allowed number devices which have uploaded a patch inventory to the server. These inventories are only collected via an agent.
Patch Knowledge Base Update	Patch Manager	This is the date when the automated patch knowledge-base updates will cease to download and be imported into the system (This subscription is typically co-terminus with the support expiration date).
Remote Control	Remote Manager	This is the number of devices which the system is entitled to take remote control of.
Direct Access	Remote Manager	This is the number of devices which the system is entitled to remotely access the registry and file system on devices.

You can download the components mentioned herein from the Electronic Product Distribution website. Use the same user name and password that you use to access the Customer Support website.

If you do not have a current license for the components you want, contact a BMC sales representative by calling (+1) 800 793 4262 . If you cannot download the components, contact a sales representative and ask for a physical kit to be shipped to you.

Network ports

Component	Description and defaul ports [1,2]
Client agent	General agent communication port as configured (default is 1610)
Management console	General console management port as configured (default is 1611)
Bandwidth throttling	Bandwidth management port on relay servers (default is 1609)
MyApps	MyApps port on master server (default is 1612)

Component	Description and defaul ports [1,2]
Integration port	Port used for third-party integrations and set with a specific SSL certificate (default is 1616)
TCP discovery	TCP ports scanned for auto-discovery (default is 23,25,139)
Multicast traffic	Multicast transfer agent listening port as configured (default is 2500)
Active directory LDAP	LDAP port (default is 389)
Rollout	For disk access on the remote device using SMB, TCP port 139 or 445 To access the remote RPC service, TCP port 135
Mobile Management	Mobile Manager port (default 1661)

Notes

- Ports are configurable.
- The ports for client agent and management console are required; all other ports are optional.
- The port for client agent (default 1610) is the primary port used by BMC Client Management for network communications with respect to assignment information, inventory data, or any Parent-Child data transfers. This port should be open on all systems which have the BCM agent installed and will be designated for use as a parent device.
- The port for management console (default 1611) provides the same functionality as the port for client agent, but traffic is given priority over pending traffic on port for client agent. This port should be open on all systems which have the BCM agent installed and will be designated for use as a parent device. TCP port 1611 is often used for the console connection, or for client devices that must maintain an active tunnel to their parent device.

Database best practices

This section provides general database hardware recommendations and hardware sizing guidelines for your configuration.

Optimal database performance requires regular monitoring and health checks. BMC recommends analyzing the longest running queries and modifying indexes to improve the overall performance.

This section provides recommendations for the following databases:

- Oracle 12c recommendations
- PostgreSQL recommendations

- SQL Server recommendations

This topic also includes:

- General database hardware recommendations
- Hardware sizing recommendations

General database hardware recommendations

The following table lists hardware recommendations for any database server used with BMC Client Management .

Hardware type	Recommendation
Disks	• SAS disks • 10,000 - 15,000 RPM or higher
RAID	RAID 10 or 1+0, RAID 10 for write-heavy environments and high-performance database systems
Disk controllers	Separate disk controller, to free the CPU to perform other tasks. A separate disk controller also manages the movement of the disk head and reading or writing of data on the disk.
Memory	ECC RAM
CPUs	• High speed • Large L2 cache for dealing with large amounts of data • 64-bit performance
Network	• Gigabyte • Dedicated connections between application and database server

Hardware sizing recommendations

The following table lists sizing recommendations for the dedicated hardware resources required by the server database, depending on the number of nodes.

Number of nodes	Memory	CPU/Core/Speed/Cache	Estimated database size
20,000	16 GB	2/4/2 GHz/8.0 MB	20 GB
50,000	24 GB	2/4/3 GHz/12 MB	50 GB
100,000	48 GB	2/8/3 GHz/20 MB	100 GB
150,000	72 GB	2/8/3 GHz/20 MB	150 GB
200,000	96 GB	2/8/3 GHz/20 MB	200 GB

Oracle 12c recommendations

The database is an important part of BMC Client Management , especially in highly distributed environments. For each of the three basic types of database-Web Application (Web), Online Transaction Processing (OLTP), and Data Warehousing (DW)-the hardware component priorities are different. Client Management works like a web application with web services; it behaves like an OLTP application when integrating all information reported by devices; and it performs like a DW application for report generation, aggregating the results and displaying inventory views.

This topic provides recommendations for the appropriate database configuration for Oracle 12c in highly distributed environments:

Disk layout

When you run the `Create_TS.oracle.sql` script, which is provided for tablespace creation on your database, BMC recommends that you segregate the tablespaces on different disks, as shown in the following tables:

Tablespaces for tables

Small	Large	Static
BCM_DATA	BCM_EL	BCM_VMCKB
BCM_VM	BCM_INV	BCM_ESIDKB
BCM_WQ	BCM_DELTAINV	BCM_PATCH
—	BCM_VMINV	—
—	BCM_ESIDDATA	—
—	BCM_SCAP	—

Tablespaces for indexes

Small	Large	Static
BCM_INDEX	BCM_ELINDEX	BCM_VMCKBINDEX
BCM_VMINDEX	BCM_INVINDEX	BCM_ESIDKBINDEX

Small	Large	Static
BCM_WQINDEX	BCM_DELTAINDEX	BCM_PATCHINDEX
—	BCM_VMINVINDEX	—
—	BCM_ESIDDATAINDEX	—
—	BCM_SCAPINDEX	—

Recommended minimum disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	ext3	/ SYSTEM - ORACLE
1	10 K / 15 K	ext3	/ REDO LOG
1	10 K / 15 K	ext3	/ TABLESPACES FOR TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR INDEXES
1	10 K / 15 K	ext3	/ TEMPORARY TABLESPACES

Recommended best disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	ext3	/ SYSTEM - ORACLE
2	10 K / 15 K	ext3	/ REDO LOG
1	10 K / 15 K	ext3	/ TABLESPACES FOR SMALL TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR LARGE TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR STATIC TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR SMALL INDEXES
1	10 K / 15 K	ext3	/ TABLESPACES FOR LARGE INDEXES
1	10 K / 15 K	ext3	/ TABLESPACES FOR STATIC INDEXES
1	10 K / 15 K	ext3	/ TEMPORARY TABLESPACES

Recommended RAID implementation

Disk	Rmp/s	RAID level	File system	Purpose
2	10 K / 15 K	10	ext3	/ SYSTEM
8	10 K / 15 K	10	ext3	/ ORACLE + TABLESPACES
2	10 K / 15 K	10	ext3	/ REDO LOG
2	10 K / 15 K	10	ext3	/ TEMPORARY TABLESPACES

Storage capacity sizing

When sizing storage capacity for an Oracle system, you need to consider the following Oracle database components:

- Database files
- Online REDO log files
- Backup/flash data

Database element	Space requirement	20,000 nodes	50,000 nodes	100,000 nodes	150,000 nodes	200,000 nodes
Database files	DB size	20 GB	50 GB	100 GB	150 GB	200 GB
Temporary tablespace	DB size * 0.2	4 GB	10 GB	20 GB	30 GB	40 GB
System/undo tablespace	DB size * 0.1	2 GB	5 GB	10 GB	15 GB	20 GB
Online redo logs	DB size * 0.2	4 GB	10 GB	20 GB	30 GB	40 GB
Archive logs	DB size * 1.0	20 GB	50 GB	100 GB	150 GB	200 GB
Backup/flash data	DB size * 2.0	40 GB	100 GB	200 GB	300 GB	400 GB
Total		**90 GB**	**225 GB**	**450 GB**	**675 GB**	**900 GB**

Memory management

Memory management is the most critical and complex part of tuning Oracle databases for performance. Our testing environment confirmed that using `AMM` provided better performance if the correct initial settings for `MEMORY_TARGET` are specified.

Number of nodes	MEMORY_TARGET
20,000	16 GB
50,000	24 GB
100,000	48 GB
150,000	72 GB
200,000	96 GB

Initialization parameters

For optimal performance with Client Management , the following Oracle database initialization parameters are recommended.

Parameter	Value
filesystemio_options	SETALL
query_rewrite_enabled	FALSE
optimizer_mode	CHOOSE
optimizer_features_enable	9.2.0
cursor_sharing	FORCE
open_cursors	800

Parameter	Value
session_cached_cursors	5000
compatible	11.2.0
commit_logging	BATCH
commit_wait	NOWAIT
optimizer_index_cost_adj	20

PostgreSQL recommendations

The database is an important part of BMC Client Management , especially in highly distributed environments. For each of the three basic types of database-Web Application (Web), Online Transaction Processing (OLTP), and Data Warehousing (DW)-the hardware component priorities are different. Client Management works like a web application with web services; it behaves like an OLTP application when integrating all information reported by devices; and it performs like a DW application for report generation, aggregating the results and displaying inventory views.

This topic provides recommendations for the appropriate database configuration for PostgreSQL 9.1 in highly distributed environments:

Disk layout

When you run the `Create_TS.pgsql.sql` script, which is provided for tablespace creation on your database, BMC recommends that you segregate the tablespaces on different disks, as shown in the following table:

Tablespaces for tables

Small	Large	Static
BCM_DATA	BCM_EL	BCM_VMCKB

Small	Large	Static
BCM_VM	BCM_INV	BCM_ESIDKB
BCM_WQ	BCM_DELTAINV	BCM_PATCH
—	BCM_VMINV	—
—	BCM_ESIDDATA	—
—	BCM_SCAP	—

Tablespaces for indexes

Small	Large	Static
BCM_INDEX	BCM_ELINDEX	BCM_VMCKBINDEX
BCM_VMINDEX	BCM_INVINDEX	BCM_ESIDKBINDEX
BCM_WQINDEX	BCM_DELTAINDEX	BCM_PATCHINDEX
—	BCM_VMINVINDEX	—
—	BCM_ESIDDATAINDEX	—
—	BCM_SCAPINDEX	—

Recommended minimum disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	ext3	/ SYSTEM - POSTGRESQL
1	10 K / 15 K	ext3	/ PG_XLOG - WALL
1	10 K / 15 K	ext3	/ TABLESPACES FOR TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR INDEXES
1	10 K / 15 K	ext3	/ TEMPORARY TABLESPACES

Recommended best disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	ext3	/ SYSTEM - POSTGRESQL
1	10 K / 15 K	ext3	/ PG_XLOG - WALL
1	10 K / 15 K	ext3	/ TABLESPACES FOR SMALL TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR LARGE TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR STATIC TABLES
1	10 K / 15 K	ext3	/ TABLESPACES FOR SMALL INDEXES
1	10 K / 15 K	ext3	/ TABLESPACES FOR LARGE INDEXES
1	10 K / 15 K	ext3	/ TABLESPACES FOR STATIC INDEXES
1	10 K / 15 K	ext3	/ TEMPORARY TABLESPACES

Recommended RAID implementation

Disk	Rmp/s	RAID level	Location	File system	Purpose
2	10 K / 15 K	1	/sda	ext3	/ SYSTEM
2	10 K / 15 K	10	/sdb	ext3	/ POSTGRESQL + TABLESPACES
2	10 K / 15 K	1	/sdc	ext3	/ PG_XLOG -WALL
2	10 K / 15 K	None	/sde	ext3	/ TABLESPACE TEMP

Storage capacity sizing

When sizing storage capacity for a PostgreSQL system, you need to consider the following PostgreSQL database components:

- Database files
- Transaction log files
- Backup

Database element	Space requirement	20,000 nodes	50,000 nodes	100,000 nodes	150,000 nodes	200,000 nodes
Database files	DB size	20 GB	50 GB	100 GB	150 GB	200 GB
Transaction log "Wall"	DB size * 0.1	2 GB	5 GB	10 GB	15 GB	20 GB
Backup	DB size * 0.2	4 GB	10 GB	20 GB	30 GB	40 GB
Total		**26 GB**	**65 GB**	**130 GB**	**145 GB**	**260 GB**

System tuning for write-heavy operations

You can tune your system for better performance for the following write-heavy operations:

File access times

Applying the `noatime` attribute can significantly improve the file I/O performance of your server. Edit the **/etc/fstab** file and add the `noatime` attribute as follows:

```
/dev/sdb1 on / PostgreSQL ext3   rw,noatime
/dev/sdc1 on / Pg_xlog ext3   rw,noatime
/dev/sdd1 on / Tablespaces for tables ext3   rw,noatime
/dev/sde1 on / Tablespaces for indexes ext3 rw,noatime
# repeat for each additional disk
```

Read ahead

Modifying the `Read-Ahead` parameter can improve the read performance of a disk.

Type **# blockdev --getra /dev/sda** to check the `Read-Ahead` value of an individual disk. The default value is generally 256.

To permanently increase this value to 4096, edit the `/etc/rc.local` file by adding the following block to the end of the file:

```
blockdev --setra 4096 /dev/sda
blockdev --setra 4096 /dev/sdb
blockdev --setra 4096 /dev/sdc
# repeat for each additional disks
```

Read caching and swapping

Modifying the following parameters increases database performance:

Parameter	Recommendation
`vm.dirty_background_ratio`	Decrease this value to 5 to make flushes more frequent but result in fewer I/O spikes.
`vm.dirty_ratio`	Decrease this value to 10 to make flushes more frequent but result in fewer I/O spikes.
`vm.swappiness`	Deactivate swapping to eliminate the tendency of the kernel to move processes out of physical memory and onto the swap disk.

To permanently change these parameter values, edit the `/etc/sysctl.conf` file as follows:

```
vm.dirty_background_ratio = 5
vm.dirty_ratio = 10
vm.swappiness = 0
```

To set the values without rebooting, run the `sysctl -p` command after saving and exiting the `sysctl.conf` file.

Shared memory and semaphores

A large PostgreSQL installation can quickly exhaust various operating system resource limits. The following example shows how to increase the shared memory to 16 GB of RAM:

```
# sysctl -w kernel.shmmax=8420048896
# sysctl -w kernel.shmall=2055676
# sysctl -w kernel.sem = 250 32000 32 128
```

PostgreSQL configuration

PostgreSQL can easily be tuned using the third-party-tool pgtune . It is licensed under a standard three-clause BSD license. pgtune works by taking an existing **postgresql.conf** file as an input and making changes to it based on the amount of RAM in your server and a suggested workload. pgtune then outputs a new file with suggestions.

The following example is for a server with 16 GB of RAM and a suggested workload of 100 simultaneous connections to the server.

1. Enter the following command line:**# ./pgtune -i $PGDATA/postgresql.conf -o $PGDATA /postgresql.conf.pgtune --type MIXED --connections=100**
   The values recommended by pgtune are appended at the end of the **postgresql.conf.pgtune** file, for example:

```
#------------------------------------------------------------------------------
# pgtune run on 2013-07-08
# based on 16445412 KB RAM, platform Linux
#------------------------------------------------------------------------------
default_statistics_target = 100
maintenance_work_mem = 960MB
checkpoint_completion_target = 0.9
effective_cache_size = 11GB
work_mem = 80MB
wal_buffers = 16MB
checkpoint_segments = 32
shared_buffers = 3840MB
```

2. Add the following additional values at the end of the **postgresql.conf.pgtune** file:

```
bgwriter_lru_maxpages = 1000
bgwriter_lru_multiplier = 4.0
random_page_cost = 2.0
cpu_tuple_cost = 0.03
log_autovacuum_min_duration = 0
autovacuum_max_workers = 5
autovacuum_vacuum_cost_delay = 10ms
```

3. Run the following commands to apply the new parameters and values to the original **postgresql.conf** file by renaming the **postgresql.conf.pgtune** pgtune file to **postgresql.conf** and then restarting PostgreSQL:

```
mv $PGDATA/postgresql.conf $PGDATA/postgresql.conf.sav
mv $PGDATA/postgresql.conf.pgtune $PGDATA/postgresql.conf
chown postgres:postgres $PGDATA/postgresql.conf
chmod 0644 $PGDATA/postgresql.conf
service postgresql restart
```

SQL Server recommendations

The database is an important part of BMC Client Management, especially in highly distributed environments. For each of the three basic types of database-Web Application (Web), Online Transaction Processing (OLTP), and Data Warehousing (DW)-the hardware component priorities are different. Client Management works like a web application with web services; it behaves like an OLTP application when integrating all information reported by devices; and it performs like a DW application for report generation, aggregating the results and displaying inventory views.

This topic provides recommendations for the appropriate database configuration for Microsoft SQL Server 2014 in highly distributed environments:

Disk layout

When you run the `Create_TS.sqlserver.sql` script, which is provided for tablespace creation on your database, BMC recommends that you segregate the tablespaces on different disks, as shown in the following table.

Tablespaces for tables

Small	Large	Static
BCM_DATA	BCM_EL	BCM_VMCKB
BCM_VM	BCM_INV	BCM_ESIDKB
BCM_WQ	BCM_DELTAINV	BCM_PATCH
—	BCM_VMINV	—
—	BCM_ESIDDATA	—
—	BCM_SCAP	—

Tablespaces for indexes

Small	Large	Static
BCM_INDEX	BCM_ELINDEX	BCM_VMCKBINDEX
BCM_VMINDEX	BCM_INVINDEX	BCM_ESIDKBINDEX
BCM_WQINDEX	BCM_DELTAINDEX	BCM_PATCHINDEX
—	BCM_VMINVINDEX	—
—	BCM_ESIDDATAINDEX	—
—	BCM_SCAPINDEX	—

Recommended minimum disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	NTFS	/ SYSTEM - SQL Server
1	10 K / 15 K	NTFS	/ TRANSACTION LOG

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	NTFS	/ TABLESPACES FOR TABLES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR INDEXES
1	10 K / 15 K	NTFS	/ TEMPDB

Recommended best disk layout

Disk	Rmp/s	File system	Purpose
1	10 K / 15 K	NTFS	/ SYSTEM - SQL Server
2	10 K / 15 K	NTFS	/ TRANSACTION LOG
1	10 K / 15 K	NTFS	/ TABLESPACES FOR SMALL TABLES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR LARGE TABLES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR STATIC TABLES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR SMALL INDEXES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR LARGE INDEXES
1	10 K / 15 K	NTFS	/ TABLESPACES FOR STATIC INDEXES
1	10 K / 15 K	NTFS	/ TEMPDB

Recommended RAID implementation

Disk	Rmp/s	RAID level	File system	Purpose
2	10 K / 15 K	10	NTFS	/ SYSTEM + SQL Server + Backup
2	10 K / 15 K	1	NTFS	/ TRANSACTION LOG
8	10 K / 15 K	10	NTFS	/ ALL TABLESPACES
2	10 K / 15 K	10	NTFS	/ TEMPDB

Storage capacity sizing

When sizing storage capacity for an SQL Server system, you need to consider the following SQL Server database components:

- Database files
- Transaction log files
- Tempdb and backup

Storage capacity

Database element	Space requirement	20,000 nodes	50,000 nodes	100,000 nodes	150,000 nodes	200,000 nodes
Database files	DB size	20 GB	50 GB	100 GB	150 GB	200 GB
Transaction log "Simple"	DB size * 0.2	4 GB	10 GB	20 GB	30 GB	40 GB

Database element	Space requirement	20,000 nodes	50,000 nodes	100,000 nodes	150,000 nodes	200,000 nodes
tempdb	DB size * 0.1	2 GB	5 GB	10 GB	15 GB	20 GB
Backup	DB size * 1.0	20 GB	50 GB	100 GB	150 GB	200 GB
Total		**46 GB**	**115 GB**	**230 GB**	**345 GB**	**460 GB**

Database volume creation

BMC recommends that you use a basic disk storage type for all volumes. Also use the default disk alignment provided by Windows 2012 or later, and use the NTFS file system with a 64-KB allocation unit for SQL database and log partitions.

For `tempdb` , Microsoft recommends up to a 1:1 mapping between the number of files and logical CPUs. A more reasonable approach is to have a 1:1 mapping between files and logical CPUs up to eight files. If, for example, you have a server with 4 logical CPUs that manages 20,000 nodes, it creates 4 files of 500 MB for tempdb.

MS SQL configurations

To ensure that the SQL Server delivers optimum performance when working with BMC Client Management , you need to specifically configure some parameters.

> **Note**
>
> Do not run or modify any database configuration without the approval of the database administrator.

1. Run the following query on the BCM database :

```
SELECT
is_parameterization_forced as 'Parameterization Forced',
is_read_committed_snapshot_on as 'Read Committed Snapshot On' ,
snapshot_isolation_state as 'Snapshot Isolation State On'
FROM sys.databases
WHERE name LIKE '<BCM_DB_NAME>'
```

> Replace <BCM_DB_NAME> with the BCM database name, for example, **bcmdb** .

The preceeding query returns the current configuration of the database for the following parameters:

- Parameterization
- Read Committed Snapshot

- Snapshot Isolation State Verify the result for these parameters and ensure that they are all set to 1.

2. *(Optional)* If the value for one or more parameters is set to 0, execute the following steps to activate them:
   a. Connect to the SQL server instance as a user with ALTER permission on the database.
   b. Ensure that there are no active connections to the database except for the connection executing the `Alter` database command.
   c. *(Optional)* Type the following command to set the **Parameterization** option to **Forced**:

```
Alter database '<BCM_DB_NAME>' set PARAMETERIZATION FORCED
```

> Replace <BCM_DB_NAME> with the BCM database name, for example, **bcmdb** .

3. *(Optional)* Run the following SQL commands to turn on the **Read Committed Snapshot** and **Snapshot Isolation State** options:

```
ALTER DATABASE <BCM_DB_NAME> SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE <BCM_DB_NAME> SET READ_COMMITTED_SNAPSHOT ON;
```

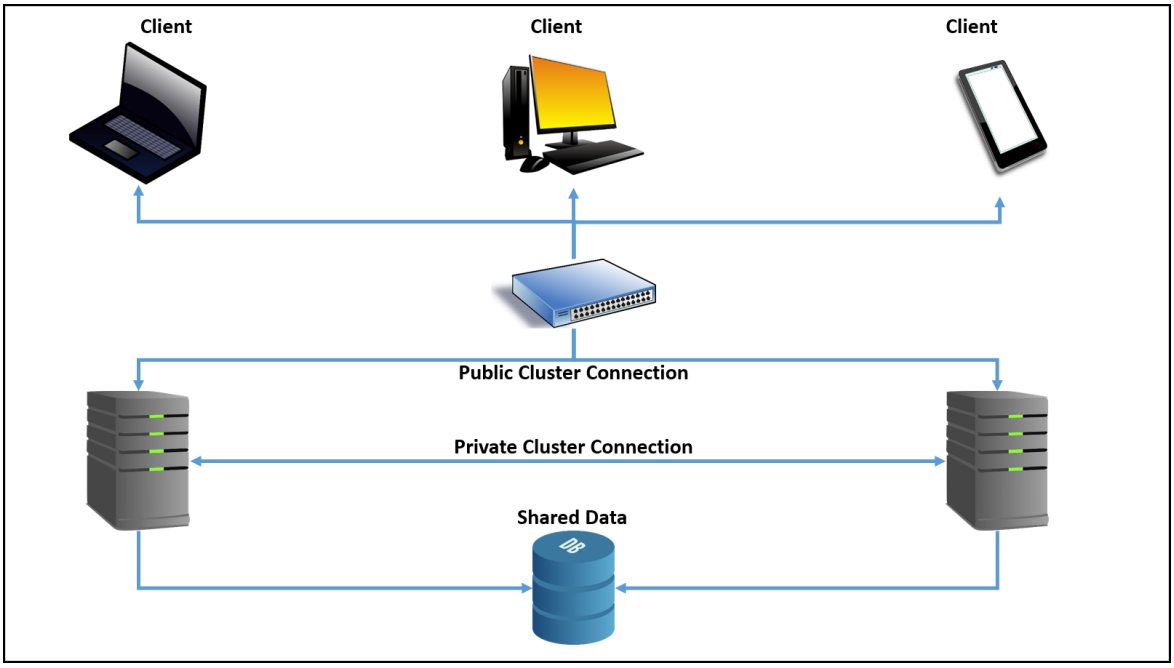
> Replace <BCM_DB_NAME> with the BCM database name, for example, **bcmdb** . If you installed version 12.1 of BMC Client Management , these recommendations are set automatically by the setup.

Best practices for fault-tolerant BMC Client Management server cluster deployment

A fault-tolerant (high-availability (HA)) deployment safeguards you against any unplanned downtime of a member node. If one member node of the cluster goes down, the connection is automatically diverted to the other available nodes. This topic walks you through some best practices for such fault-tolerant BMC Client Management server cluster deployment.

Architecture

The basic concept of a BMC Client Management fault-tolerant cluster deployment is to have the service run on individual member nodes and use a common master file directory from a shared location. The following diagram provides a high-level view of the architecture:



Prerequisites

When deploying this cluster architecture, ensure the following:

- Minimum two servers as member nodes for the cluster with individual static IP address.
- Only one master directory on a shared location, which must be accessible to each member node in the cluster.
- A cluster management system to ensure that only one member node has the service running at any given time.
  - For Windows: See http://technet.microsoft.com/en-us/library/cc731844(v=ws.10).aspx .
  - For Linux: Different distributions have different high-availability (HA) suites in their repositories. See the corresponding documentation or consult technical support for the distribution.

> **Note**
>
> You can manage the cluster by starting and stopping the service on each member node manually. However, it is not recommended for production environment.

- All the member nodes have Java installed as per software requirement. It is recommended that all the member nodes have the same Java version.

Setting up the cluster

1. Install the database client on each node.
   For more information, see corresponding database client documentation.
2. On the currently active node, install BMC Client Management master server.
   For more information, see Installing onsite.
3. On the other cluster nodes, create BMC Client Management agent service.
   For more information, see Installing onsite.
4. In the **\BMC Software\Client management\Client\config\mtxagent.ini** file, set the `StaticIPAddress` parameter to include the IP address created by your cluster management system.
   For more information, see the relevant cluster management system documentation or contact their technical support.
5. In the **\BMC Software\Client management\Client\config\identity.ini** file, in the **[identity]** section, add a hostname parameter and provide a value to it as follows:
   `hostname = myMasterName`.

   > **Note**
   >
   > By default, the **hostname** parameter is not available in the **identity.ini** file. You need to add this parameter and provide a master server name.

   This name is displayed in the console all the time and not the name of the currently active cluster node.
6. Provide the IP address of the cluster to BMC Technical Support to generate appropriate license file.

   > **Notes**
   >
   > - The IP address must be of the cluster and not of a member node.
   > - The license must not include a MAC address.

7. When rolling out agents, set the `TrustedAddress` parameter in the **FileStore** module configuration to include IP address of the each member node of the cluster and the cluster itself.
8. To create the BMC Client Management service on other member nodes:

- For Windows cluster, use the SC command. For example:

```
sc create "BMC Client Management Agent" binPath= "f:\Program Files\BMC Software\Client
Management\Master\bin\mtxagent.exe" DisplayName= "BMC Client Management Agent"
```

- For Linux cluster, copy the **/etc/init.d/BMCClientManagementAgent** file to each node.

Installing

This section provides information about installing the BMC Client Management product.

The following table provides links to relevant topics based on your goal:

Goal	Instructions
Install BMC Client Management on premises	• Installing onsite • Prerequisites for onsite installation • Downloading the installation files • Installing onsite on Windows and installation options • Installing onsite on Linux and installation options • Configuring after onsite installation • Uninstalling onsite BMC Client Management components
Install BMC Client Management in a cloud environment	• Installing OnDemand • Downloading and installing the BMC Client Management console • Configuring after OnDemand installation • Installing the master (first-level) relay • Uninstalling OnDemand BMC Client Management components

Installing OnDemand

This topic describes the steps required to install BMC Client Management components for OnDemand installation. This topic includes:

- Downloading and installing the BMC Client Management console
- Configuring after OnDemand installation
- Installing the master (first-level) relay
- Rolling out relay agents in a cloud environment
- Rolling out client agents in a cloud environment
- Uninstalling OnDemand BMC Client Management components

Note

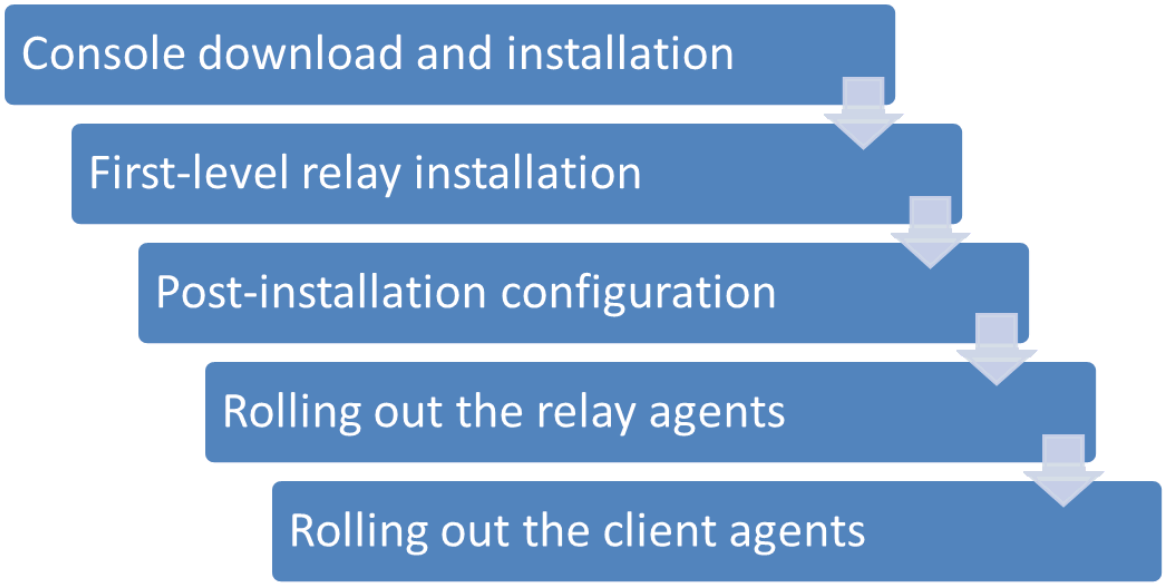
Before you start any installation task, verify that you have received your license from the BMC support team. If not, you can still install BMC Client Management with a trial license that allows you to start using BMC Client Management, but it is limited to 20 devices (including master and relays) and 30 days. When you receive your final license, you can import it and continue working and installing your remaining infrastructure devices.

Installation process overview

If you have Client Management 9.x or later installed, see Upgrading OnDemand for the upgrade procedure.

Step	Operation	Comments
1	Plan your environment	Before you start on any installation tasks you should create a schema of your network and design its components.
2	Review the system requirements (hardware and software) for Client Management	The compatibility information is subject to change. For the latest, most complete information about what is officially supported, see System requirements .
3	Download and install the console on at least one device in your network	See Downloading and installing the BMC Client Management console for detailed information on this topic.
4	First level-relay installation	In a Client Management cloud installation, one or several master relays are take the specific functionalities that are normally executed by the master server. See Installing the master (first-level) relay to install a master relay on a Windows system.
5	Perform specific configurations	After the console and the master relay are installed and before the agents are rolled out, some specific configuration tasks need be done. See Configuring after OnDemand installation .
6	Prepare for agent rollout	Before you can roll out the agent to the master relay, relays and clients in your environment, a few preparatory tasks must be done, such as importing your license and creating the target groups for the rollouts. See Configuring for agent rollout .
7	Roll out the relay agents	See Rolling out relay agents in a cloud environment for detailed information on how to roll out the BMC Client Management agents to all your relays.
8	Roll out the client agents	See Rolling out client agents in a cloud environment.

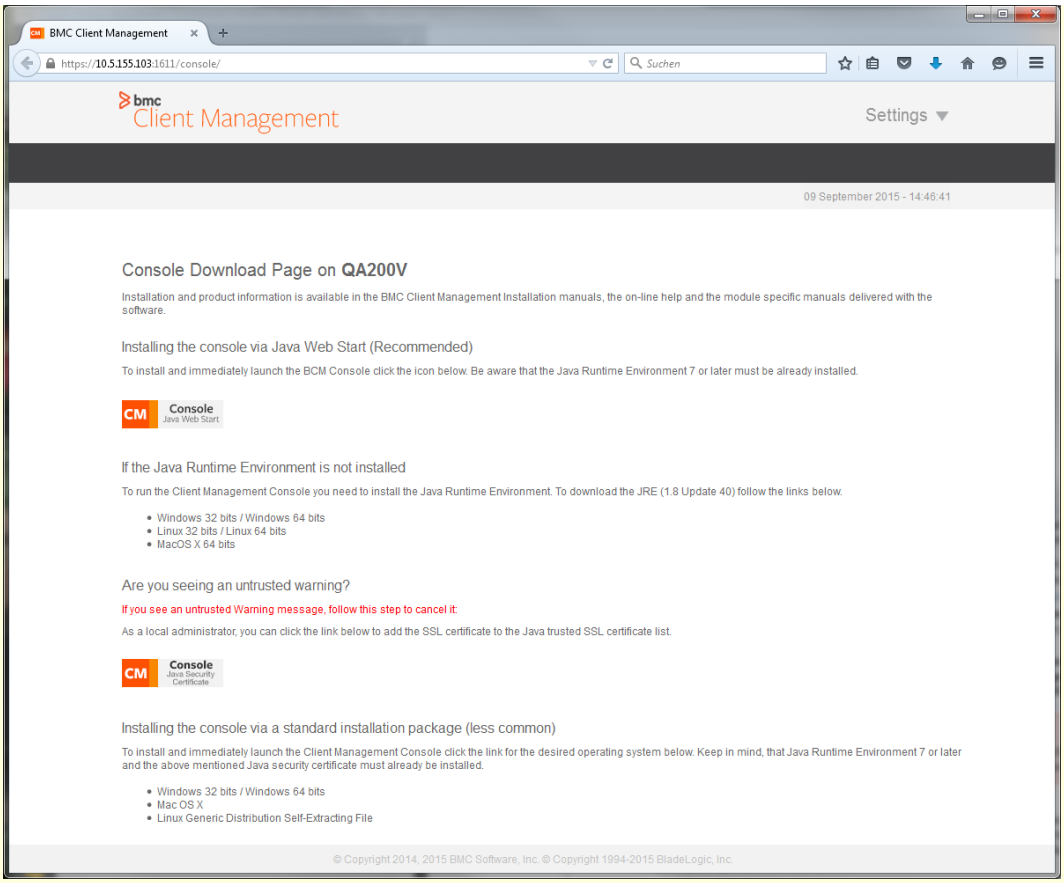
The installation procedure consists of the following steps:



Downloading and installing the BMC Client Management console

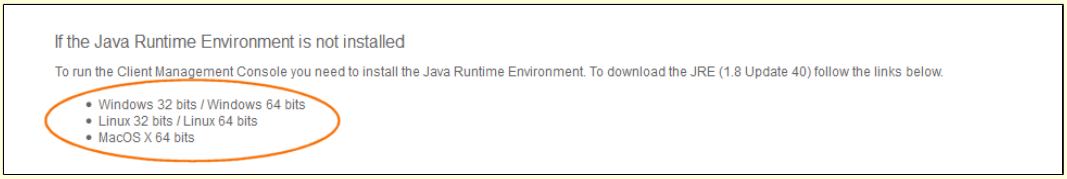
The **Console Download Page on** provides the necessary links for downloading and installing the BMC Client Management console. This page is only accessible via a browser through a specific link that is communicated to you by the OnDemand team, the format of which looks like this : `master port/console" class="external-link" rel="nofollow">http://master name:master port/console` , for example, `http://Customer123.OnBMC.com:1611 /console`.

Note:



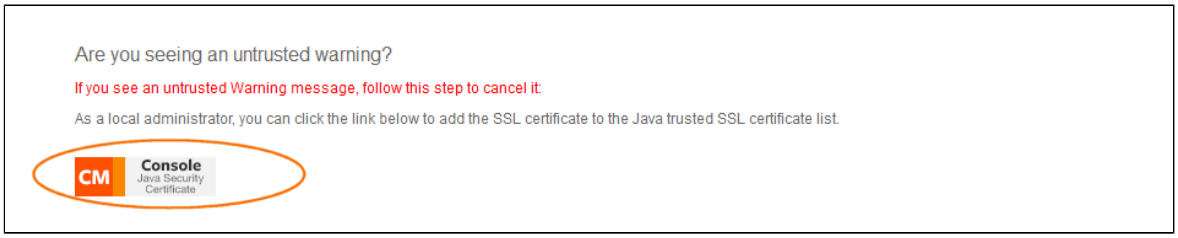
A recent version of Java Runtime Environment (JRE) must be installed on the device the console is used on.

On Linux devices, to verify if the Java is installed, type **java -version** in your terminal window and then press the **Enter** key. The version number of the installed Java is displayed. BMC recommends that you use JRE version 8.0 or later with the console. This can be downloaded from the Oracle website . You can also use the often preinstalled OpenJDK java version; it is not necessary to use the Oracle JRE.

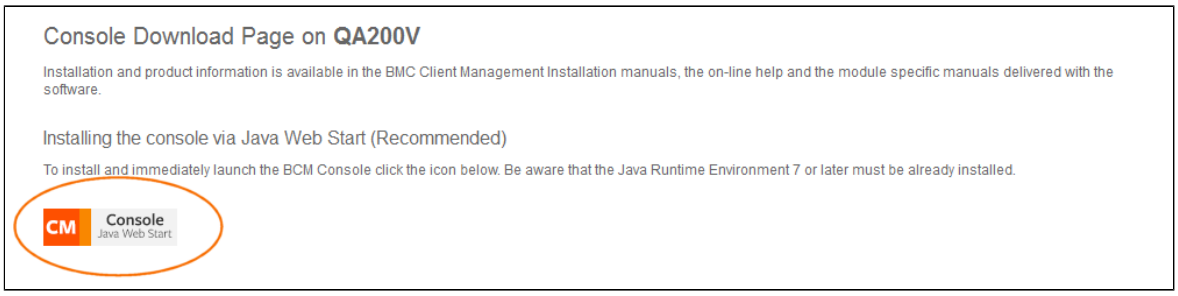


If no Java is installed on your device, click the link on the console page and install it.

A security certificate is required to allow the console to log on to the database. If you do not have one installed yet, you can use the BMC certificate provided on the console page. Click the link to install it.



To download and install the BMC Client Management console , click the respective icon on the page.



This installs the console as Java Web Start with a link to the master. A desktop link for the console is created on the device and the device keeps the files required to launch the console in its cache memory. At every console launch, a verification takes place to determine if later versions of these console files are available. If so, they are automatically updated.

> **Note**
>
> Do not empty or delete the Java cache memory, as this deletes the files required for the console Web Start. If this happens, the console must be reinstalled.

After you install the console, you can log on to the console. To do so, double-click the BMC Client Management console desktop icon, specify the login information provided by the support team, and follow the instructions to log on. For more information, see Working with BMC Client Management console.

Configuring after OnDemand installation

This section contains information about activities that you must perform *after* you install BMC Client Management and before you roll out the relay and client agents in your network:

- Import BMC Client Management licenses
- Antivirus exclusions
- Far-Eastern language support (Optional)

Installing the master (first-level) relay

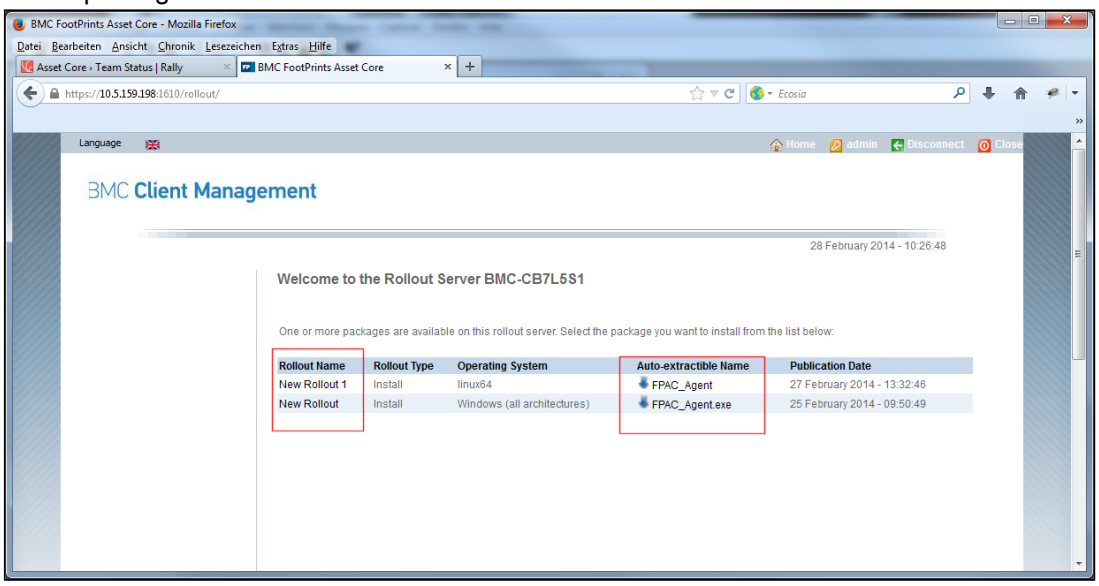
In the BMC Client Management cloud installation, one or several master relays take over the specific functionalities that are normally executed by the master server. Depending on the size of your network, you might require only one first-level relay (master relay) or several. The first relay that is installed is automatically assigned all master functionalities, such as the rollout server, patch manager, asset discovery scanner, and so on.

If you intend to only install one first-level or master relay, it is recommended that you install it on a Microsoft Windows operating system. This then allows you to roll out agents to all other devices of any type of operating system in your environment. If you only install a Linux master relay, you need to pull the rollout individually for the other operating systems. To use this type of rollout, you need to be able to physically access the relay computer or to establish a remote control session with which you can download the installation files.

The OnDemand team has specifically prepared and configured master relay rollouts for all supported operating systems for you and they are available on the rollout server page. You can download and install them on your relays.

To install a Windows master relay

1. On the Windows relay computer, open a browser and type the address that was communicated to you by the OnDemand team, the format of which normally is: **https://<master relay IP address>:<master relay port>/rollout**. For example, https://192.164.159.148:1611/rollout.
   A login window appears.
2. In the respective text boxes, enter the credentials that were communicated to you by the OnDemand team.The browser opens the rollout server page on which you can find your rollout package.



3. Click the **Rollout Name** or the **Auto-extractable Name** to start the download of the installer package.
   The **Save As** window appears.
4. Select the path in which to save the package and click **Save**.
5. Go to the file location and launch the installation.
   The new relay is now silently installed. You can see that the installation is finished and the relay is up and running when the BMC Client Management agent icon displays in the systray. The agent icon is gray  while the agent is initializing and then it changes to blue  when the agent is running.

You have now installed your first-level Windows relay and are ready to create and push the BMC Client Management agent out to all targets with supported operating systems. However, before you can proceed with the rollout, you need to do some preparatory configuration tasks. For more information, see Configuring for agent rollout.

If you want to install additional master relays, you need to repeat this procedure for each one.

Rolling out relay agents in a cloud environment

A typical Client Management architecture has a smaller number of relays directly under the master and a larger number of clients under each relay. The following topic guides you through the process of a relay rollout with one of the master relays as the direct parent of the targets.

> **Note:**
>
> This rollout uses device groups, specifically those that were synchronized with a directory server (see the Defining the rollout targets via a directory server topic). If you have not yet created a group, do so before starting this example procedure. It is also possible to find your rollout targets via other lists, such as the Microsoft Network option or autodiscovered devices. You can find information on these options in the Rollout alternatives section.

1. Select **Wizards > Agent Rollout** .
   The **Core Setup Configuration** window appears.
2. Check the box for **Enable agent as a relay for the other agents** .

   > If you want to schedule the rollout at a specific date and time check the box for second last question.

3. Click **Next** .
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, *Linux Relay Agents*) in the **Name** box.

5. Enter the name for the rollout package executable in the **Auto-extractable Name** box (for example, *linux64relayagent12.sh* for a Linux rollout, or *win7relayagent12.exe* for a Windows 7 installation).
6. Select the operating system group to which the agent is to be rolled out from the **Operating System** list, for example, *Linux 64 bit* .
7. Click **Next** .
   The **Rollout Server** window appears. It provides the list of all defined rollout servers.
8. Select the rollout server you want to use. If none of the exising rollout servers fits your requirements you can also add a new rollout server in this window. For this proceed as follows:
   a. Click **Add Device** on top of the table.
      The **Add a new rollout server** pop-up window displays displaying the list of all devices, that can be a server due to their operating system.
   b. Select the device to be added from one of the list boxes.
   c. Click **OK** to confirm and close the window.
      The device is added to the table of available servers and selected.
9. Click **Next** .
   The **Targets & Accounts** window appears.
10. Click **Select a device** .
11. Select the desired group that contains the relay rollout targets of the defined operating system type in the **Available Objects** box.
12. To select individual devices instead of a group click **All** on the left bar and select your devices from the list that appears.
13. Click **OK** to add the group and close the window.
14. Click **Add Administrator** .
15. Enter the required data for the account login in the respective text boxes.
16. To add a new account, click **Add Administrator** .
    The **Properties** dialog box appears on the screen.
17. Enter the following data for a new account login in the respective text boxes:
    a. Enter the name of the domain to which the rollout is going in the **Administrator Domain** box. If the rollout is going to all domains, you can use an asterisk (*).
    b. Enter the login name of the admin (for when the agent deployment tries to log on to the remote target to install the agent) in the **Administrator Login** box.

> - For Windows XP Professional rollouts, you *must* enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) and targets.
> - If you are not sure if your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already were set up between the different domain controllers.

c. Enter the password of the above-entered admin in the **Password** box. For security reasons the passwords is only displayed in the form of asterisks (*).
d. Confirm the above-entered the password in the next text box.
e. Click **OK** to confirm the new account and add it.
It is now shown in the list above.

18. Click **Verify Rollout** at the bottom to ensure that the credentials are correct.
19. Click **Finish** .
20. In the **Confirmation** dialog box, select the **Go to Rollout** radio button to change the focus of the console window to the new rollout.
21. Click **Yes** to confirm the immediate activation.
The focus of the console is now switched to the the **Assigned Schedule** tab of the newly created rollout. Here you can follow the general progress of the relay rollout assignment. If you did not check the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.
22. When the status value displays `Executing` , select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and the final status should be `Installed`).

Your first group of relays is now installed. If you need to have another level of relays below these, repeat this procedure for all other relays.

To continue installing your architecture with clients below the relays continue with the Rolling out client agents in a cloud environment topic.

> **Note:**
>
> When you are rolling out agents on MAC OS X devices and you want to remotely control these devices you must reboot them after the installation.

Rolling out client agents in a cloud environment

Before you continue with the following procedure, ensure that you have at least one relay installed. For instructions, see the Rolling out relay agents in a cloud environment topic.

1. Select **Wizards > Agent Rollout** .
The **Core Setup Configuration** window appears.
2. Check the **Configure the relay selection or use master otherwise** box to select a specific relay for the rollout targets.
3. If you want to schedule the rollout at a specific date and time check the **Configure a custom schedule for this rollout (default is one immediate execution)** box. Otherwise it is rolled out with the default schedule, only once immediately.
4. Click **Next** .
The **General Parameters** window appears on the screen.

5. Enter a name for the new rollout in the **Name** field, for example, *Windows 32 Bit Clients* .
6. Enter the name for the rollout package executable that will be created into the **Auto-extractable Name** field, for example, *win32clientagent12.exe* for a Windows 32-bit client rollout.
7. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** field, for example, *Windows XP/2003 ... (32 bit)* .
8. Click **Next** .
   The **Communication** window appears.
9. To find the relay click **Select a device** next to the **Parent Name** box.e
10. Click **All** .
11. Select the desired parent device from the list that appears and click **OK** .
12. Click **Next** .
    The **Targets & Accounts** window appears.
13. Click **Select a device** .
14. Select the desired group that contains the client rollout targets of the defined operating system type in the **Available Objects** box.
15. To select individual devices instead of a group click **All** on the left bar and select your devices from the list that appears.
16. Click **OK** to add the group and close the window.
17. Click **Add Administrator** .
18. Enter the required data for the account login into the respective boxes.
19. To add a new account, click **Add Administrator** .
    The **Properties** dialog box appears on the screen.
20. Enter the following data for a new account login into the respective boxes:
    a. Enter the name of the domain to which the rollout is going into the **Administrator Domain** field. If the rollout is going to all domains, you can use an asterisk (*).
    b. Enter the login name of the administrator whose account the rollout uses to log on to the remote target to install the agent into the **Login** field.

- For Windows XP Professional rollouts, you *must* enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) and targets.
- If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already were set up between the different domain controllers.

    c. Enter the password of the previously entered admin into the Password field. For security reasons the passwords will only be displayed in the form of asterisks (*).
    d. Confirm the previously entered the password into this field.

e. Click **OK** to confirm the new account and add it.
   It will now be shown in the preceding list.

21. Click **Verify Rollout** to ensure that the entered account data is correct.
22. Click **OK** and then **Finish** .
23. In the **Confirmation** dialog box, select the **Go to Rollout** radio button to change the focus of the console window to the new rollout.
24. Click **Yes** to confirm the immediate activation.
    The focus of the console is now switched to the the **Assigned Schedule** tab of the newly created rollout. Here you can follow the general progress of the relay rollout assignment. If you did not check the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.
25. When the status value displays `Executing` , select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and the final status should be `Installed`).

Your first client rollout is now completed and your installed base is large enough to execute any other operation. To install all remaining clients in your network repeat this procedure for all other target device groups.

Where to go from here

Your next step should be to familiarize yourself with the console and its objects and functionalities. You can find information on this in the **Using** section, starting with Working with BMC Client Management console.

Uninstalling OnDemand BMC Client Management components

If you need to uninstall some of the Client Management components that were installed on your infrastructure, you have the following options:

- Manually uninstalling BMC Client Management components
  - Uninstalling from Windows devices
  - Uninstalling from Linux devices
- Uninstalling BMC Client Management agents via rollout
  - Verifying the uninstallation

Be aware that uninstalling an agent from a device does *not* automatically remove the device from the BMC Client Management database; it must be removed manually from there via the console. If you do not delete the device in the database, it is still displayed in all its groups with the connection status **Lost** and a red icon () after the device lost time defined in the system variables.

Manually uninstalling BMC Client Management components

You can manually locate and uninstall the following BMC Client Management components:

- BMC Client Management Client

- BMC Client Management Console

BMC Client Management agents (relays as well as simple clients) can only be uninstalled manually if they also were installed manually. If they were installed by rollout, they also must to be uninstalled by rollout.

Uninstalling from Windows devices

You can uninstall the BMC Client Management components from a Windows device from the **Add /Remove Programs** window of **Control Panel**. When the uninstallation is complete, you can see that the respective BMC Client Management component is removed from the programs list in the **Add /Remove Programs** window and the agent icon has disappeared from the system tray.

Uninstalling from Linux devices

You can uninstall the BMC Client Management components from a Linux device using the following commands in a terminal window:

1. Open a terminal window and type the following commands as required:

Component to be uninstalled	Command
BMC Client Management Console	`bmc-client-management-console-uninstall`
BMC Client Management Client	`bmc-client-management-client-uninstall`

> **Note**
>
> You can only manually uninstall a client that was manually installed. Clients that were installed via rollout must also be uninstalled via rollout.

2. Press the **Enter** key.

> **Note**
>
> Be aware that any files which are generated during the use of BMC Client Management , such as log files, data files, and so on, are not automatically deleted during the uninstallation of the components. They must be deleted manually.

Uninstalling BMC Client Management agents via rollout

Agents that were installed via a rollout must also be uninstalled via a rollout. For more information on uninstalling the BMC Client Management agent via rollout, see Uninstalling the client agent via rollout.

Verifying the uninstallation

1. In the **Global Settings> Rollouts> (Uninstall rollout) > Servers> (Your Rollout Server)** node, select the **Targets** tab.
   All defined target devices are listed.
2. Monitor the advancement of the rollout under **Status**. The different statuses are as following:

Rollout Status	Description
Initial	Rollout is defined and preparing to execute
Successful	Rollout is successfully executed
Processing	Rollout is still executing
At least one device failed	Rollout failed on one or more target devices

Note

Devices that cannot be accessed directly by the rollout (for reasons such as they are in another domain or behind a firewall) must download the uninstallation package from the **Rollout Server** page of the server's agent browser interface and execute it. The link to server's agent browser interface is typically in the following format: **http://<rollout server name>:<rollout server port>/rollout**.

Installing onsite

This topic describes the steps required to install all components of BMC Client Management on your infrastructure. This topic includes:

- Prerequisites for onsite installation
- Downloading the installation files
- Installing onsite on Windows and installation options
- Installing onsite on Linux and installation options
- Configuring after onsite installation
- Uninstalling onsite BMC Client Management components
- Applying a patch to BMC Client Management

Note

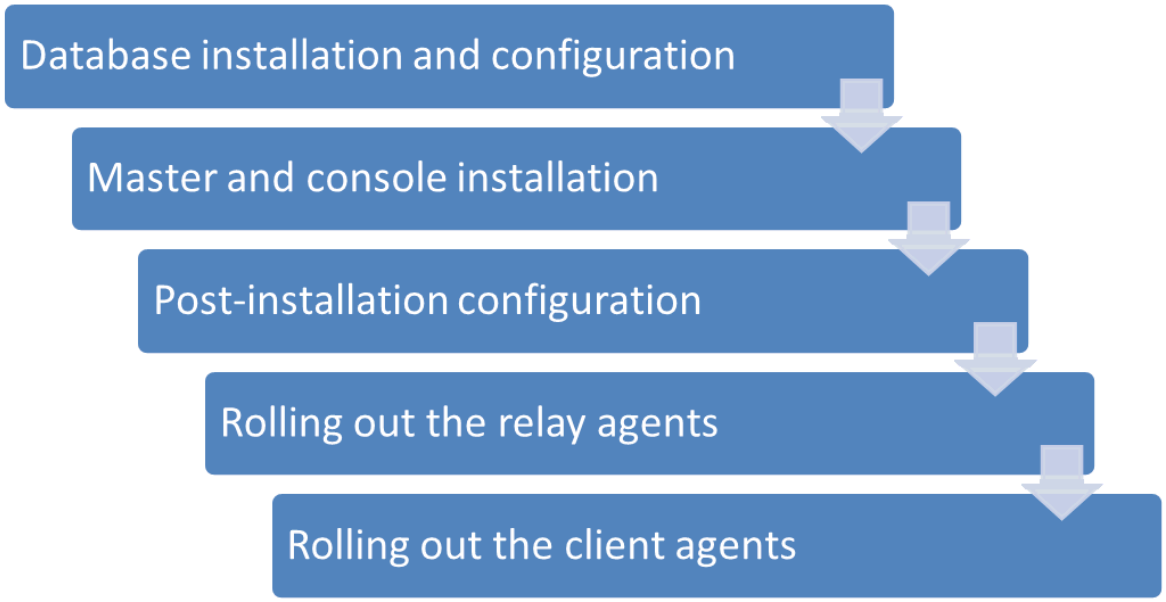
Before you start any installation task, verify that you have received your license from the BMC support team. If not, you can still install BMC Client Management with a trial license that allows you to start using BMC Client Management, but it is limited to 20 devices (including master and relays) and 30 days. When you receive your final license, you can import it and continue working and installing your remaining infrastructure devices.

Installation process overview

If you have Client Management 10.x or later installed, see Upgrading for the upgrade procedure.

Step	Action	Comments
1	Plan your environment	Before you start on any installation tasks, you should create a schema of your network and design its components.
2	Review the system requirements (hardware and software) for Client Management	The compatibility information is subject to change. For the latest, most complete information about what is officially supported, see Planning .
3	Download the installation files	See Downloading the installation files .
4	*(Optional)* Install, tune and configure the database	If you are also the database administrator, you need to ensure that a database engine is available for use and that all configuration prerequisites are fulfilled. For more information, see Database best practices.
5	Verify installation prerequisites	Verify that all prerequisites for the master are fulfilled; see Prerequisites for onsite installation.
6	Install the master and console	See the information that is appropriate for your installation: • Installing onsite on Windows and installation options • Installing onsite on Linux and installation options
7	Perform specific configurations	After the master and console are installed, specific configuration tasks are required, especially if you are installing a super master architecture. See Configuring after onsite installation.
8	Prepare for agent rollout Roll out the relay agents Roll out the client agents	Before you can roll out the agent to the relays and clients in your environment, a few preparatory tasks are required, such as importing your license and creating the target groups for the rollouts. For more information, see Rolling out agents.

The installation procedure consists of the following steps:



Prerequisites for onsite installation

This section details the prerequisites for installing the individual Client Management components:

- Database prerequisites
- Master prerequisites
- Console prerequisites on Windows
- Miscellaneous prerequisites
  - Keeping software core data and generated data separate

> **Note**
>
> Ensure that you have checked the information about the supported platforms and other technical specifications as well as the database-specific information in the System requirements section.

Database prerequisites

The BMC Client Management setup offers the possibility to install MS SQL Server Express on the master server for Windows platforms that have no database engine already installed on their network. MS SQL Server Express is installed during master server installation. If you have a version of MS SQL Server, Oracle, or PostgreSQL already installed, you must ensure that the following prerequisites are fulfilled before starting the Client Management setup process:

- MS SQL Server 2012 and 2014 with ODBC connection
- MS SQL Server 2012 and 2014 (Express Edition) with ODBC connection
- Oracle v11g or 12c
- PostgreSQL 9 and later

Master prerequisites

Java Runtime Environment (JRE) version 1.8 or later must be installed on the master device to enable you to generate template-based reports. For Windows platforms, the BMC Client Management setup automatically detects the JRE version and installs a compatible version, if necessary.

Console prerequisites on Windows

JRE version 1.8 or later must be installed on the device from which the console is run. For Windows platforms, the BMC Client Management setup automatically detects the JRE version and installs a compatible version, if necessary.

Miscellaneous prerequisites

If your company's internal standards differ from the general way of dealing with data in BMC Client Management, you can keep the software core data and generated data separate. You must consider this before the master installation to allow for the differences.

Keeping software core data and generated data separate

All data that is generated by BMC Client Management is located in a directory called **<InstallDir> /master/data** . To take this directory out of the installation directory, create an empty partition and change the path of this partition in the disk management mmc. Then select the data folder (the folder must be empty; otherwise you cannot select it).

MS SQL Server 2012 and 2014 with ODBC connection

If SQL Server 2012/2014 is already installed as a database engine, you need to execute the following tasks before installing the master:

- Ensure that the SQL Server Express and the SQL Server Browser are exempted by the firewall on the server. This is done by adding **sqlservr.exe** and **sqlbrowser.exe** as exceptions in the Windows firewall.
- You might need to completely reboot the server after making these changes; starting and stopping the SQL Server Express and SQL Server Browser software might not be sufficient.

In addition the following operations must be executed:

- Defining case sensitivity for SQL
- Creating a database on SQL Server
- Creating tablespaces for SQL Server
- Creating SQL server with ODBC (Optional)

Defining case sensitivity for SQL

SQL Server 2012/2014is case insensitive. You can make it case sensitive by modifying the **Collation Name** parameter which is located in the **Maintenance** zone of the **Database Properties** dialog box. In this list box select the regional language corresponding to your operating system (CI

= case insensitive, CS = case sensitive). To apply this value, the parameter must be set either during the installation of SQL Server or when creating the **bcmdb** database. It cannot be modified afterwards. If the database is set to case sensitive you must pay attention to the spelling when creating queries or when using the search tool in Client Management .

Creating a database on SQL Server

Creating a database for the BMC Client Management in advance is optional. You can either create it directly during the master server installation or you can manually create it in advance and then provide the required information at the installation. You can accept the default database name (**bcmdb**) or create a new name. The name is requested during the BMC Client Management master installation in the **Agent Configuration** dialog box (this applies to Windows platforms only).

Creating tablespaces for SQL Server

Creating the tablespaces for the BMC Client Management database in advance is optional. You can either create them directly during the installation of the master server or you can manually create them in advance and then provide the required information during installation. Creating the tablespaces is done through the execution of a script delivered with the Client Management installation archive in the **support/database** directory. Proceed as follows:

1. Go to the SQL Server to create a directory in which the tablespaces are to be installed (for example, **Microsoft SQL Server/MSSQL/Data/bcmdb**).
2. Open the **SQL Query Analyzer** and select the device on which the BCM database is located (for example, **local** , if it is on the local device).
3. Open the file **Support/Database/Create_TS.sqlserver.sql** of the Client Management installation archive in the **SQL Query Analyzer** window.
4. In the script, replace the placeholder **&2** with the name of the BCM database (for example, **bcmdb**), and **&1** with the path to the tablespaces subdirectory created under step 1 (for example, **Microsoft SQL Server/MSSQL/Data/bcmdb**).
5. Verify that the script works correctly by clicking **Parse Query** . If the script works, execute it by clicking **Execute Query**.

Creating SQL server with ODBC (Optional)

To create an ODBC (Open Database Connectivity) connection (System DSN), proceed as follows:

1. Open the window **ODBC Data Source Administrator** and select the **System DSN** tab.
2. Click **Add** and select the SQL Server driver from the list, then click **Next** .
3. In the window that opens enter the name for the data source (for example, **bcmdb**), select the SQL Server to which to connect and click **Next** .
4. Select the authentication type *Windows* or *SQL Server* and click **Next** .
5. Select the previously created database (for example, **bcmdb**), click **Next** and then **Finish** .
6. In the window that appears click **Test Data Source** to verify the connection.

MS SQL Server 2012 and 2014 (Express Edition) with ODBC connection

If the master and the database are on different devices, make sure that the following conditions are fulfilled; otherwise, the database does not accept any connections from the master:

- Enabling TCP/IP protocol using the Surface Area Configuration Utility
- Enabling the TCP/IP protocol in the SQL Server Configuration Utility
- Starting the SQL Server browser

Enabling TCP/IP protocol using the Surface Area Configuration Utility

1. Go to the **Surface Area Configuration Utility** window.
2. Under the section **Configure Surface Area for localhost** select the **Surface Area Configuration for Services and Connections** link.
3. In the window that now appears select the **Remote Connections** option under **SQLEXPRESS > Database Engine** in the left window pane.
4. In the table on the right window pane ensure that the **Local and remote connections** radio button is selected, as well as the **Using TCP/IP only** radio button.

Enabling the TCP/IP protocol in the SQL Server Configuration Utility

1. Open the **SQL Server Configuration Utility** window.
2. Select the **Protocols for SQLEXPRESS** option under **SQL Server Network Configuration** in the left window pane.
3. In the right window pane ensure that the entry **TCP/IP** is set to status `Enabled` .
4. Right-click the entry to open the **Properties** window.
5. In the **Protocol** tab ensure that the **Enabled** entry is set to **Yes** .
6. Select the **IP Addresses** tab.

> Here you probably see several sections, one for each network connection. Normally there would be one network card and one or more loopback connections indicated by the standard address of **127.0.0.1** . You can disregard these for SQL Server Express.

7. In the section for the network card ensure that the options **Active** and **Enabled** are both set to **Yes** .
8. If you want to enable dynamic ports for your SQL Server Express instance, the **TCP Dynamic Ports** option should be set to 0. To disable this option and use a fixed port, change this value to a blank and fill in the port number of the **TCP Port** option.

Starting the SQL Server browser

This step is optional. It is possible to set the SQL Server instance to use a fixed IP address, but this is non-standard for named instances.

1. In the **SQL Server Configuration Utility** window select the **SQL Server Service** entry in the left window pane.
2. Right-click the entry **SQL Browser** in the right window pane to open the **SQL Browser Properties** window.
3. If it is not yet started, click the **Start** button in the **Service Status** area of the **Log on** tab.
4. Select the **Service** tab.
5. If the **Start Mode** option is not set to **Automatic** , do so now.

Oracle v11g or 12c

The following Oracle versions are supported for Windows and Linux platforms:

- 11.2.0.2 with 10.2.0.4, 10.2.0.5 or 11.2.0.2 client
- 11.2.0.3
- 12c Release 1 (12.1.0.2)78u78

> **Note**
>
> Make sure your Oracle client has the same architecture as the BMC Client Management agent (x86 or x64); otherwise, the BMC Client Management agent cannot communicate with the database.

If Oracle 11g or 12c is already installed as a database engine, you need to execute the following before installing the master:

- Setting the character set to unicode
- Creating a database on Oracle v11g or 12c
- Creating tablespaces for Oracle v11g or 12c
- Removing Oracle identification on the client
- Defining language settings on Oracle v11g or 12c
- Configuring database for Linux

Setting the character set to unicode

1. In the **Database Configuration Assistant** select the **Character Set** tab when the **Initialization Parameters** window appears.
2. Select the **Use Unicode (AL32UTF8)** radio button.
3. In the **National Character Set** box select the **UTF8** value.

Creating a database on Oracle v11g or 12c

Create a database for the BMC Client Management before running the installation process. This database can be default named as **bcmdb** or freely named. The name is requested during the BMC Client Management master installation in the **Database Settings** dialog box (this applies to Windows platforms only).

Creating tablespaces for Oracle v11g or 12c

Before installing the master you must also create a user and the tablespaces for the BCM database . This is done through the execution of scripts delivered with the BMC Client Management installation archive in the **Support/Database** directory. Proceed as follows:

1. Create a new directory under the Oracle installation directory for the tablespaces, for example, **Oracle/OraData/BmcClientManagement** .
2. Copy the files **Create_User_TS.oracle.bat** and **Create_User_TS.oracle.sql** to the temp directory of the machine on which the BMC Client Management master is to be installed.
3. Open a command line window on this machine.
4. Enter the following command line followed by the ENTER button: **Create_User_TS.oracle.bat <System_Password> <Net_Service_Name> <Tablespaces_Path> <DB_User_Name> <DB_User_Password>** whereby:

System_Password	is the password to the Oracle system
Net_Service_Name	is the name of the Oracle service
Tablespaces_Path	is the path to the directory in which the tablespaces are located, for example, **Oracle/OraData/BmcClientManagement**
DB_User_Name	is the name of the Oracle account, with which you connect to the BMC Client Management database
DB_User_Password	is the corresponding password

The tablespaces are now created and you can continue with the master installation.

Removing Oracle identification on the client

The following line must be commented with a hash (#) in the following file to remove the Oracle identification on the Oracle client:

```
file: sqlnet.ora line: SQLNET:AUTHENTICATION_SERVICES=(NTS)
```

Defining language settings on Oracle v11g or 12c

The following settings are required for the NLS_LANG parameter:

- The Oracle parameter NLS_LANG (stored as either an environment variable, or in the registry at HKLM/SOFTWARE/ORACLE/HOME0/NLS_LANG) needs to be set properly. It is of the form "Language"_"Location"."Charset" and Charset needs to be set to AL32UTF8, for example, NLS_LANG=Japanese_Japan.AL32UTF8.
- If your language is not one of the Western European group, the Oracle parameter NLS_LANG (stored as either an environment variable, or in the registry at HKLM /SOFTWARE/ORACLE/HOME0/NLS_LANG) needs to be set properly. It is of the form "Language"_"Location"."Charset" and Charset needs to be set to AL32UTF8, for example, NLS_LANG=Japanese_Japan.AL32UTF8.

Configuring database for Linux

- On Linux systems, ensure that the Oracle library `libclntsh.so` exists on the master in the **oracle_home/lib** directory of the Oracle client. It is sometimes possible that this library exists under another name, such as `libcIntsh.so.9.2`. If this is the case, create a symbolic link for `libclntsh.so` pointing to `libcIntsh.so.9.2/`. Also, ensure that the directory that contains this file is referenced in the **/etc/ld.so.conf**file. Any changes to this file require `ldconfig` to be run for the changes to take effect.
- In the the `BMCClientManagementAgent` file (this file corresponds to the service of BMC Client Management agent) located in the **/etc/init.d/** directory, ensure the following entries are listed under the **# Some definitions** section in this file:

```
############### ORACLE START#########################################
PATH=$PATH:/usr/local/bmc-software/client-management/master/bin
ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/client
export ORACLE_HOME
NLS_LANG=AMERICAN_AMERICA.AL32UTF8
export NLS_LANG
SQLPATH=$ORACLE_HOME/sqlplus
export SQLPATH
PATH=$ORACLE_HOME/bin:$PATH
export PATH
TNS_ADMIN=$ORACLE_HOME/network/admin
export TNS_ADMIN
if [ $?LD_LIBRARY_PATH ]
then
LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
else
LD_LIBRARY_PATH=$ORACLE_HOME/lib
fi
export LD_LIBRARY_PATH
############### ORACLE END############################################
```

Notes

- The PATH, ORACLE_HOME and NLS_LANG entries might need to be changed to match the path where BMC Client Management is installed, the path where Oracle is installed, and the NLS_LANG defined for the Oracle database respectively.
- If BMC Client Management agent is already running, you can use the `serviceBMCClientManagementAgentstop` and `serviceBMCClientManagementAgentstart` commands to respectively stop and start the agent before making the above changes.

PostgreSQL 9 and later

If PostgreSQL is already installed as a database engine with default settings, you need to execute the following:

- Ensure that PostgreSQL was compiled with UTF8 support.
- If you are installing the master on a CentOS x64 system, make sure that the symbolic link to the **libpq.so** library exists. If not, it must be created via the following command before installing the master:

```
ln -s /usr/lib64/libpq.so.4 /usr/lib64/libpq.so
```

In addition, you need to execute the following before installing the master:

- Configuring PostgreSQL
- Connecting the master to PostgreSQL
- Creating a database on PostgreSQL
- Creating tablespaces for PostgreSQL 9 and later

Configuring PostgreSQL

- Verify that the database is configured as follows:
  1. Configure the appropriate authentication with **pg_hba.conf** in your **PGDATA** directory:

```
<?xml version="1.0" encoding="UTF-8"?>
# TYPE DATABASE USER CIDR-ADDRESS METHOD
# "local" is for UNIX domain socket connections only
local all all ident sameuser
# IPv4 local connections:
host all all 127.0.0.1/32 trust
#host all all 192.168.1.0 255.255.255.0 md5
host all all 192.168.1.0 255.255.255.0 trust (this example allows connection from an IP
included in the range from 192.168.1.1 to 192.168.1.254)
# IPv6 local connections:
host all all ::1/128 trust
```

  2. Enable TCP sockets by verifying or adding the following lines to **postgresql.conf** in your PGDATA directory:

```
<?xml version="1.0" encoding="UTF-8"?>
listen_addresses = * #this entry defines what IP addresses are listened on, it contains
either a comma separated list of addresses, localhost which is the default or * for all.
port = 5432
```

  3. Restart PostgreSQL.
  4. Verify that the file **PG_VERSION** is present in the path where the tablespaces were created.

- Verify that parameters in the **postgresql.conf** file are set as follows:

Parameter	Description
autovacuum = on	All entries that are deleted in the database are also deleted from the files on the disk.

Parameter	Description
standard_conforming_strings = off	The backslash character is interpreted as the escape character (behavior similar to version 8 and earlier).
escape_string_warning = off	The backslash character does not generate any warnings. This option is not mandatory, but it is recommended to set it to off.

Connecting the master to PostgreSQL

1. Set the full log on the master by editing the **mxtagent.ini** file and setting the **EnableTypes** parameter to **(All)**.
   The file is located in the master installation directory (by default **/usr/local/**) in the **etc** folder.
2. Start the Client Management service, `BMCClientManagementAgent` by default.

> The first time the master connects to the previously created database, it creates all tables. This initialization phase can take several minutes.

3. In the **log** directory of the master installation directory, open the **mtxagent.log** file and verify that there are no errors.

> **Note:**
>
> If the master cannot connect to the database, you should see a connection problem error entry in the log. If this is the case, take the following actions:
>
> a. Verify the connection parameter in the **Vision64database.ini** file on the master (parameters to check: **DatabaseType, DatabaseName, Host, Port, User** and **Password**).
> b. If all the parameters in the **Vision64database** seem to be correct, try to connect to PostgreSQL with the following command line:
>
> ```
> psql -U <USERNAME> -d DATABASENAME
> ```
>
> **Example**
>
> ```
> psql -U postgres -d bcmdb )
> ```

Creating a database on PostgreSQL

If you want to execute the default example installation on a SUSE Linux system, the database must use the default name **bcmdb**, and the default user name **postgres** with no password. To do so, proceed as follows:

1. Copy the **create_bcm_tables.sh** file from the **support/database/postgres** directory to the PostgreSQL server.
2. Log in as the PostgreSQL user or as **root**, and type **su postgres**.
3. Change to the directory where the database files should be created.
4. Type **sh /[script path]/ create_bcm_tables.sh** .

> This creates a directory called **bcmdb** with the required folder structure for the PostgreSQL tablespaces.
> To create the database with another name, you must first open the file used for the following procedure and modify the name from **bcmdb** to the new name.

Creating tablespaces for PostgreSQL 9 and later

By default, the BMC Client Management database tablespaces are created in the system account. It is however strongly recommended to create a specific account for BMC Client Management and create the tablespaces in this account. To do so, some further operations need to be carried out. The scripts to create the tablespaces are located in the **support/database/postgres** directory.

1. Open the **support/database/postgres/Create_TS.postgres.sql** file in any text editor.
2. Replace all occurrences of:
   - **&1** with the path to the BMC Client Management database folders, for example, if the path previously defined was **/var/lib/pgsql/data** , **&1** should be replaced with **/var/lib /pgsql/data/ bcmdb**.
   - **&2** with the **DatabaseBmcdbUser** , that is, the user name that is used to connect to the BMC Client Management database. If a user other than postgres is used, this user name must be created manually.
   - **&3** with the **[Database Name]** (only one occurrence).
3. Save the file.
4. Run this script with any PostgreSQL tool capable of running scripts, or use the **psql -U postgres -W -f /[file path]/Create_TS.postgres.sql** command line.
   The tablespaces are now created and you can continue with the master installation.

Downloading the installation files

This topic explains how to obtain the files that you need for installation from the BMC Electronic Product Distribution (EPD) site.

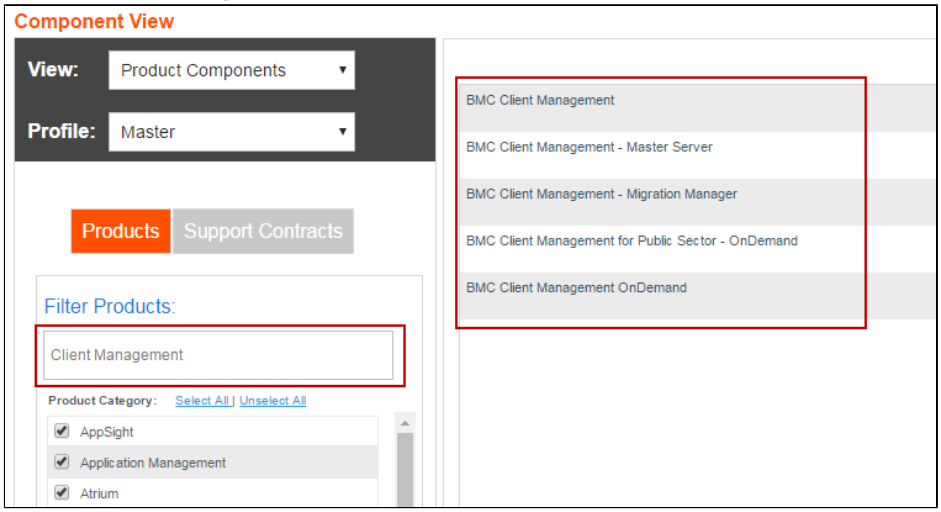
Downloading the files

The BMC Client Management installation program includes the latest service packs and patches. When new service packs and patches are released for BMC Client Management 12.5, you need to perform an upgrade of the product to apply the latest changes. You can find information about available service packs and patches under Release notes and notices.

1. Create a directory in which to place the downloaded files.

> **Note**
>
> On Microsoft Windows computers, ensure that the directory is only one level into the directory structure. The EPD package creates a directory in the temporary directory when you extract the files, and the directory that contains the installation image should not be in a directory deeper than two levels into the directory structure.

2. Go to http://www.bmc.com/available/epd.html.
3. At the logon prompt, enter your user ID and password, and click **Submit** .
4. On the **Export Compliance and Access Terms** page, provide the required information, accept the terms of the agreements, and click **Continue** .
5. If you are accessing this site for the first time, create an EPD profile to specify the languages and platforms that you want to see, per the EPD site help ; otherwise, skip to step 6.
6. Verify that the correct profile is displayed for your download. Use the **Profile** list to select a different profile.
7. From the **Component View** (the default view), in the **Filter Products** text box under **Products** , type **Client Management** and press **Enter** , or click **Go**.



8. From the filtered list on the right side, click **BMC Client Management**.
9. In the pop-up window, select the version (default selection is the latest GA version) and the platform, and click **Go** .
10. Click one of the following tabs, and select the check boxes next to the files and documents to download:
    You cannot select files across the tabs. When you click another tab, current selections are cleared.
    - **Products** - Displays the patch files available for download.

- **Patches** - Displays the product files and supplementary related files available for download, including service pack files.
- **License Information** - Displays the files related to licenses.
- **Documentation** - Displays the Online Technical Documentation links and the offline zip files of the documentation available for download.

11. Click **Download (FTP)** or **Download Manager** :
    - **Download (FTP)** - Places the selected items in an FTP directory. The credentials and FTP instructions are sent to you in an email message.
    - **Download Manager** - Enables you to download multiple files consecutively and to resume an interrupted download if the connection drops. This method requires a one-time installation of the Akamai NetSession client program on the target computer and is usually the faster and more reliable way to transfer files. A checksum operation is used to verify file integrity automatically.
12. Repeat steps 10 and 11 for each tab.
13. To go back to the product listing page to download other product files, or to log out from EPD, click the **<< Back to Product List** link that appears at the top-right of the pop-up window.

Where to go from here

Carefully review the system requirements listed in the Planning topic for your platform. You must perform these tasks before you launch the installation program.

For installation instructions, see Installing onsite or Upgrading on site .

Installing onsite on Windows and installation options

The installation of BMC Client Management is a simple, straightforward process carried out via a Windows Installer Service. While installing a master server, Windows Installer provides the possibility of installing SQL Server Express (if no database engine is preinstalled on your network), and the BMC Client Management console (these installations are described in the following steps).

This topic includes:

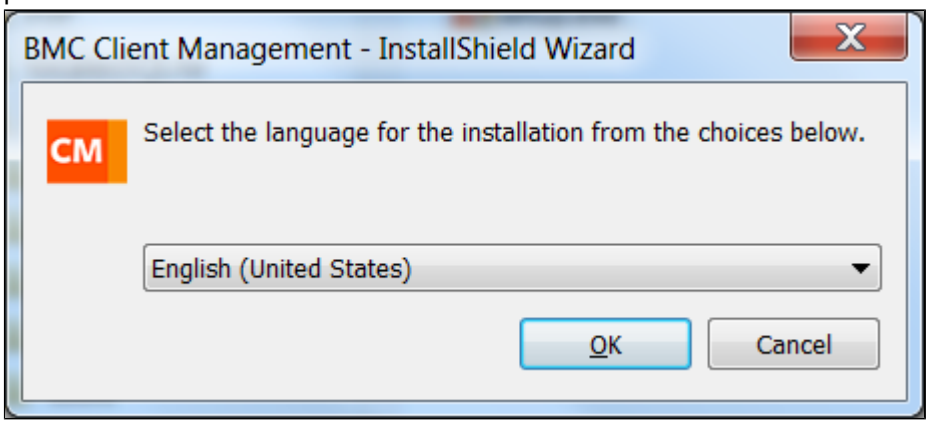
Installing master and console on Windows

The setup program takes you through the steps required to install the BMC Client Management master, including its predefined objects, on your server. The database used for this example installation is the SQL Server Express engine for which a new database and user are created with the default names and password. The tablespaces are created during the installation process as well. Links to the installation options topics are available wherever applicable.

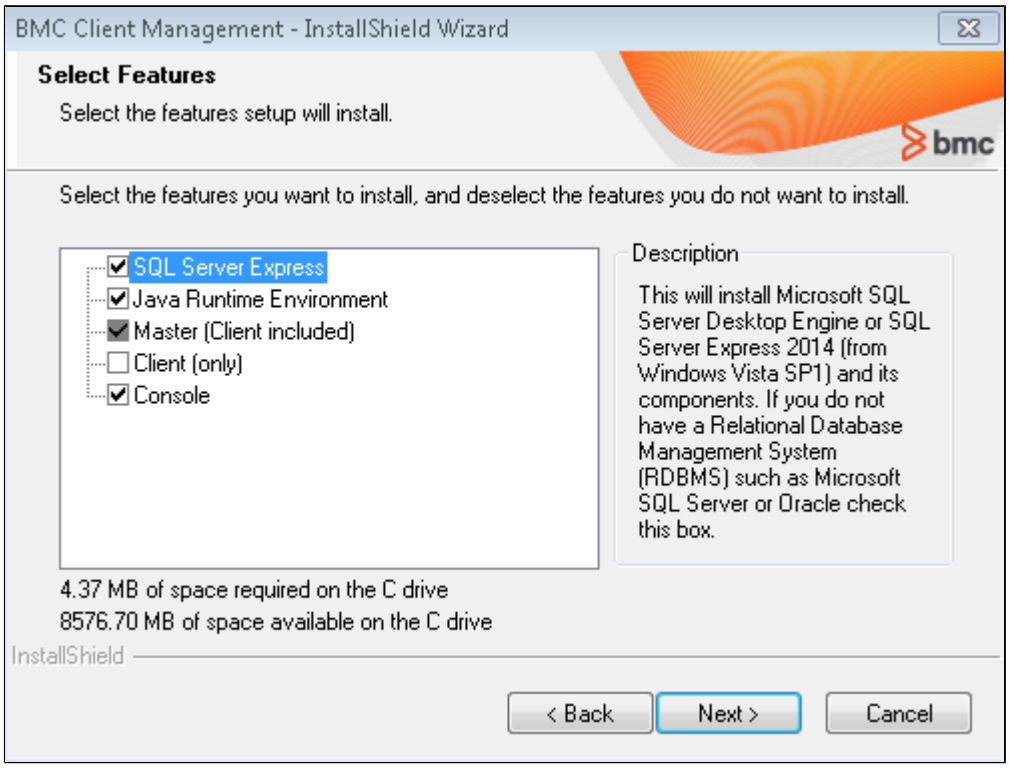
Notes

- The installation example is executed on a Windows 8 device. To install the master and database on any other supported Windows version, you can see the necessary information where applicable in the Installation options for Windows section.
- For this example of master and console installation, neither SQL Server Express nor SQL Server are installed on the master server device.
- If you intend to install the master server with an Oracle database, first see Installing the master with an Oracle database for the necessary prerequisites before starting the installation process.
- If you intend to install the master server with an SQL server database with ODBC connection or an Oracle database, you need to manually create the database and tablespaces as explained in the MS SQL Server 2012 and 2014 with ODBC connection and Oracle v11g or 12c sections before starting the installation process.

1. Decompress the downloaded archive in a temporary folder.
2. Double-click the setup.exe file.
   A **Choose Setup Language** pop-up requests you select your language for the installation procedure.



3. Select your language and click **OK** .
4. Wait a few moments while InstallShield prepares the Windows Installer installation and the configuration of BMC Client Management.
5. A **Welcome** screen appears; click **Next** .
   The **License Agreement** dialog box appears.
6. Select the radio button to accept the license and then click **Next** to continue.
   The **Select Features** dialog box appears on the screen.
7. If you execute the example installation using an SQL Server Express database, leave all preselected options as they are and click **Next**. Otherwise you need to select the components to be installed in this window.



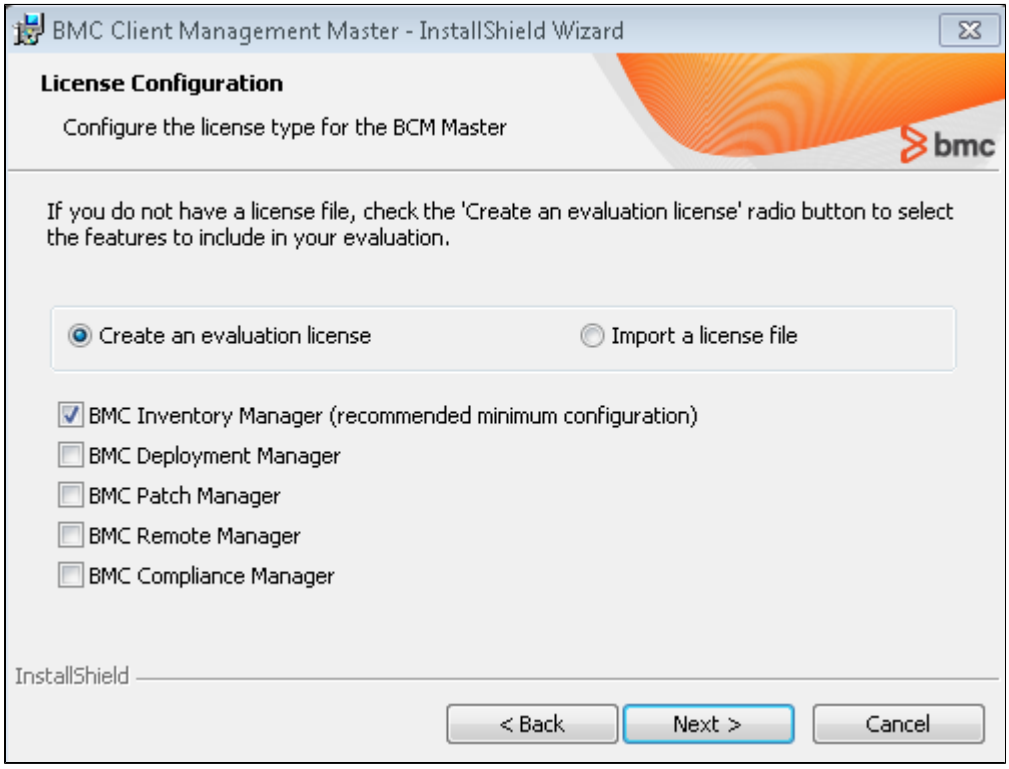
> **Note**
>
> The master requires that Java Runtime Environment (JRE) version 1.8 or later be installed on your device. If the JRE is not yet installed and you do not check the respective box in this window, you cannot generate template-based reports.

At this point, you have several different options that are explained outside this main procedure:

- If you want to use another database, clear the **SQL Server Express** box and see the respective option in the **Installation options** section of this topic when the respective information is required.
- If you want to use SQL Server with an ODBC connection, clear the **SQL Server Express** box and see SQL Server with ODBC connection now. If you want to use SQL authentication, ensure that you already created your database, user, and tablespaces, as explained in the prerequisites topic.
- If you want to install the console on a device other than the master, clear the **Console** box in this view, install the master, and then see option Installing master and console on different devices .
- If you want to install the console as a Java Web Start console, clear the **Console** box in this view, install the master, and then see Option Installing the Java Web Start console on a 3rd party HTTP server.

A **Ready to Install** window appears. It starts the actual installation process.

8. Click **Install** .
   The **Microsoft SQL Server Setup** installation box appears with a number of changing views.
9. Wait until the database installation is configured and finished.
10. If the JRE must be installed, its installation process is shown now. Click **Install** to proceed with the installation.
    The JRE installation might take a few minutes.
11. When the installation is finished, click the **Terminate** button.
12. Once the **InstallShield Wizard Initialized** dialog box appears with its **Welcome** window, click **Next** to proceed with the BMC Client Management installation.
    The **License Configuration** dialog box appears on the screen.
13. Define if you are installing an evaluation or a production license:
    a. If you purchased the software and BMC has provided you with a specific license file, click the **Select License File** radio button.
    b. Click the **Browse** button and select the path to the license file in the **Select License File** window that appears.
    c. Click **Open** to confirm the file and its path and close the window to return to the wizard.



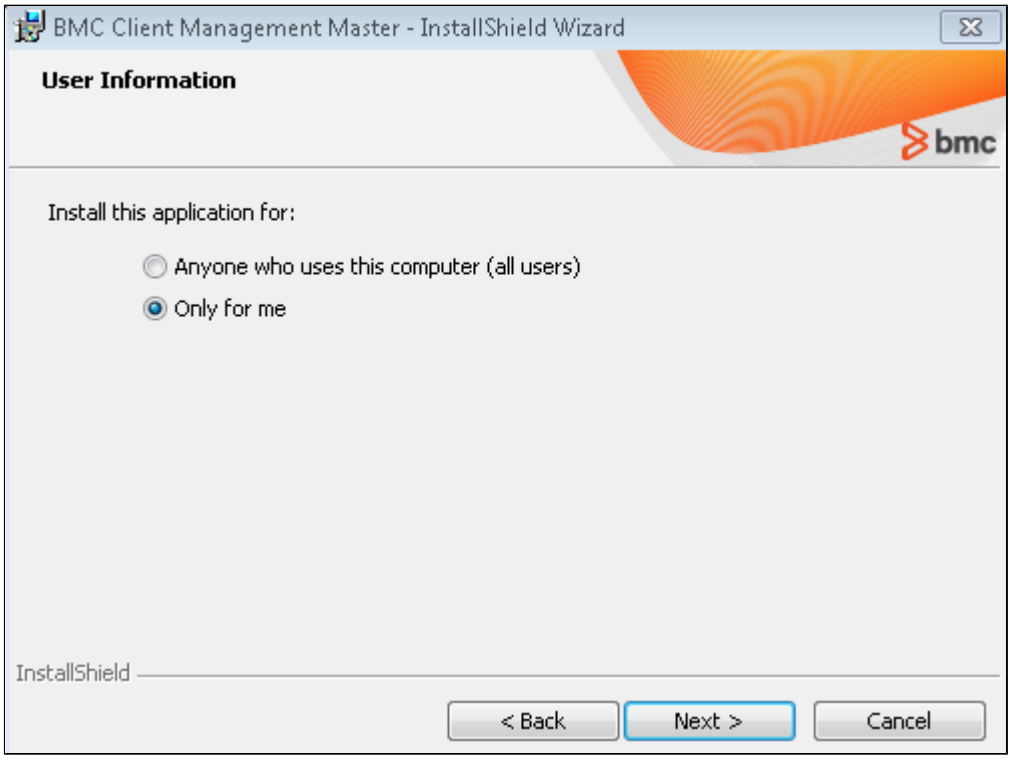
    d. Leave the **Create an Evaluation License** radio button selected to evaluate the software.
    Now all possible functionalities are displayed with a check box for each:

License	Description
BMC Client Management - Inventory	Provides access to the software, hardware, security, and custom inventory functionalities, as well as the object, application, and resource monitoring. This functionality is also the minimum configuration.

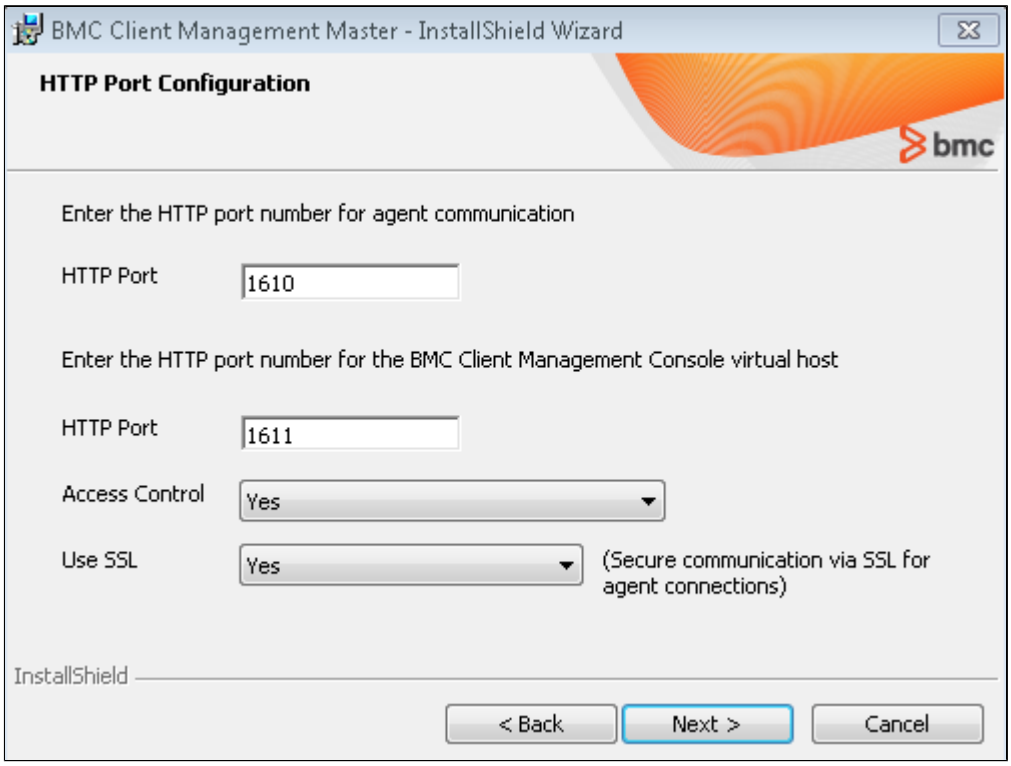
License	Description
BMC Client Management - Software Distribution	Provides access to software packaging and distribution of MSI, RPM, custom, and snapshot packages, as well as to the operating system deployment features
BMC Client Management - Patch Management	Activates the patch management functionality (patch inventories and deployment)
Remote Manager	Provides you the possibility to remotely control all BMC Client Management devices and directly access the devices
BMC Client Management - Compliance Management	Activates the device compliance feature

e. Check the boxes for the desired functionalities, then click **Next** to continue.
The **User Information** dialog box appears.

14. To define whether the BMC Client Management master is installed for all user accounts of this device or only the account that is currently logged on, select the appropriate radio button and click **Next** to continue.



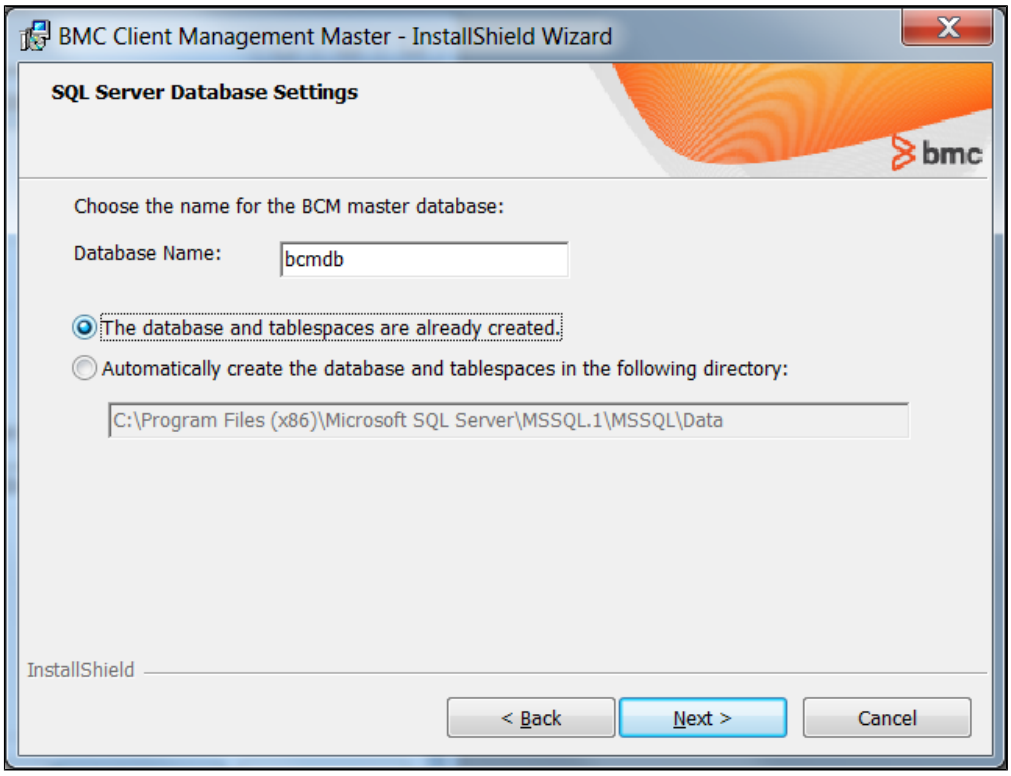
15. In the **Destination Folder** dialog box you must define the installation directory. You can either select to keep the proposed default directory or click **Browse** to change the directory or create a new directory for installation. When you are ready to continue, click **Next** .The **HTTP Port Configuration** dialog box appears. In this window the HTTP ports for the agent communication and the console connection are defined, as well as the type of secure connection.



16. For a default installation leave all preselected options as they are. You can change these values, however, you need to make note of these changes as you are required to enter them for specific operations such as when accessing the agent browser interface or upgrading to a new version.
    You now have the following options::
    - For information about the agent communication options, see option Using Access Control for interagent communication now.
    - For more information about the SSL options for all agent communication, see option Using SSL for interagent communication now.
17. Click **Next** to continue.
    The **SQL Server Database Settings** dialog box appears. It allows you to define the BMC Client Management database properties.
18. For a default installation leave all preselected options and prepopulated values as they are. In this case the database is created automatically with its default name **bcmdb** as well as the default user **bcmdbuser** with the corresponding password *Bcmuser@06* .

> **Note**
>
> You can change these values, however, you need to make note of these changes.

19. To create a user to connect to the database with a different name fill in the boxes **Login** , **Password** and **Confirm Password** with the desired values.

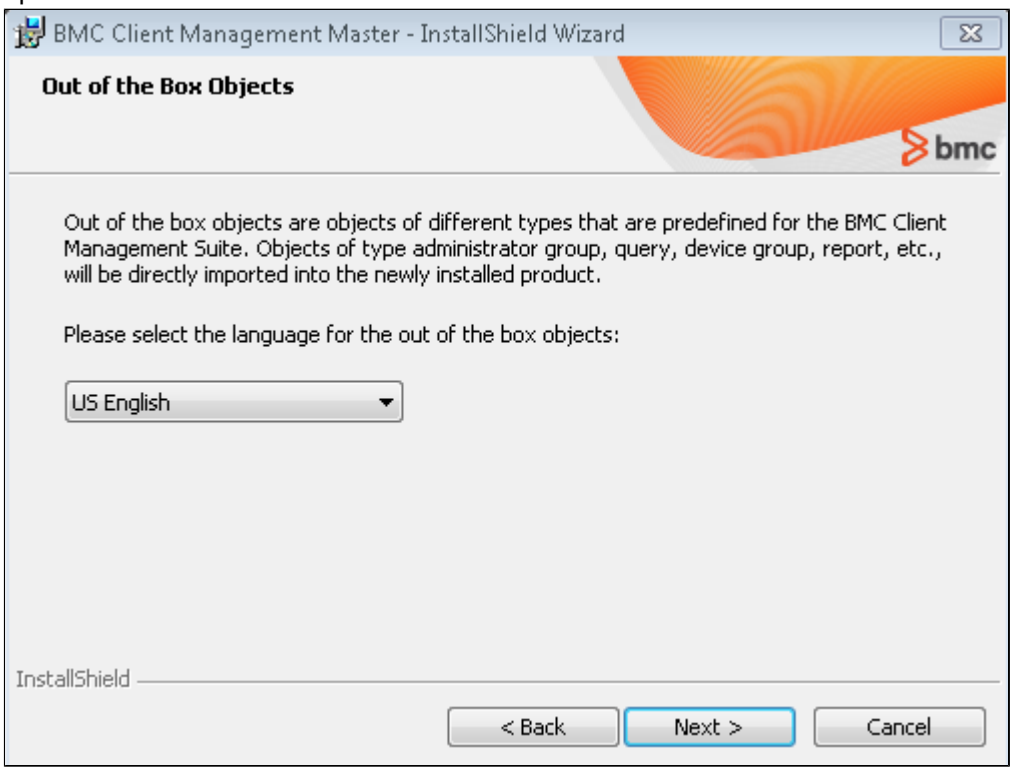


Depending on the choices you made at the beginning of the procedure regarding the database, at this point you have several different options that are explained outside this main procedure:

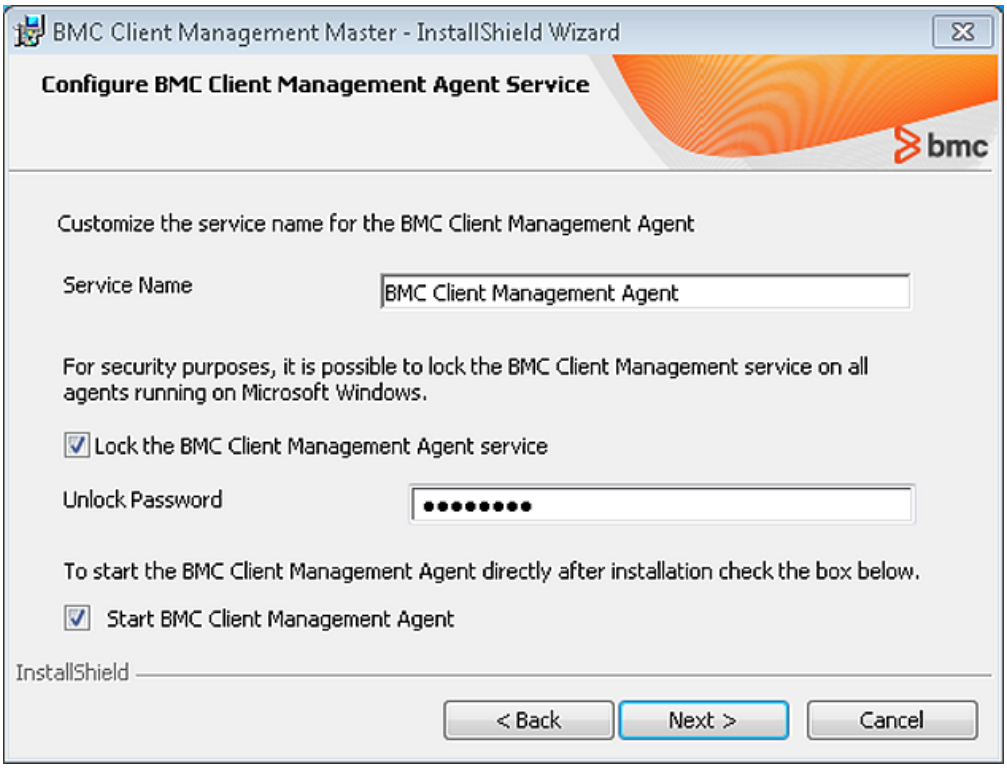
- If you selected to install **SQL Server Express** with the setup, the user part of this window is not displayed, and the default user is automatically created with the database.
- If you want to use an existing user, see option SQL server with existing user now.
- If the tablespaces are already created, select the **The database and tablespaces are already created.** radio button and enter the name of the existing database in the preceding **Database Name** box.
- For SQL Server the option **Automatically create the database and tablespaces in the following directory** is preselected and the path to the tablespaces filled in (**C:/Program Files/Microsoft SQL Server/MSSQL/Data or C:/Program Files/Microsoft SQL Server/MSSQL.1/MSSQL/Data**).

> **Note**
>
> If the boxes are not correctly selected or prepopulated, the connection with the database cannot be established. In this case stop the installation and verify that your database installation is correct.

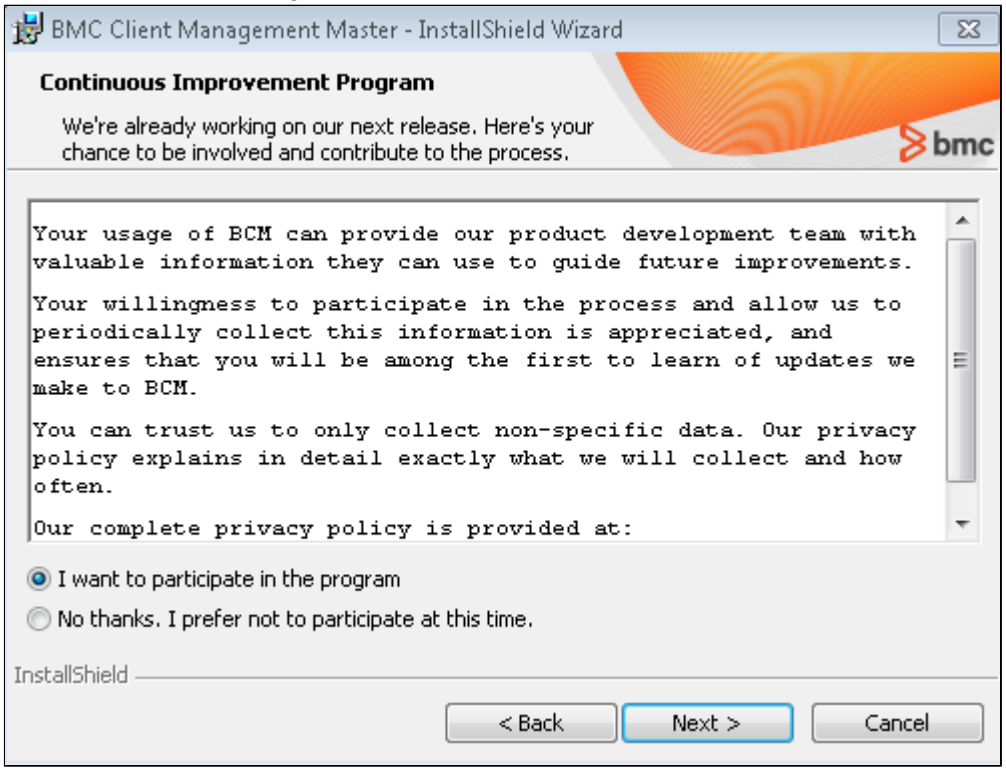
20. Click **Next** to continue.The **Out-of-the-Box Objects** window appears, displaying a list of languages available for the predefined objects that come with BMC Client Management. These are a set of objects of different types, such as administrator groups, device groups, queries, compliance rules and reports, that provide you with a basic setup for your operations in the network.



21. Select your language from the list box.
22. Click **Next** to continue.The **Configure BMC Client Management Agent Service** dialog box appears. The **Service Name** box allows you to define the name for the BMC Client Management agent service. Select the **Lock the BMC Client Management service on all agents running on Microsoft Windows** option to prevent the local users of Windows devices from stopping the agent service. If you select this option, you also need to specify **Unlock Password**. If you are installing a *Super Master Server* system, clear the box for automatically starting the agent, because some manual modifications must be executed in the configuration files for this type of architecture.



23. Leave all preselected options as they are and click **Next** .
24. In the **Continuous Improvement Program** window, select whether or not you want to participate in the amelioration of the product and let BMC know your thoughts and ideas about BMC Client Management, and then click **Next**.



25. Verify your settings in the **Ready to Install** window and then select **Install** to launch the actual installation process.
    When installation is complete the **InstallShield Wizard Completed** dialog box appears to inform you that the installation was successful and the link to the console was successfully created.
26. Click **Finish** to terminate the master installation.
    If the console is installed on the master device it is not installed in its own directory, but it is part of the master installation and only a link is created to the required files.
    You should now see the gray agent icon  in your systray, indicating that the master agent is initializing. When the agent is up and running the icon turns blue  . A second **InstallShield Wizard Completed** dialog box appears to terminate the overall BMC Client Management installation process.
27. Click **Finish** to exit the wizard.

Installation options for Windows

- Installing the master with an SQL server with an existing user
- Installing the master with an SQL Server database and ODBC connection
- Installing the master with an Oracle database
- Using SSL for interagent communication
- Using PAC for interagent communication
- Installing the master and console on different devices
- Manually installing relays (clients) on Windows
- Installing the console via the command line
- Installing the Java Web Start console on a 3rd party HTTP server
- Using the console download page for different types of installations

Where to go from here

The master and console are installed and you are now almost ready to log on to BMC Client Management and start rolling out your agents across your environment. The following topics will help you set up your environment so that you avoid running in problems later, and guide you through your first login and your first relay and client agent rollout:

- Configuring after onsite installation
- Rolling out agents

The installation process comprises the following steps:

1. Master and console installation.
2. Installation options.

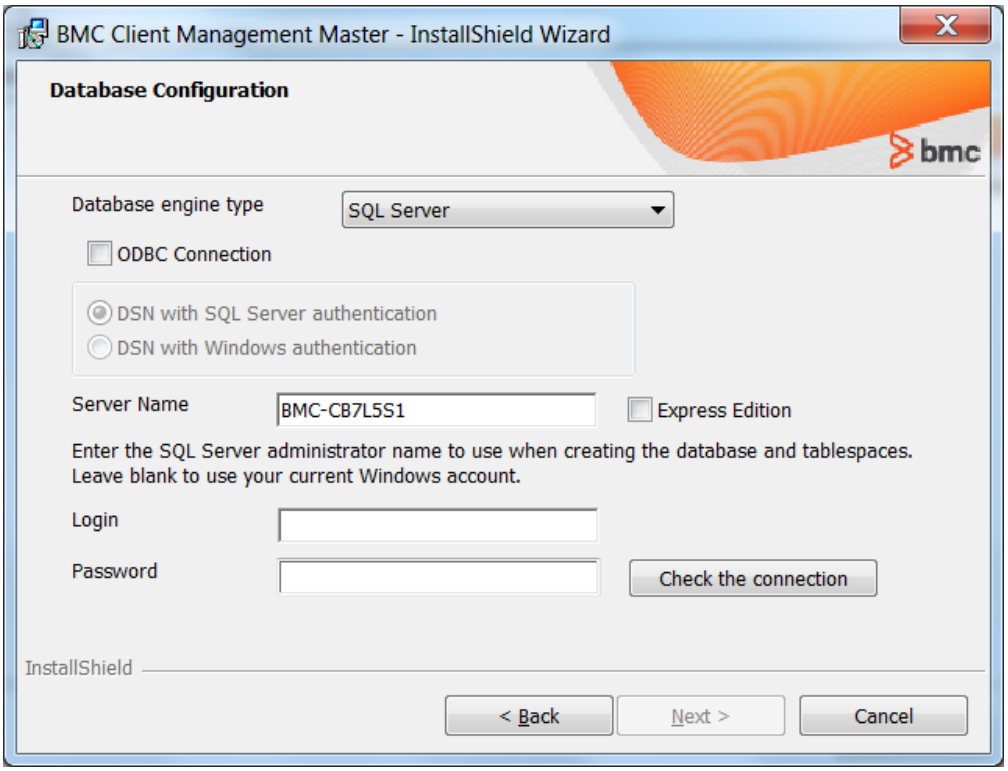
> **Note**

BMC recommends installing the BMC Client Management master and its database on a dedicated server. To avoid issues and improve performance do not install on application servers.

Installing the master with an SQL server with an existing user

To use an existing user for the connection with the database, complete the following entries. Be aware that these entries are case sensitive.

- Fill in the name of the user in the **Login** box.
- Enter the password corresponding to the login in the **Password** box.



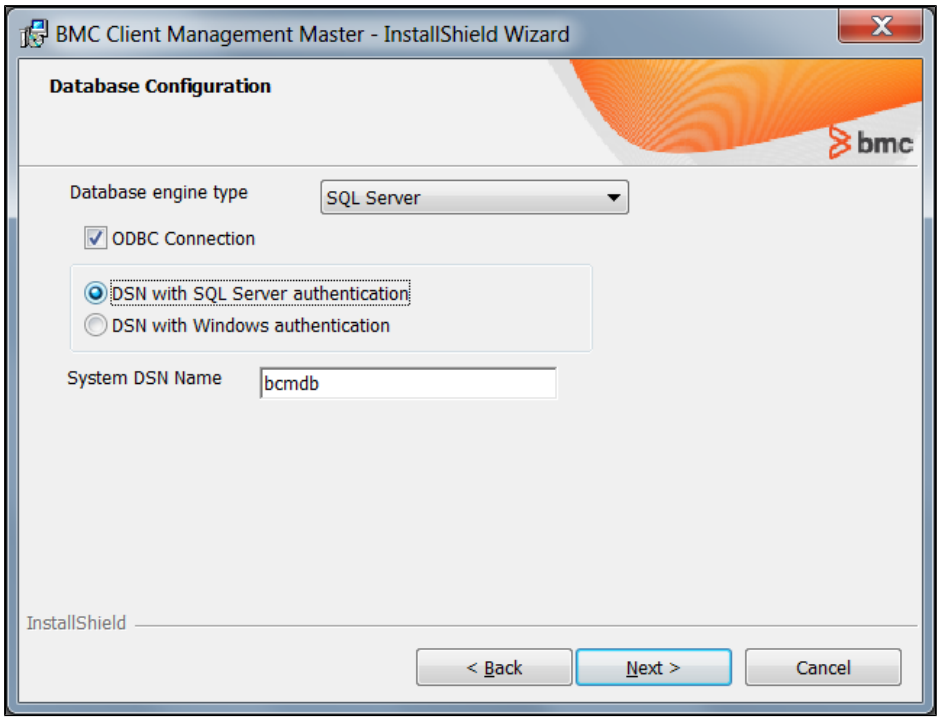
Installing the master with an SQL Server database and ODBC connection

To install the master with an SQL Server Express or SQL Server database with an ODBC connection proceed as follows:

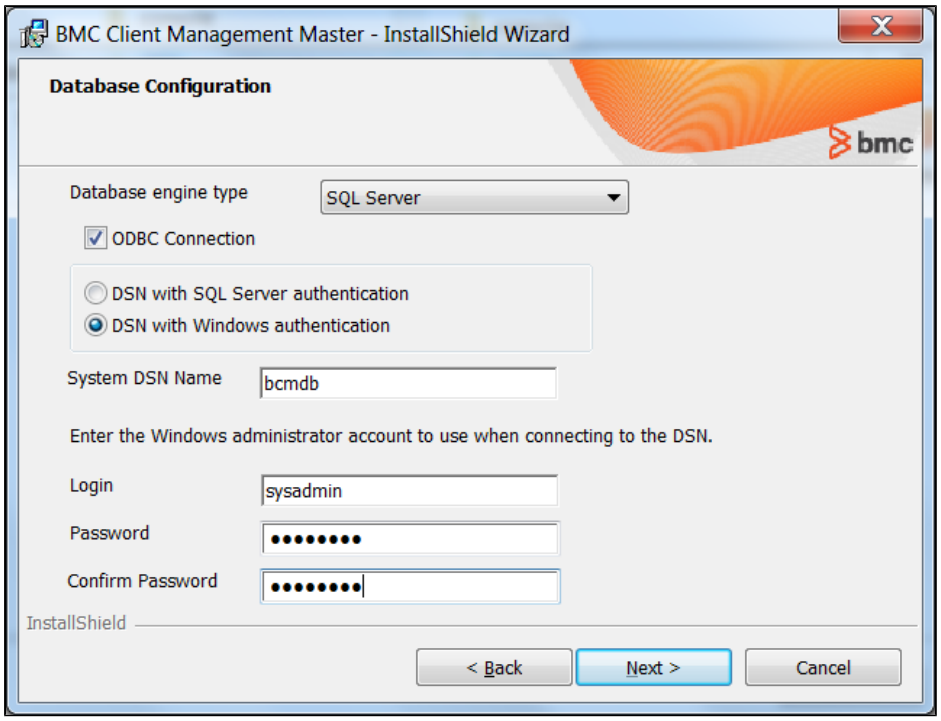
1. At step 18, **SQL Server Database Settings** check the option **ODBC Connection** .
2. Select one of the two possible authentication types:
    a. **DSN with SQL Server Authentication**:
        - To install with the default values leave all prepopulated boxes as they are.
        - To use an already created DSN name enter the name in the **System DSN Name** box.

Note

You can only use this option with a previously created database and user. For more information, see MS SQL Server 2012 and 2014 with ODBC connection.



b. **DSN with Windows Authentication**:
   - To install with the default values leave all prepopulated boxes as they are.
   - To use an already created DSN name enter the name in the following **System DSN Name**.
   - Enter the login and password of the Windows account to be used for connecting to the DSN.



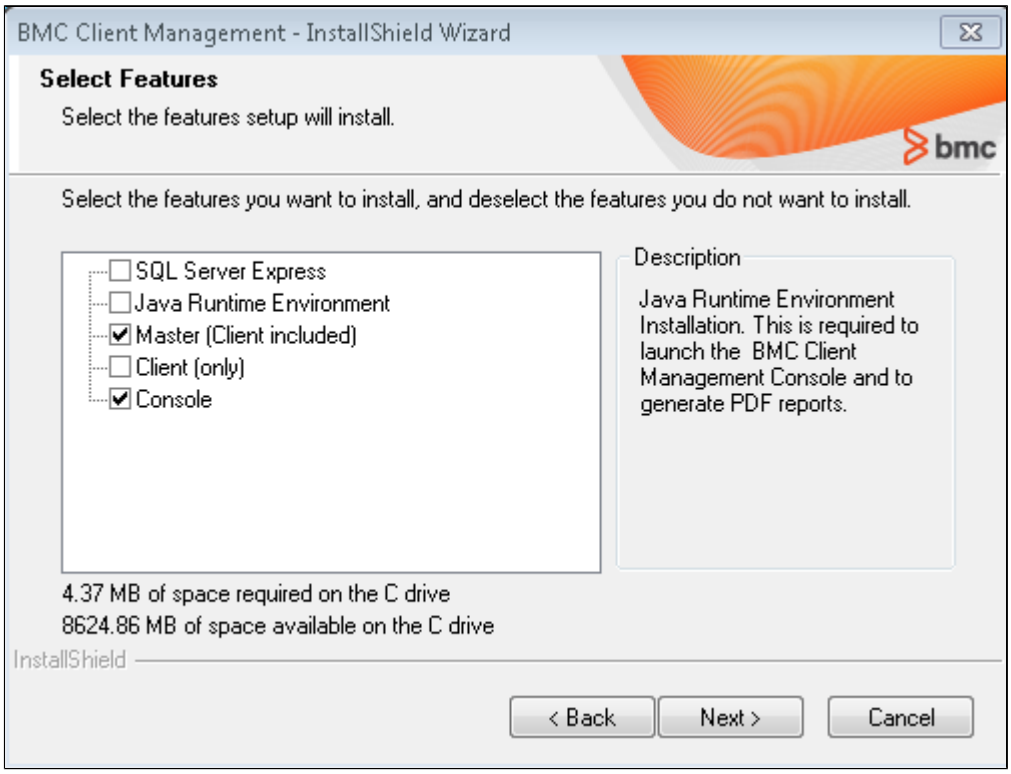
3. Click **Next** to continue with step 19 of the general procedure.

Installing the master with an Oracle database

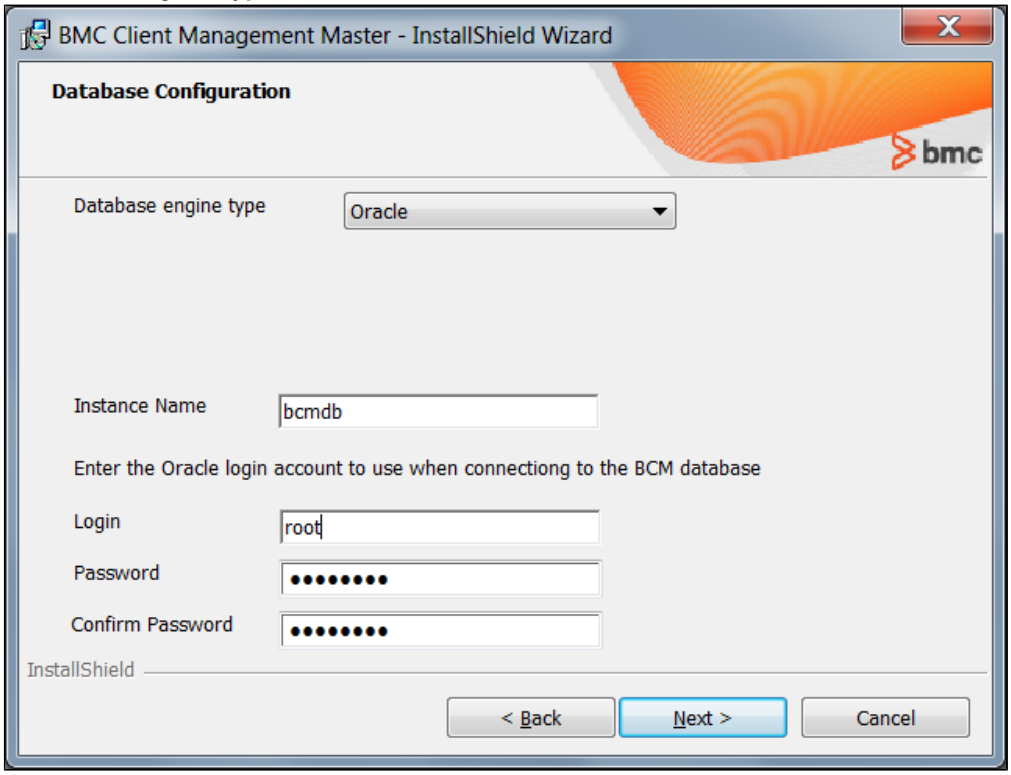
If you intend to install BMC Client Management with an Oracle database refer first to topic Oracle v10g, 11g or 12c prerequisites and execute all necessary steps.

Then proceed with the general installation process as described in the general installation procedure.

1. In step 7, clear the **SQL Server Express** option.



2. Continue with the general procedure.
3. In step 18 in the **Database Configuration** window, select the **Oracle** option from the **Database Engine Type** box.



4. Enter the name of the existing instance.

5. Enter the name and password of the Oracle account, as which you want to connect to the BMC Client Management database .
6. Click **Next** to continue with step 19 of the general procedure.

Using SSL for interagent communication

If you would like to use SSL for interagent communication you must activate this option for *all* components, that is, during the master (step 16) and relay (step 10) installations explained in this topic, for the console and for the agent rollout in the respective topics. The console provides an exception, because the SSL option cannot only be chosen during the installation process, it can also be activated or deactivated when you log on to the console. A note makes you aware of this at the appropriate paragraph in this documentation.

The following options are available for SSL communication:

Parameter	Description
No	With this option the agent accepts both securized and non-securized communication, however it sends only non-securized communications.
Receive Both, Securised Send	This value indicates that the agent accepts both securized and non-securized communication, however it sends only securized communications.
Yes	When this option is selected the agent only communicates in secure mode, that is, it only receives and sends securized communication.

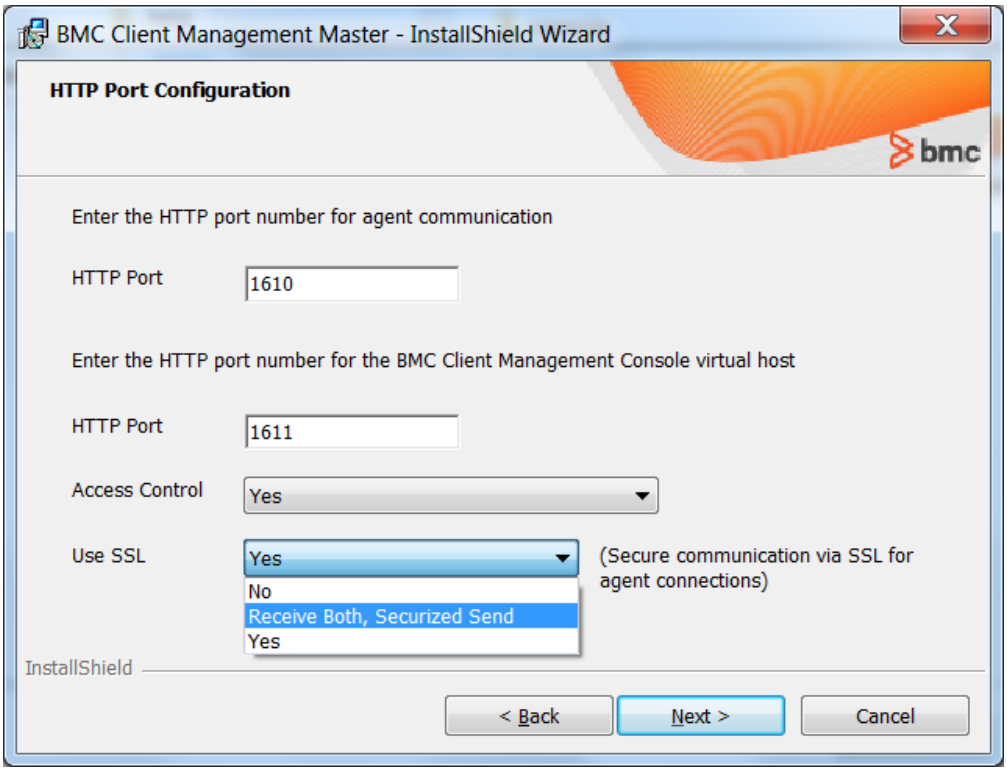
The following topics are provided:

- Installing the master agent with SSL
- Installing relay agent with SSL

Installing the master agent with SSL

To install the master agent with SSL, proceed as follows:

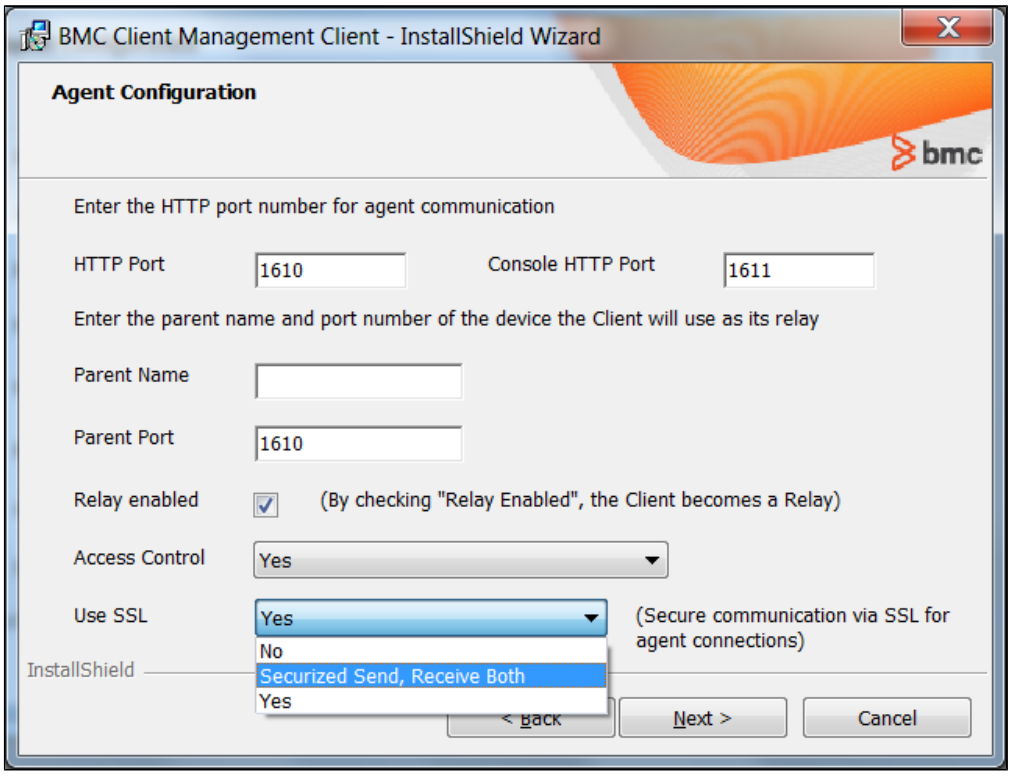
- At step 16, make the following additional selection:
  In **HTTP Port Configuration** dialog box, make your choice from the **Securized Send, Receive Both** list box. Then proceed with step 17 as defined for the rest of the procedure.



Installing relay agent with SSL

To install the relay agent with SSL, proceed as follows:

- At step 10, make the following additional selection:
  In the **Agent Configuration** dialog box, make your choice from the **Securized Send, Receive Both** box. Then proceed with step 11 as defined for the rest of the procedure.



Using PAC for interagent communication

This parameter defines security when agents communicate with each other (that is, if the **Access Control** PAC) handshake is to be used for interagent communication). Be aware that PAC communication is not possible between a current agent and a 6.0 or earlier agent. By default this parameter is set to No/0, to make sure all agents can communicate with each other when upgrading.

If you would like to use access control for agent communication you must activate this option for the master as well as *all* agents (that is, during the master step 16 and relay step 10 installations explained in the installation topic as well as for the agent rollout in the rollout topic.

The following options are available for access control:

Parameter	Description
Receive Both, No PAC Connections	As server, allow PAC connections with client authentication as well as non-PAC connections. As client, no PAC connections are required.
Receive Both, PAC Connections	As server, allow PAC connections with client authentication as well as non-PAC connections. As client, only allow PAC connections.
Yes	Only allow PAC connections (as server or client).
Yes (With server authentication)	Only allow PAC connections (as server or client) with mutual authentication.

The following topics are provided:

- Installing the master agent with access control
- Installing the relay agent with access control

Installing the master agent with access control

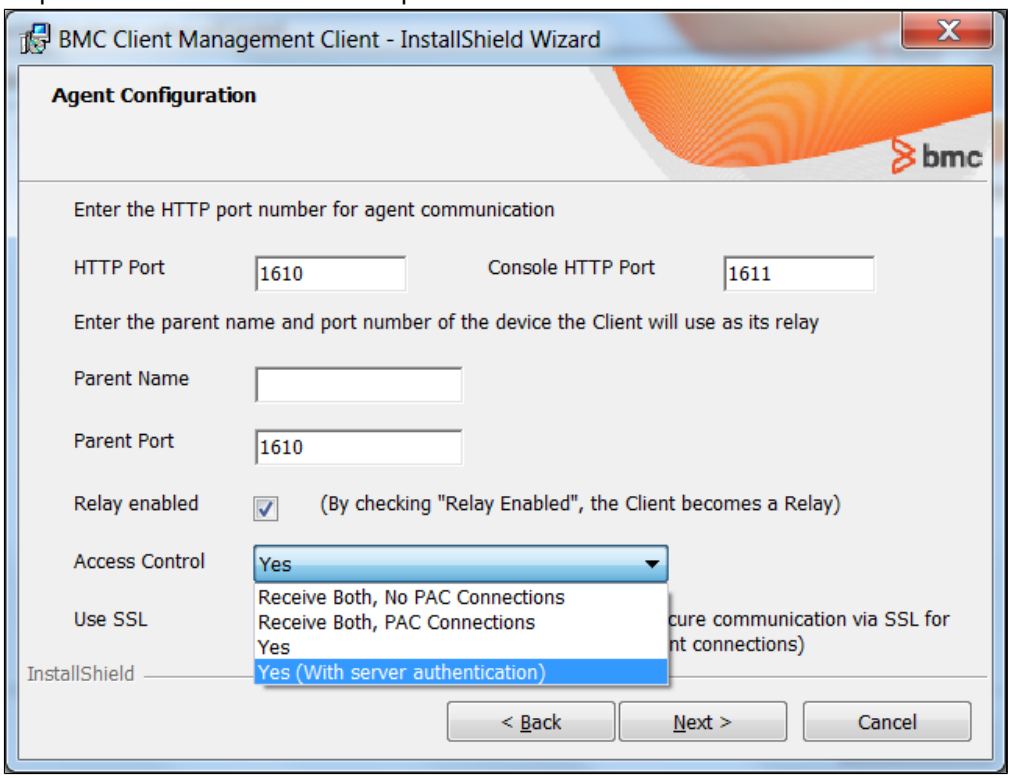
To install the master agent with access control proceed as follows:

- At step 16, make the following additional selection:
  In the **HTTP Port Configuration** window, select the desired option from the **PAC** box. Then proceed with the next step as defined for the rest of the procedure.

Installing the relay agent with access control

To install the relay agent with access control, proceed as follows:

- At step 10, make the following additional selection:
  In the **Agent Configuration** dialog, select **Yes** from the **PAC** box. Then proceed with the next step as defined for the rest of the procedure.



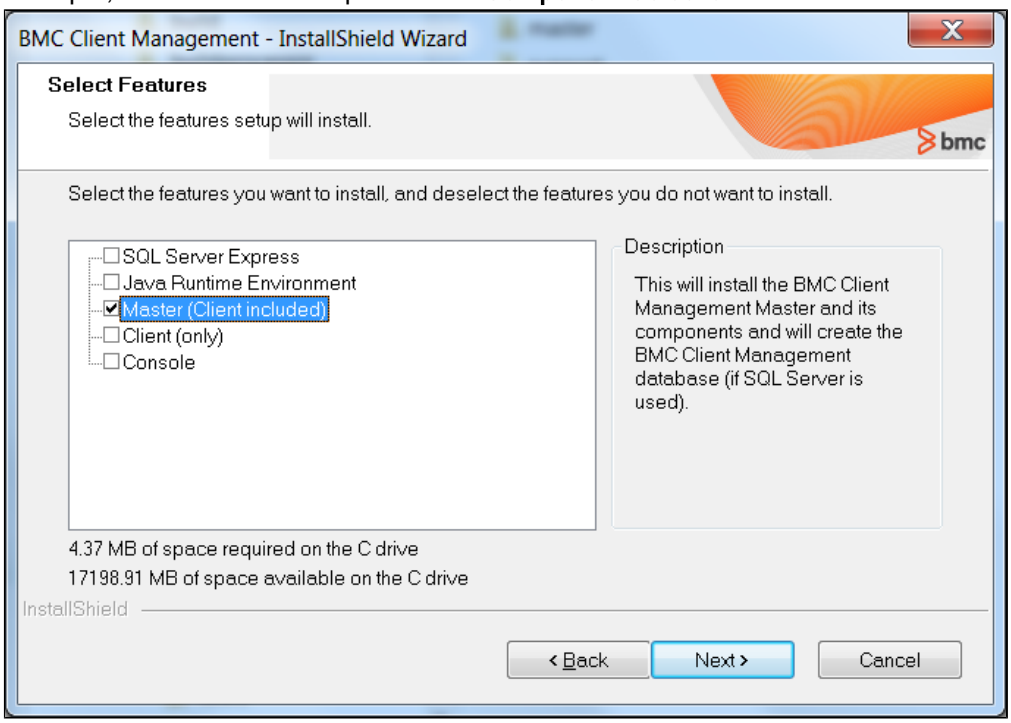
Installing the master and console on different devices

If you would like to install the console on a different device than the master, the installation process is divided in two different parts. Proceed as follows:

- Installing only the master
- Installing the console

Installing only the master

1. Launch the installation as described.
2. In step 7, clear the console option in the **Component Selection** window.



3. Proceed with the installation as described until step 23.
   After you click **Finish** , the installation process terminates and you must install the console separately.

Installing the console

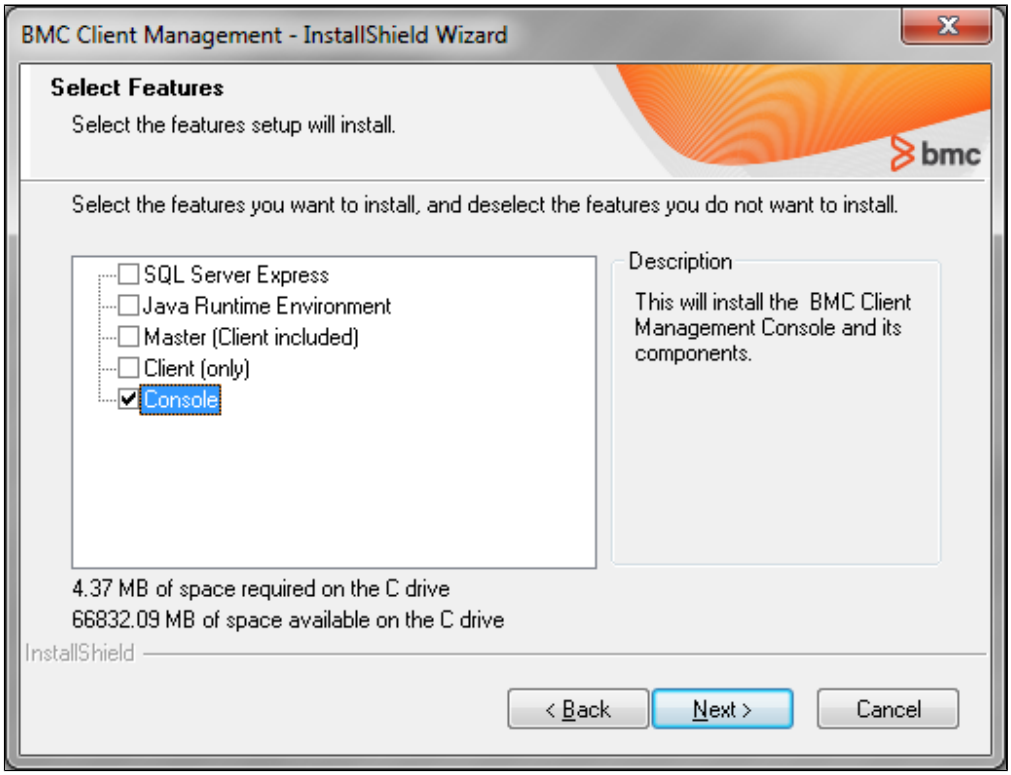
The console installation process starts in the same way as the master--you have the following options:

- Install the console as a Java Web Start console (see option Console download page for different types of installation now).
- Install the console via the command line (see option Installing the console via the command line now).
- Install the console on another device with an active HTTP Server (proceed as described in the following paragraphs).

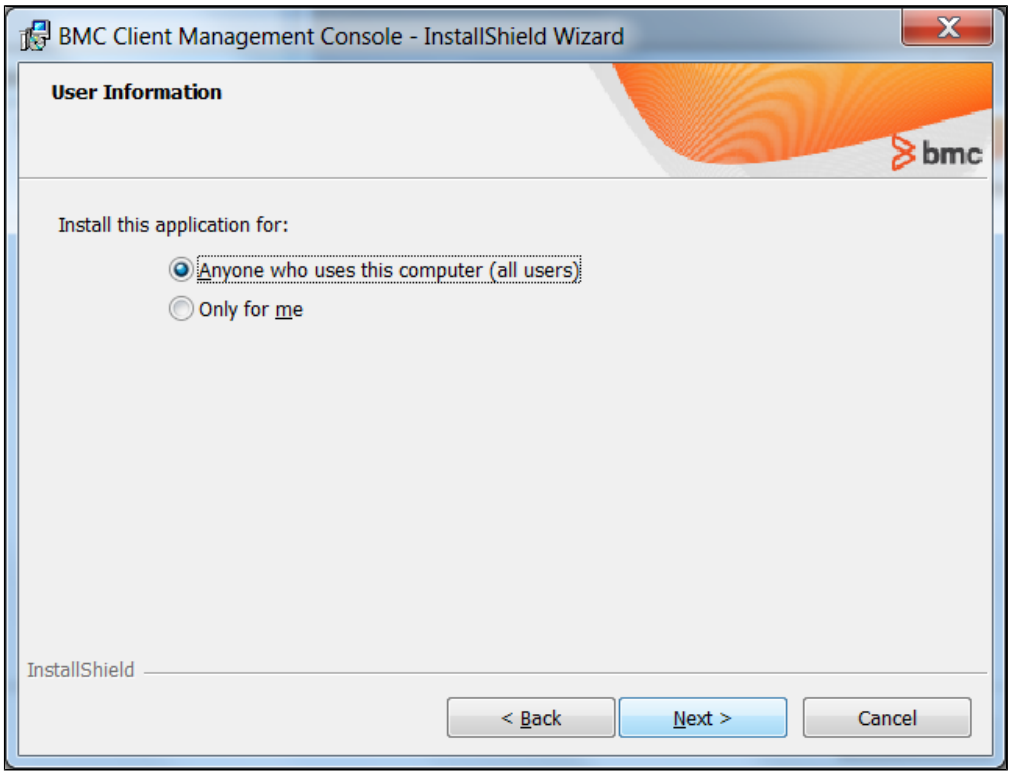
The installation of the console starts in the same way as the master installation; therefore, proceed as follows:

1. Go to the device on which the console is to be installed and proceed as described in the general installation process (steps 1 to 6).
2. At step 7, clear all options apart from *Console* in the **Component Selection** window.

3. Click **Next**.
   The **InstallShield Wizard Initialized** dialog box appears with its *Welcome* screen again to install the console.

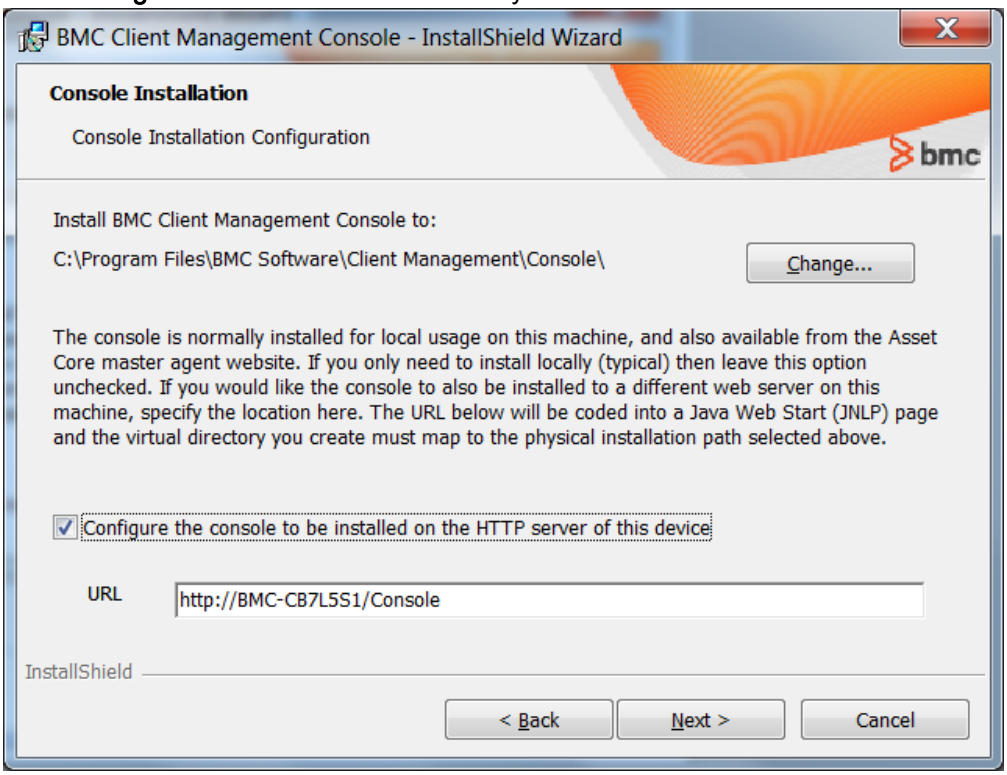


4. Click **Next** to continue.
   The **InstallShield Wizard** for the console installation dialog box appears on the screen.
5. Wait until the InstallShield Wizard is completely initialized, then click **Next** to install.
   The **User Information** dialog box allows you to define if the BMC Client Management master is installed for all user accounts of this device or only the account which is currently logged on.
6. Select the required radio button and click **Next** to continue.



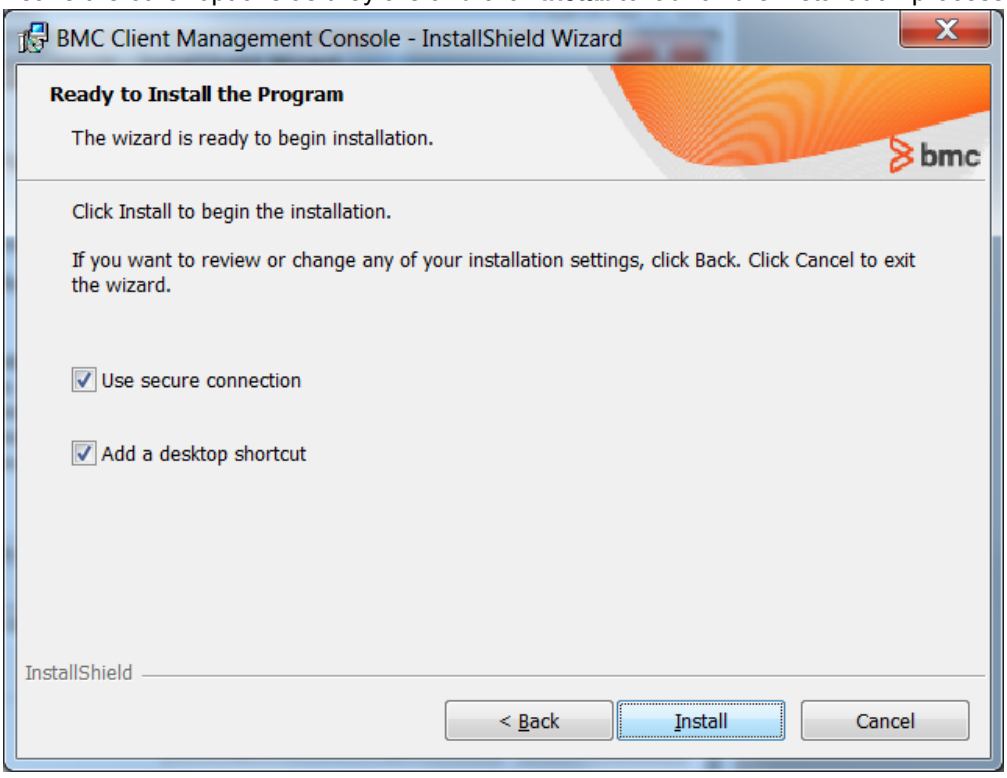
The next **Console Installation** window defines the way the console is installed. By default it is installed as an application in the indicated directory.

7. Click **Change** to install it in another directory.



At this point in the procedure you have another option that is explained outside this procedure:
To install the console with Java Web Start support on an HTTP server other than the master, see option Installing the Java Web Start console on a 3rd party HTTP server now.

8. Click **Next** to continue.
   The **Ready to Install** window appears the chosen installation directory and also allows you to create a shortcut to the console on the desktop.
9. Leave the other options as they are and click **Install** to launch the installation process.



Note

If you defined the master installation with SSL, you need to select the **Use secure connection** box here.

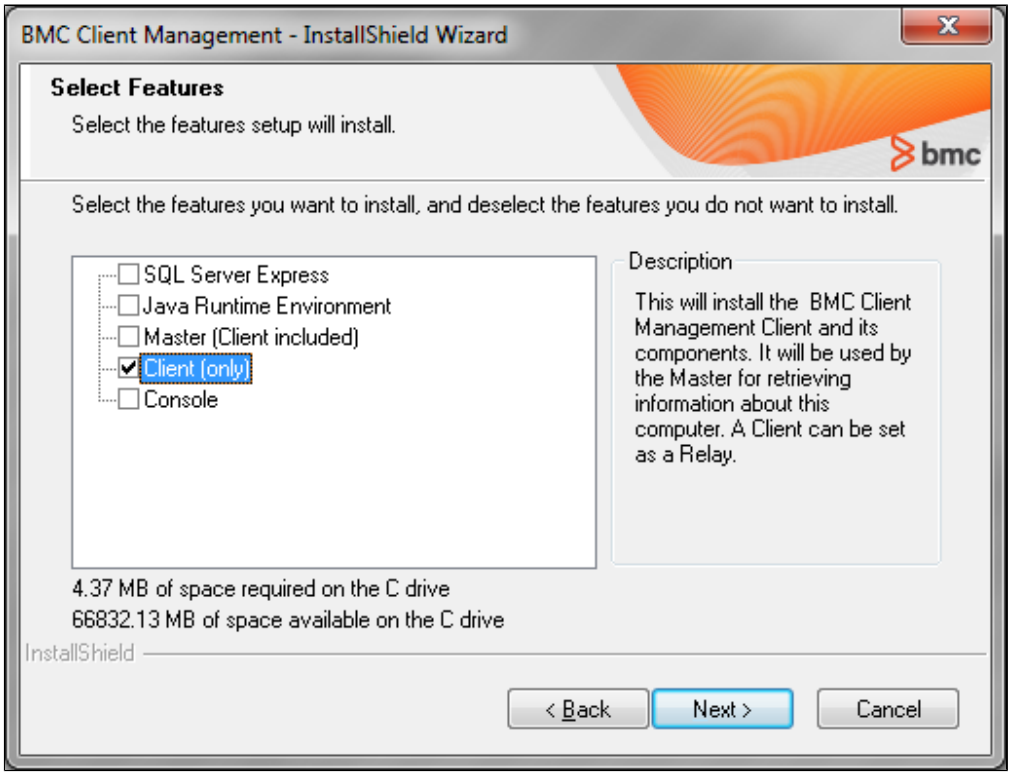
When the console installation is completed, the **InstallShield Wizard Completed** dialog box appears to inform you if the console installation was successful.

10. Click **Finish** .
    A second **InstallShield Wizard Completed** dialog box appears to terminate the overall BMC Client Management installation process.
11. Click **Finish** to exit the wizard.

Manually installing relays (clients) on Windows

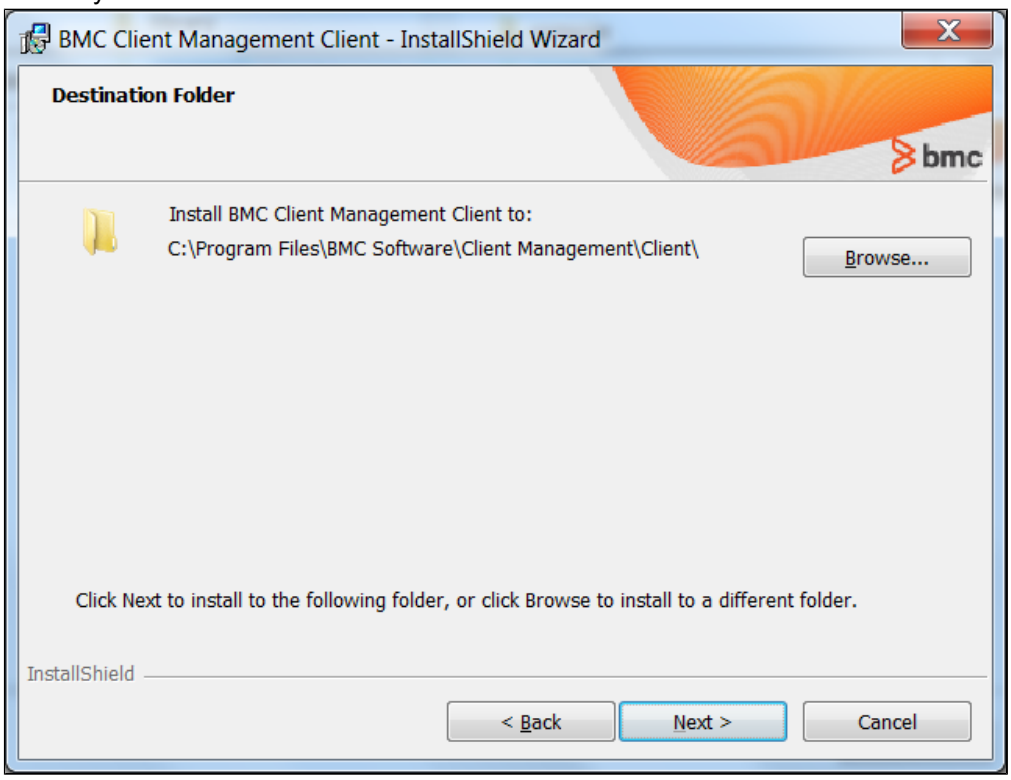
The agent is installed on each client and operates completely independently from the master server (the master has its own agent), sending information either at regularly defined intervals or when polled by the master or any other module. As we are going to roll out the agents to some clients later on, we use this installation to install a relay for our clients, because the installation program is the same for a client or relay. A relay agent is the same type of agent as that of the client and is treated as such, but it has more functionalities. Similar to the master and console installation, the installation of the BMC Client Management agent is a simple, straightforward process carried out via the Windows Installer Service. The setup program takes you through the steps and installs the agent on your selected device. To install the relay agent, follow these steps:

1. Double-click the setup.exe file.
   The **Choose Setup Language** pop-up requests you to select your language for the installation procedure.
2. Select your language, in our case most probably **English** , then click **OK** .
3. Wait a few moments while InstallShield prepares the Windows Installer and the BMC Client Management configuration.
   The **License Agreement** dialog box appears.
4. Select the radio button to accept the license and then **Next** to continue.
   The **Select Features** dialog box appears.
5. For the agent installation you must first clear all options and then check the **Client (Relay)** box.



6. Click **Next** to continue.

7. In the **Start Copying Files** dialog box that now displays, click **Next** to prepare for installation.
8. Wait until the InstallShield Wizard is completely initialized, then click **Next** to continue.
   The **Destination Folder** dialog box now proposes a default installation directory.
9. You can choose to keep the default or click **Browse** to change the directory or create a new directory for installation.



10. When you are ready to continue, click **Next** .
    The **Agent Configuration** dialog box now appears with the communication settings for relays.
11. Define the following parameters for your relay:

Parameter	Description
HTTP Port	Define the HTTP port of your local computer. The default value for this port is 1610 for Windows computers. If you left the default settings at the master installation, also leave this value.
Parent Name	The direct parent of our relay here is the master, therefore you must enter the name of the master server into this text box.
Parent Port	Enter the port number of the master. If you left the default settings at the master installation also leave this value.
Relay Enabled	Check this box to make the particular client you are about to install a relay.
Access Control	Define whether agent communication is secured via access control. Leave the preselected option.
Use SSL	Define whether agent communication is secured via SSL. Leave the preselected option and click Next.

At this point in the procedure you have different options for agent communication that are explained outside this main procedure:

- For more information about the access control options for all agent communication, see option Using Access Control for interagent communication now.
- For more information about the SSL options for agent communication, see option Using SSL for interagent communication now.

The **Service Name** dialog box appears. It allows you to define the name for the BMC Client Management agent service, the default value for the service. BMC Client Management agent is prepopulated.

12. Leave the preselected option and click **Next** .
13. Verify your settings in the **Ready to Install** window and then select **Install** to launch the actual installation process.
14. When installation is complete the **InstallShield Wizard Completed** dialog box appears to inform you if the client/relay installation was successful. Click **Finish** .
15. A second **InstallShield Wizard Completed** dialog box appears to terminate the overall BMC Client Management installation process. Click **Finish** to exit the wizard.You should now see the gray agent icon  in your systray, indicating that the relay agent is initializing. When it is running the icon turns blue  and the relay is ready for operation.

Installing the console via the command line

The BMC Client Management console may also be installed via the command line using the **console.msi** executable file which is located in the **/software/console/winnt** directory of the archive. To do this, enter the following command with the desired options:

```
msiexec /i numara-footprints-asset-core-console.msi INSTALLDIR='<ConsoleInstallationDirectory>' ALLUSERS=
2 DESKSHORTCUT=1 SSL=1
```

- The **INSTALLDIR** option defines the installation directory of the console. If the optional command is not used the default directory **C:/Program Files/BMC Software/Client Management/console** is used.
- The **ALLUSERS** option defines where the configuration information of the installed console is stored. The following values are possible:
  - **ALLUSERS="** : Determines a per-user installation using folders in the user's personal profile. For this option no administrator rights are required.
  - **ALLUSERS=1** : Specifies a per-device installation using folders in the **All Users** profile. Administrator rights are required for this option.
  - **ALLUSERS=2** : Offers two possibilities:
    - Specifies a per-device installation using folders in the **All Users** profile if the installation is launched by a user with administrator rights.
    - Determines a per-user installation using folders in the user's personal profile if the installation is launched by a user with only user rights.
- The **DESKSHORTCUT** option defines if a shortcut to the console is to be created on the desktop. By default the shortcut is created. If the value **0** is set, no shortcut is created.
- The **SSL** option defines if the communication between the console and the master agent is secured. By default this option is activated (**1**).

Installing the Java Web Start console on a 3rd party HTTP server

If the console is installed as a Java Web Start (JWS) console, the default option is to install it with a link to the master. It is, however, possible to use an HTTP server other than the master server. To install the JWS console this way the **Console Installation** process must be run on the device of the respective HTTP server. But before you can install the console you must ensure that the HTTP server fulfills the following prerequisites:

- An alias must exist for the location of the JWS console in the format **http:<IP address or server name>:<port number>/<installation directory>** (for example, http://192.168.1.1:80 /amp-jws). This alias is coded into a Java Web Start page (JNLP) and the virtual directory you create must map to the physical installation path which is defined during the console installation.
- The ***.jnlp** extension must be added to the MIME types.
- If the console should also be installable from outside of the company network, the directory containing the Java Web Start page (JNLP) must be duplicated to another directory and an alias must be created (**amp-jws-extern**) for this directory. Then the **.jnlp** file must be modified to use the public address of this server and the new alias (for example, http://175. 16.11.140:80/amp-jws-extern).

To install the JWS console, proceed as follows:

> **Note**
>
> To be able to use this option the HTTP server must be active on the device.
> To be able to connect to this server from outside the company network the JNLP files must be created with the IP address and the port number of the HTTP server's outside address (IP address and port number). When the console is then started on the device you must enter this outside address and port into the **Server:Port** box.

1. If the console is to be installed in its default directory, leave the directory path unchanged. To select another installation directory, click the **Change** button to the right and select the target directory in the **Change Current Destination Folder** pop-up window that appears.

   - This is the physical path where you install the console (corresponding to the alias), for instance **c:/Inetpub/wwwroot/amp-jws** .
   - This directory must correspond to the alias to be defined in the **URL** box.

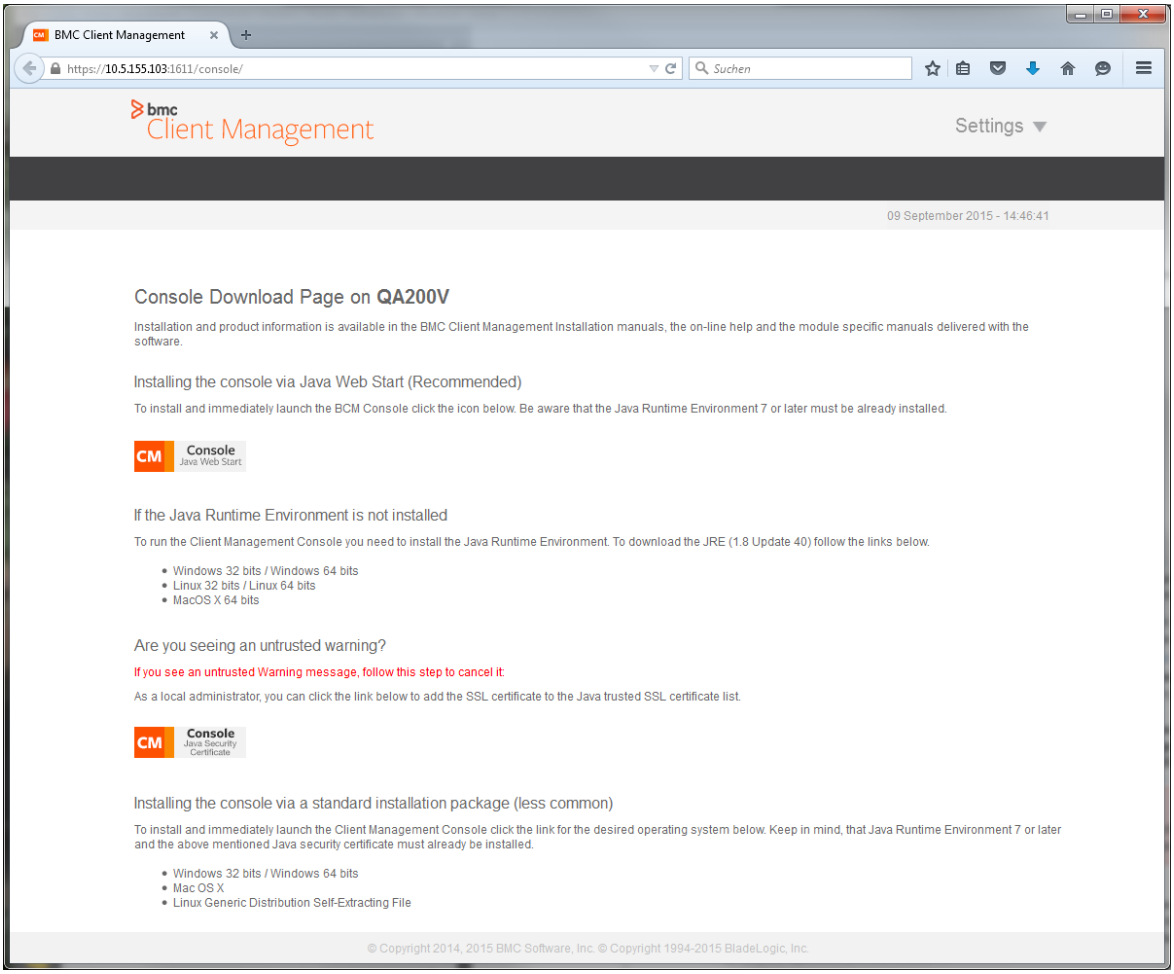
2. Select **Configure the console to be installed on the HTTP server of this device** .
   The **URL** box becomes available.
3. Enter the alias from where the JNLP is to be accessed, including the target installation directory for the console (for example, http://192.168.1.1:80/amp-jws).

> This URL is coded into a Java Web Start page (JNLP) and the virtual directory you create must map to the physical installation path selected in step 1.

4. Click **Next** and continue with step 9 of the main procedure.

Using the console download page for different types of installations

The **Console Download Page on** is only available on the master server and it provides the links to download the different types of installations available for the BMC Client Management console. This page is only accessible via a browser through the following address: **http://\[master name]:[master port]/console**. For example, http://scotty:1611/console. It cannot be accessed through the regular browser interface of the agent.



The BMC Client Management console exists for the different operating systems as well as Java Web Start. To download and install a specific console version, click the link of the desired version under the respective section.

To install the console as Java Web Start with a link to the master or another HTTP server, click the respective icon on the page. A desktop link for the console is created on the device and the remote device keeps in its cache memory the files required to launch the console. At every console launch a verification takes place, to check if a newer version of these console files is available.

> **Note:**
>
> Make sure that JRE version 1.7 is installed on the remote device and selected as default for using JWS. Do not empty or delete the Java cache memory, because this deletes the files required for the Java Web Start console. If this happens the console must be reinstalled.

The **Console Download Page on** also provides the current version of the Java Runtime Environment (JRE) that is required by the console as well as the master (on Mac OS X the JRE is preinstalled by default).

Installing onsite on Linux and installation options

The installation of BMC Client Management is a simple, straightforward process carried out via a graphical user interface or via a terminal window and command lines.

The installation process is divided into the following steps:

- Installing master and console on Linux
- Installation options for Linux
- Where to go from here

Installing master and console on Linux

> **Notes**
>
> - If the console is installed on a localized system (for example, for a French system, the "Desktop" directory might be renamed to "Bureau") the shortcut to the console cannot be created. In this case you must manually create a symbolic link to redirect the **Desktop** directory to the **Bureau** directory before installing the console via the following command: **ln -s /home/<username>/Bureau /home/<username> /Desktop**
> - After the console installation, you need to modify the execution rights to properly display the icon via the following command:
>
> ```
> chmod +x /home/<username>/Bureau/jws_app_shortcut_<xxxx>.desktop
> ```

To install the master server using the previously created default PostgreSQL database and the console, follow these steps:

1. Log on as root for the installation.
2. Unzip the downloaded archive into a temporary directory, for example, **/root/bmc**.
3. Open a console or terminal window and type the following command:

```
cd /root/bmc/software/master/linux
```

4. Type the following command line:

```
LICENSE=y SILENT=y ./bmc-client-management-master-12_5_0.sh
```

- If you install a *Super Master Server* enter the following command line:

```
LICENSE=y AGENTSTART=n SILENT=y ./bmc-client-management-master-12_5_0.sh
```

- This installation uses all the default parameters for installation. If you need to modify any of these values see Master installation options now.

5. *(Optional)* Define further options by adding the respective parameters to the command line (see available options in the installation options section).
   For any mandatory options not listed in the command line, you must answer questions displayed in the terminal window.
   File copying and installation starts. When installation is complete, a successful installation message appears.

Note

If PAM is used with Client Management , PAM must be specifically configured on the Linux server. To do so, see option Configuring PAM on the Linux server now.

6. *(Optional)* If you are using LDAP with Client Management , you must now create two symbolic links for the integration to work. To do so, open a terminal window:
   a. Go to the **/usr/lib** directory and check the version of the installed **libldap** and **liblber** files. For SUSE 10, for example, this might be **libldap-2.3.so.0** and **liblber-2.3.so.0** .
   b. Go to the **/master/bin** directory and add the following to links: **ln -s libldap [current_version} libldap.soln -s liblber[current_version] liblber.so**

```
Example
```

```
ln -s /usr/lib/libldap-2.3.so.0 libldap.so
ln -s /usr/lib/liblber-2.3.so.0 liblber.so
```

Your master is now installed and up and running on your Linux system.

Installation options for Linux

- Configuring PAM on the Linux server
- Installing relays (clients) on Linux
- Master installation options on Linux
- Agent installation options on Linux
- Console installation options on Linux

Where to go from here

The master and console are installed and you are now almost ready to log on to Client Management and start rolling out your agents across your environment. The following topics will help you set up your environment so that you avoid running in problems later, and guide you through your first login and your first relay and client agent rollout:

- Configuring after onsite installation
- Rolling out agents

Configuring PAM on the Linux server

If Pluggable Authentication Modules (PAM) is used with the BMC Client Management agent, it must be specifically configured on the Linux server. The following steps must be executed:

1. Time synchronization
2. Hosts file verification
3. **krb5.conf** file configuration
4. SAMBA configuration
5. Winbind service
6. Nsswitch.conf
7. Authentication configuration

To execute these steps, open a terminal window and proceed as follows:

1. Synchronize the Linux server with the KDC server:
    a. Stop the **/etc/init.d/ntpd** service.
    b. Synchronize the time by entering the following command:

```
ntpdate KDC server address
```

    c. Restart the **/etc/init.d/ntpd** service.

2. Ensure that the KDC server, the AD server (this might be on the same device), and the AD domain are reachable by name. If they cannot be pinged, the name resolution must be added to the hosts file. For example:

192.168.110.3	support.sophia.metrixsystems.com	dns
192.168.110.3	hotline.support.sophia.metrixsystems.com	host
127.0.0.1	MonLinux.sophia.metrixsystems.com	localhost

3. To apply the modifications, restart the network service by typing the following command:

```
/etc/init.d/network restart
```

4. Open the **/etc/krb5.conf** file and use the following example to define the server and domain definitions for communications required for Kerberos authentication:

```
<?xml version="1.0" encoding="UTF-8"?>
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = SUPPORT.SOPHIA.METRIXSYSTEMS.COM
 dns_lookup_realm = true
 dns_lookup_kdc = true

[realms]
 SUPPORT.SOPHIA.METRIXSYSTEMS.COM = {
 kdc = support.sophia.metrixsystems.com
 default_domain = support.sophia.metrixsystems.com
 admin_server = support.sophia.metrixsystems.com
 }

[domain_realm]
 .support.sophia.metrixsystems.com = SUPPORT.SOPHIA.METRIXSYSTEMS.COM
 support.sophia.metrixsystems.com = SUPPORT.SOPHIA.METRIXSYSTEMS.COM

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 kinit = {
 forwardable = true
 }

 pam = {
 debug = false
 ticket_lifetime = 36000
 renew_lifetime = 36000
 forwardable = true
 krb4_convert = false
 }
```

5. Open the **/etc/samba/smb.conf** file and use the following example to configure Samba:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
[global]
 realm = SUPPORT.SOPHIA.METRIXSYSTEMS.COM
 password server = support.sophia.metrixsystems.com
 workgroup = SUPPORT
 server string = Samba Server
 printcap name = /etc/printcap
 load printers = yes
 cups options = raw
 log file = /var/log/samba/%m.log
 max log size = 50
 security = ADS
 socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
 dns proxy = no
 winbind separator = @
 idmap uid = 10000-100000
 idmap gid = 10000-100000
 winbind enum users = yes
 winbind enum groups = yes
 template homedir = /home/%D/%U
 template shell = /bin/bash
 client use spnego = yes
 winbind use default domain = yes
 domain master = no
 local master = no
 prefered master = no
 os level = 0

[homes]
 comment = Home Directories
 browseable = no
 writable = yes

[printers]
 comment = All Printers
 path = /var/spool/samba
 browseable = no
 guest ok = no
 writable = no
 printable = yes
```

After modifying the file the samba service must be restarted for the updated samba configuration to take effect. For this, enter the following command line: **/etc/init.d/smb restart**

6. Start or restart the `winbind` service by entering enter the following command:

```
/etc/init.d/winbind restart
```

7. Verify that the **nsswitch.conf** file contains the following information:

```
<?xml version="1.0" encoding="UTF-8"?>
passwd: compat winbind
shadow: compat winbind
group: compat winbind

hosts: files dns

bootparams: nisplus [NOTFOUND=return] files

ethers: db files
netmasks: files
```

```
networks: files winbind
protocols: db files
rpc: db files
services: db files

netgroup: files

publickey: nisplus

automount: files
aliases: files nisplus
```

8. To configure the authentication, create the file **bmc** in the directory **/etc/pam.d** with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
#%PAM-1.0
# This file is auto-generated.
# User changes are destroyed the next time authconfig is run.
auth required /lib/security/$ISA/pam_env.so
auth sufficient /lib/security/$ISA/pam_winbind.so
auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok
auth required /lib/security/$ISA/pam_deny.so

account sufficient /lib/security/$ISA/pam_winbind.so
account required /lib/security/$ISA/pam_unix.so
account sufficient /lib/security/$ISA/pam_succeed_if.so uid < 100 quiet
account required /lib/security/$ISA/pam_permit.so

password requisite /lib/security/$ISA/pam_cracklib.so retry=3
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password sufficient /lib/security/$ISA/pam_krb5.so use_authtok
password required /lib/security/$ISA/pam_deny.so

session required /lib/security/$ISA/pam_limits.so
session required /lib/security/$ISA/pam_unix.so
session optional /lib/security/$ISA/pam_mkhomedir.so skel=/etc/skel umask=027
session optional /lib/security/$ISA/pam_krb5.so
```

For more information, see https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto

Installing relays (clients) on Linux

The agent is installed on each client and operates completely independently from the master server (the master has its own agent), sending information either at regularly defined intervals or when polled by the master or any other module. A relay agent is the same type of agent as the client and is treated as such, but it has more functionalities.

The manual installation of the BMC Client Management agent is a simple, straightforward process carried out via a terminal window and command lines:

1. Log on as `root` for the installation.

2. Unzip the downloaded archive in a temporary directory. For example, **/root/bmc** .
3. Open a console or terminal window and type the following command:

```
cd /root/bmc/software/client/linux
```

4. Type the following command line:

```
LICENSE=y SILENT=y PARENTNAME=[Parent Name] HTTPPARENTPORT=[Parent Port]./bmc-client-management-client-12_1_0.sh
```

> This installation uses all the default parameters for installation. If you need to modify any of these values, see Agent installation options now.

You can define further options by adding the respective parameters to the command line (see the available options in Agent installation options). For any mandatory options not listed in the command line, you are required to answer questions displayed in the terminal window. File copying and installation starts. When installation is complete a successful installation message appears.

Master installation options on Linux

To install the master you have the following options:

Option	Description
PREVUNINSTALL	Specifies if an installed earlier version of the master is to be uninstalled before the new one is installed. If this option is set to **No** or not defined and a previous master is installed, the installation terminates.
LICENSE	Accepts or refuses the BMC license. If it is refused, the installation terminates.
SILENT	Allows you to use all the default values without disturbing the user at installation time. You can override some default values by entering them in the command line. If you do not specify the SILENT option in the command line, the installation procedure requires you to provide all parameters by answering questions.

ALLUSERS	Defines where the configuration information of the installed console is stored. The following values are possible:
	• **ALLUSERS=""** : Determines a per-user installation using folders in the user's personal profile. For this option no administrator rights are required.
	• **ALLUSERS=1** : Specifies a per-device installation using folders in the "All Users" profile. Administrator rights are required for this option.
	• **ALLUSERS=2** : Offers two possibilities:
	  ◦ Specifies a per-device installation using folders in the "All Users" profile if the installation is launched by a user with administrator rights.
	  ◦ Determines a per-user installation using folders in the user's personal profile if the installation is launched by a user with only user rights.

INSTALLDIR	Defines the installation directory of the master. If the optional command is not used, the default directory **/usr/local/bmc-software/client-management/master** is used.

Option	Description
HTTPPORT	Defines the HTTP port for the agent, which is by default 1610.
HTTPCONSOLEPORT	Defines the HTTP port for the console, which is by default 1611.
DBENGINE	Defines the type of the database; the possible values are **postgres** and **Oracle** . **Postgres** is the default value.
DBHOST	Defines the host name of the computer on which the database is installed. This computer can be identified through its short or full network name, such as **scotty** or **scotty.enterprise.com** or through its IP address in dotted notation, for example, **149.132.255.1** . The default value for this option is **localhost** .
OUTOFBOX	Defines in which language the predefined objects should be installed. Use **us** to install in American English (default), **uk** to install in British English, **de** to install in German, **fr** to install in French, **jp** to install in Japanese, **bp** to install in Brazilian Portuguese or **es** to install in Spanish.
PAC	Defines if the interagent communication is securized via access control; the following values are possible: • **Receive Both, No PAC Connections** - As server, allow PAC connections with client authentication as well as non-PAC connections. As client, no PAC connections are required. • **Receive Both, PAC Connections** - As server, allow PAC connections with client authentication as well as non-PAC connections. As client, only allow PAC connections. • **Yes** - Only allow PAC connections (as server or client). • **Yes (With server authentication)** - Only allow PAC connections (as server or client) with mutual authentication. **Note** For a first test installation, BMC recommends that you do not activate Access Control (enter 0). If you selected Access Control (1, 2 or 3) for the master installation, ensure that you also activate the corresponding access control option for the relay/client.
SSL	Defines if the interagent communications is securized via SSL; the following values are possible: • **No** - With this option the agent accepts both securized and non-securized communication, however it sends only non-securized communications. • **Receive Both, Securised Send** - This value indicates that the agent accepts both securized and non-securized communication, however it sends only securized communications. • **Yes** - When this option is selected the agent only communicates in secure mode, that is, it only receives and sends securized communication. **Note** For a test or initial installation BMC recommends that you do not use SSL (select 0 [**No**]. If you still select **Yes** (1 or 2), ensure that you also activate the SSL option for the relay and clients, and for the console when you install it.
DBUSER	Defines the user name to be used to connect to the database; the default value is **postgres** .
DBPASSWORD	Specifies the password of the user to connect to the database, which by default remains blank.
DBNAME	Defines the name of the database; the default value is **bcmdb** .

Option	Description
QUALITYMETRICS	Allows you to decide if you want to participate in the amelioration of the product and let BMC know your thoughts and ideas about Client Management . Possible values are **Yes** and **No** .
AGENTSTART	Allows you to define if the agent is started directly after the installation finished. By default the agent is started. Possible values are **Yes** and **No** .

> **Note**
>
> If you are installing a *Super Master Server* system, deactivate this option for automatically starting the agent, because some manual modifications must be executed in the configuration files for this type of architecture.

Agent installation options on Linux

To install the agent on Linux systems, you have the following options:

Option	Description
PREVUNINSTALL	Specifies if a installed earlier version of the agent is to be uninstalled before the new one is installed. If this option is set to no or not defined and a previous agent is installed the installation terminates.
LICENSE	Accepts or refuses the BMC license. If it is refused the installation terminates.
SILENT	Allows to use all the default values without disturbing the user at installation time. You can override some default values by entering them in the command line. If you do not specify the SILENT option in the command line, the install procedure requires you to provide all parameters by answering questions.

ALLUSERS	Defines where the configuration information of the installed console is stored. The following values are possible:
	• **ALLUSERS=""** : Determines a per-user installation using folders in the user's personal profile. For this option no administrator rights are required.
	• **ALLUSERS=1** : Specifies a per-device installation using folders in the "All Users" profile. Administrator rights are required for this option.
	• **ALLUSERS=2** : Offers two possibilities:
	  ◦ Specifies a per-device installation using folders in the "All Users" profile if the installation is launched by a user with administrator rights.
	  ◦ Determines a per-user installation using folders in the user's personal profile if the installation is launched by a user with only user rights.

INSTALLDIR	Defines the installation directory of the agent. If the optional command is not provided the default directory **/usr/local/bmc-software/client-management/client** is used.
RELAYENABLED	Defines if the agent to be installed acts also as a relay: **Yes** for relay and **No** for simple client.
PARENTNAME	Defines the direct parent of the client with which it communicates.
HTTPPORT	Defines the HTTP port of the agent through which it communicates; the default value is 1610.
HTTPPARENTPORT	Defines the port number of the direct parent to which the agent must connect; the default value is `1610` .
PAC	Defines if the agent communications is secured via access control, the following values are possible:

Option	Description
	• **Receive Both, No PAC Connections** - As server, allow PAC connections with client authentication as well as non-PAC connections. As client, no PAC connections are required. • **Receive Both, PAC Connections** - As server, allow PAC connections with client authentication as well as non-PAC connections. As client, only allow PAC connections. • **Yes** - Only allow PAC connections (as server or client). • **Yes (With server authentication)** - Only allow PAC connections (as server or client) with mutual authentication. **Note** If you selected Access Control (1, 2 or 3) for the master installation, ensure that you also activate the corresponding access control option for the relay/client.
SSL	Defines if the agent communications is secured via SSL, the following values are possible: • **No** - With this option the agent accepts both securized and non-securized communication, however it sends only non-securized communications. • **Receive Both, Securised Send** - This value indicates that the agent accepts both securized and non-securized communication, however it sends only securized communications. • **Yes** - When this option is selected the agent only communicates in secure mode, that is, it only receives and sends securized communication. **Note** If you selected **Yes** (1 or 2) for the master installation, ensure that you also activate the SSL option for the relay/client.
AGENTSTART	Provides you the possibility to define if the agent is started directly after the installation finished. By default the agent is started. Possible values are **Yes** and **No** .

Console installation options on Linux

To install the console on Linux, you have the following options:

Option	Description
PREVUNINSTALL	Specifies if a installed earlier version of the console is to be uninstalled before the new one is installed. If this option is set to no or not defined and a previous console is installed the installation terminates.
LICENSE	Accepts or refuses the BMC license. If it is refused the installation terminates.
SILENT	Allows to use all the default values without disturbing the user at installation time. You can override some default values by entering them in the command line. If you do not specify the SILENT option in the command line, the install procedure requires you to provide all parameters by answering questions.
INSTALLDIR	Defines the installation directory of the console. If the optional command is not used the default directory **/usr /local/bmc-software/client-management/console** is used.
SSL	By default this option is set to FALSE, deactivating secure connections with the master. Define this option with TRUE for secure communications. This setting covers both SSL agent options 1 and 2 (**Receive Both, Securised Send** and **Yes**).

Configuring after onsite installation

This section contains the following information about activities that you must perform *after* you install BMC Client Management. and before you roll out the relay and client agents in your network:

- Connecting the master to Postgres 9 and later
- Super Master installation
- Antivirus exclusions
- Far-Eastern language support

After completing these configuration, you can start rolling out relay and client agents. For more information, see Rolling out agents.

Connecting the master to Postgres 9 and later

1. Set the full log on the master by editing the **mxtagent.ini** file and setting the **EnableTypes** parameter to **(All)**.
   The file is located in the master installation directory (by default **/usr/local/**) in the **etc** folder.
2. Start the Client Management service, `BMCClientManagementAgent` by default.

> The first time the master connects to the previously created database, it creates all tables. This initialization phase can take several minutes.

3. In the **log** directory of the master installation directory, open the **mtxagent.log** file and verify that there are no errors.

> **Note:**
>
> If the master cannot connect to the database, you should see a connection problem error entry in the log. If this is the case, take the following actions:
>
> a. Verify the connection parameter in the **Vision64database.ini** file on the master (parameters to check: **DatabaseType, DatabaseName, Host, Port, User** and **Password**).
> b. If all the parameters in the **Vision64database** seem to be correct, try to connect to PostgreSQL with the following command line:
>
> ```
> psql -U <USERNAME> -d DATABASENAME
> ```
>
> **Example**
>
> ```
> psql -U postgres -d bcmdb )
> ```

Super Master installation

If you are installing a super master architecture, you must execute the installation procedure described in section Installing onsite at least twice: once for the super master on its device and once for each regular (nonsuper) master server that is installed on your different locations. When all masters including the super master are installed, you need to make the following modifications on the regular masters:

Configuring the Vision64Database.ini file

In the **Vision64Database.ini** configuration file (the BMC Client Management database configuration file), you define the parameters on which data is uploaded to the super master and its database. To do so, proceed as follows:

1. Go to the **[InstallDir]/master/config** directory and open the file **Vision64Database.ini** in a text editor.
2. Find the section **[AdministeredRelayUpload]** in the file.

> This section defines all parameters dealing with the relationship between regular master and super master. It provides the parameters, which, by default, are all set to true indicating all different types of inventory upload options are activated.

3. If one or the other type of inventory does not need to be uploaded (for example, because you have not acquired the respective license, such as for patch management), modify the value to **false** .
4. Save the modifications and close the file.

After you have made all these modifications, you can launch the BMC Client Management agent for all different master servers, starting with the super master, and you can continue with the regular installation procedure of the BMC Client Management agent for all other devices in your network.

Configuring the relay.ini file

In the **relay.ini** configuration file for each regular master (*not* the super master), you must indicate that even though the device is of type master server, it still has a parent - the super master. To do this, make the following modifications:

1. Go to the **[InstallDir]/master/config** directory and open the file **relay.ini** in a text editor.
2. Go to **ParentName** and enter the name or IP address of the super master device.
3. *(Optional)* If you did not use the standard installation parameters and assigned a different port to the super master, modify the entry **ParentPort** .
4. Save the modifications and close the file.

Antivirus exclusions

BMC recommends that you set in place some prerequisites to avoid false positive virus detections. This applies to all devices on which a BMC Client Management agent is installed, including the master device.

Exceptions should be made for the following two objects:

- The entire BMC Client Management agent folder
- BMC Client Management agent files and file types

BMC Client Management agent folder

If the agent's **.sqlite** and **.log** files are set to verbose mode, the BMC Client Management agent is very talkative. To avoid this, you must set an exclusion for the ***..\client*** folder on the clients and the ***..\master*** folder on the master.

> **Note**
>
> If the device is an OSD Manager, you must also set an exclusion for the **..\PXETFTP** folder.

BMC Client Management agent files and file types

Files to be excluded:

chilli.exe	libRemoteControl.dll	Nmap.zip
comerr64.dll et comerr32.dll	libssh.dll	patchwrapper.exe
dtengine64.dll et dtengine32.dll	Microsoft.VC80.CRT.manifest	pdh.dll
IntelvPro.dll	msvcm80.dll	pkgview.exe
InteVProRC.dll	msvcp80.dll	psapi.dll
k5sprt64.dll et k5sprt32.dll	msvcr80.dll	SafeReboot.locale
krb5_64.dll et krb5_32.dll	msvcr71.dll	sas.dll
krbcc64.dll et krbcc32.dll	mtxagent.exe	ssleay32.dll
libeay32.dll	mtxcert.exe	stConvertXML.dll
libMtx.dll	mtxproxy.exe	stPackager.dll
libMtxChilli.dll	mtxrproxy.exe	stUpdateManager.dll
libMtxDtSearch.dll	mtxset.exe	update.chl
libMtxHchl.dll	mtxsetup.exe	wshelp64.dll et wshelp32.dll
libMtxXslt.dll	mtxsfx.exe	

File types to be excluded:

- *.sqlite
- *.sqlite3
- *.table

Far-Eastern language support

The console and the tool generating the reports in Client Management are both Java applications. For font management, Java relies on its own fonts, as well as those installed on the operating system of the device. As Java up to now does not include support for Far-Eastern languages, the devices on which the console and the master are installed must be correctly configured to be able to display reports in any of these languages, such as Japanese.

Ensuring support for Far-Eastern languages on Windows

The following procedure is an example for Windows 7, It is the same for other Windows versions but the names of the windows and options might vary slightly:

1. Download the language pack for the Far-Eastern languages via **Windows Update** .
2. Open the **Start** menu and select **Control Panel** .
3. In the **Control Panel** select select **Region and Language** .
4. In the **Region and Language** window, select the **Keyboards and Languages** tab.
5. Click **Install/uninstall languages** .
6. In the **Install or uninstall display languages** window select **Install display languages** .
7. Browse to the location where you stored the language pack and select it from the list box.
8. Click **Next** and then follow the remaining steps.

If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Note

The **Display language** section of the **Region and Language** window is visible only if you have already installed a **Language Interface Pack** or if your edition of Windows supports a language pack. Language packs are available only in Windows 7 Ultimate and Windows 7 Enterprise.

Ensuring support for Far-Eastern languages on Linux

Under Linux, the fonts must be added in the Java JRE. To do so, proceed as follows:

1. Locate the Java Run Time installation directory.
2. Go to the **$JAVA_HOME/jre/lib/fonts** directory.
3. Create a subdirectory called **fallback**.

4. Copy the Asian fonts into this subdirectory.

> You can find the **sazanami-mincho.ttf** font, which is required for Japanese language support, in the BMC Client Management installation archive in the **/root /BMC/support/fonts** directory.

Uninstalling onsite BMC Client Management components

Depending on the installation method, the BMC Client Management components can be uninstalled in the following ways:

Be aware that uninstalling an agent from a device does *not* automatically remove the device from the BMC Client Management database; it must be removed manually via the console. If you do not delete the device from the database, it is still displayed in all its groups. When the timeframe for a lost device, which is defined in the system variables has elapsed, it is displayed with the connection status **Lost** and a red icon  .

Manually uninstalling the BMC Client Management components

You can manually locate and uninstall the following BMC Client Management components:

- BMC Client Management Master
- BMC Client Management Client
- BMC Client Management Console

Uninstalling from Windows devices

You can uninstall the BMC Client Management components from a Windows device from the **Add /Remove Programs** window of **Control Panel**. When the uninstallation is complete, you can see that the respective BMC Client Management component is removed from the programs list in the **Add /Remove Programs** window and the agent icon has disappeared from the system tray.

> **Note**
>
> If you installed MSDE/SQL Server Express as the database engine to be used with the BMC Client Management Master installation, the SQL Server Express is *not* uninstalled with the master. You need to remove it separately.

Uninstalling from Linux devices

You can uninstall the BMC Client Management components from a Linux device using the following commands in a terminal window:

1. Open a terminal window and type the following commands as required:

Component to be uninstalled	Command
BMC Client Management Master	`bmc-client-management-master-uninstall`
BMC Client Management Console	`bmc-client-management-console-uninstall`
BMC Client Management Client	`bmc-client-management-client-uninstall`

> **Note**
>
> You can only manually uninstall a client that was manually installed. Clients that were installed via rollout must also be uninstalled via rollout.

2. Press the **Enter** key.

> **Note**
>
> Be aware that any files which are generated during the use of BMC Client Management , such as log files, data files, and so on, are not automatically deleted during the uninstallation of the components. They must be deleted manually.

Uninstalling BMC Client Management agents via rollout

Agents that were installed via a rollout must also be uninstalled via a rollout. For more information on uninstalling the BMC Client Management agent via rollout, see Uninstalling the client agent via rollout.

Verifying the uninstallation

1. In the **Global Settings> Rollouts> (Uninstall rollout) > Servers> (Your Rollout Server)** node, select the **Targets** tab.
   All defined target devices are listed.
2. Monitor the advancement of the rollout under **Status**. The different statuses are as following:

Rollout Status	Description
Initial	Rollout is defined and preparing to execute
Successful	Rollout is successfully executed
Processing	Rollout is still executing

Rollout Status	Description
At least one device failed	Rollout failed on one or more target devices

Note

Devices that cannot be accessed directly by the rollout (for reasons such as they are in another domain or behind a firewall) must download the uninstallation package from the **Rollout Server** page of the server's agent browser interface and execute it. The link to server's agent browser interface is typically in the following format: **http://<rollout server name>:<rollout server port>/rollout**.

Applying a patch to BMC Client Management

This topic provides information on how to apply a patch (also known as hotfix in earlier versions) to BMC Client Management 12.5. This topic has two main sections:

- Before you begin
- To apply the patch

The BMC Client Management patches are cumulative, so the latest patch includes all the issues fixed in the previous patches. For example, BMC Client Management 12.0 patch 6 will include all the issues fixed in the patch 1 to patch 5. So, irrespective of the last patch you applied to your BMC Client Management environment, you can directly apply the latest patch. The patches are applied using the operational rules. For information about downloading the latest patch, see Downloading the installation files.

Before you begin

Before you apply a patch, you need to remove the contents of the previously applied patch:

- Delete OneOff operational rules folders
- Delete packages

Delete OneOff operational rules folders

You need to delete the following folders under the **Operational Rules** node from the previous patch:

- Client Management OneOff
- FootPrints Asset Core OneOff

To delete these folders:

1. Unassign any devices and device groups assigned to any operational rule under these folders.
2. Delete all the operational rules under these folders.

3. Delete the folders.

Delete packages

You also need to delete all the packages from the the previous patch under the following folders:

- Packages > FootPrints Asset Core OneOff folder
- Package Factory > (Master) > Custom Packages > OneOff

> **Note**
>
> If you are not able to view the **Packages** node, you may need to login using admin credentials.

To apply the patch

1. Browse to the **Master** directory on your master server.
   For example, for a default Windows installation is `C:\Program Files\BMC Software\Client Management\Master`.
2. Depending the master server's operating system and bitness (Microsoft Windows 64-bit, Microsoft Windows 32-bit, Linux 32-bit or Linux 64-bit), copy the appropriate zip file to any location on the master server.
   For example, **BCM_12.5.0_160329s_ONEOFF_linux64.zip** is a patch for BMC Client Management 12.5 deployed on a 64-bit Linux server.
3. Extract the content of the master zip.
4. Run the upgrade installer:

Operating system	Run command
Windows	upgrade.exe
32-bit Linux	linux-master-upgrade.sh
64-bit Linux	linux64-master-upgrade.sh

5. If you have enabled the **Automatic Agent Version Upgrade** option (under **Global Settings** > **System Variables** > **Connection Management**), your client devices are updated with this patch automatically.
   Otherwise, go to **Operational Rules** > **Client Management OneOff**, and assign the operational rules as described below:

-
  - 32 bit Linux systems with the BMC Client Management 12.x client should be assigned to the rule named "LinuxOneOff"
  - 64 bit Linux systems with the BMC Client Management 12.x client should be assigned to the rule named "Linux64OneOff"
  - Mac OS X systems with the BMC Client Management 12.x client should be assigned to the rule named "MacOSXOneOff"

- 32 bit Windows systems with the BMC Client Management 12.x client should be assigned to the rule named "Win32OneOff"
- 64 bit Windows systems with the BMC Client Management 12.x client should be assigned to the rule named "Win64OneOff"

> **Note**
>
> These upgrade operational rules are intended to be run on clients only. Do not attempt to assign these operational rules to the master server.

Upgrading

This section provides information about upgrading the BMC Client Management product on all supported platforms. The platform upgrade sections also contain instructions for performing any necessary preinstallation and post-upgrade procedures.

This topic includes:

Before you begin

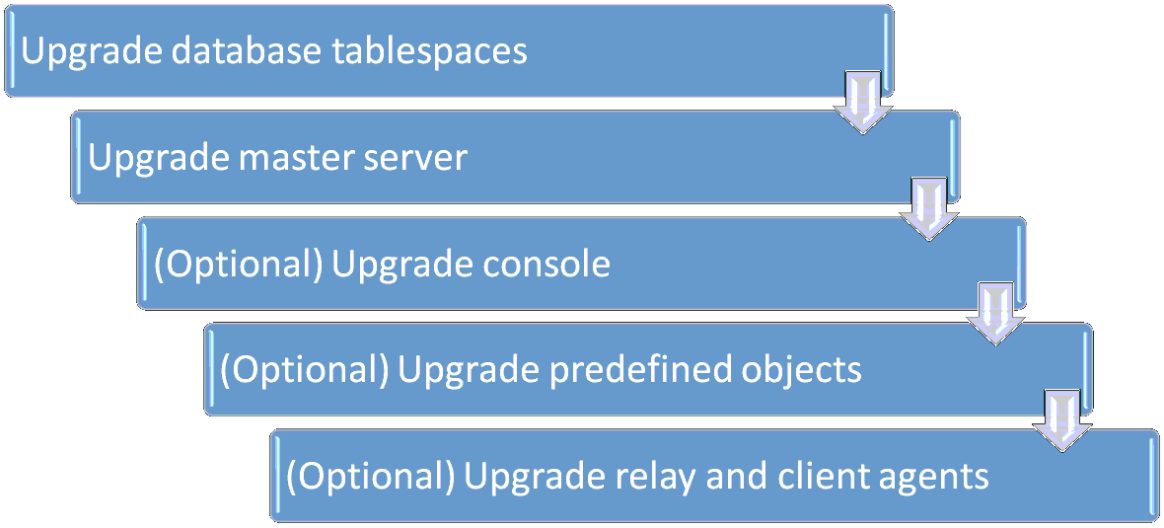
- If you are updating from BMC Client Management 12.0 or earlier using the automatic upgrade procedure for your agents and you are using the operating system deployment (OSD) functionality of BMC Client Management, you should first refer to Considerations when upgrading OSD to version 12.1 and later before you start the upgrade. The OSD functionality has undergone major changes in BMC Client Management 12.1 release that might impact your way of working, and you might consider *not* to automatically upgrade your OSD Manager devices to the new version, or execute some specific actions on these before proceeding with the upgrade.
- If you have an OnDemand installation and your system is properly set up, all BMC Client Management components should be automatically upgraded.
- Make sure you have a valid license for your upgrade to version 12.5 . Your current license continues to work for 30 days after the upgrade. You can download your new license from your support profile on our website, or by contacting Technical Support.
- If you are currently using Microsoft Internet Explorer 8 to access the agent interface, you can no longer display the graphics of these pages. You must upgrade to a newer browser. For more information, see System requirements.

Upgrading stages

The following table provides links to relevant topics in the stages of the upgrade process:

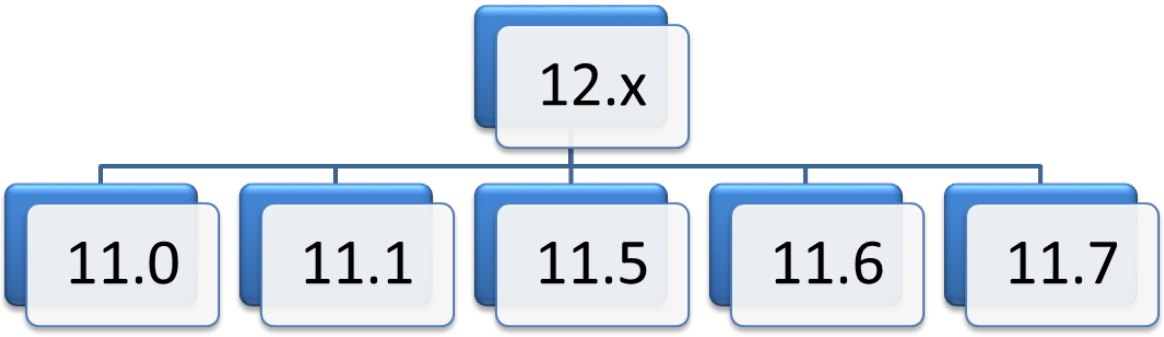
Goal	Instructions
Review the upgrade process of BMC Client Management master and database on all supported platforms	• Preparing for upgrade • Upgrading the master and database onsite • Upgrading the master and database on Windows systems • Upgrading the master and database on Linux
Review the upgrade process of the BMC Client Management Console and the predefined objects	• Upgrading the common components
Review the upgrade process of BMC Client Management agents via device groups	• Upgrading client agents individually on Windows systems • Upgrading client agents individually on Linux systems • Upgrading the agents individually on MAC systems • Upgrading client agents via device groups on Windows systems • Upgrading client agents via device groups on Linux systems • Upgrading client agents via device groups on MAC systems
Verify the upgrade process	• Verifying the upgrade

The upgrade process can be summarized as the following steps:



Supported upgrade paths

The following figure illustrates the supported upgrade paths to the various BMC Client Management versions.



If you are upgrading your agents manually, ensure that you always upgrade your master first, and then the agents. An agent cannot communicate with a master that is of an earlier version than the agent.

Upgrading the master and database onsite

This section guides you through the upgrade process of the CM master and database on all supported platforms. Before starting the actual upgrade you need to upgrade the database first.

> **Note:**
>
> If you are upgrading your agents manually, ensure that you always upgrade your master first, and then the agents. An agent cannot communicate with a master that is of an earlier version than the agent.

This topic includes:

- Preparing for upgrade
- Upgrading the master and database on Windows systems
- Upgrading the master and database on Linux

Preparing for upgrade

This topic explains how to obtain the files that you need for the upgrade of BMC Client Management from your current version to version 12.5. The following topics describe the upgrade process and provide information that you can use to prepare your environment for the upgrade:

- Files to download
- Downloading the upgrade archives

- Upgrading database

Files to download

The following table lists the upgrade archives to download according to the instructions in Downloading the upgrade archives.

Hyperlink on EPD page	Files downloaded from hyperlink
http://www.bmc.com/available/epd.html	
Documentation for BMC Client Management 12.5	BMC Online Technical Documentation portal for the BMC Client Management 12.5
BMC Client Management 12.5	A zipped installation file for each relevant platform

The product files that you download from the BMC Software Electronic Product Distribution (EPD) website might contain some or all of the patches listed on a product's Customer Support web page. If the EPD page shows that a patch is included in a file that you downloaded, you do not need to obtain that patch separately.

Downloading the upgrade archives

1. Create a directory in which to place the downloaded archives.
2. Go to http://www.bmc.com/available/epd.html.
3. At the login prompt, enter your user ID and password, and click **Submit** .
4. On the **Export Compliance and Access Terms** page, provide the required information, agree to the terms of the agreements, and click **Continue** .
5. If you are accessing this site for the first time, create an EPD profile to specify the languages and platforms that you want to see, as described in the EPD site help ; otherwise, go to step 6.
6. Verify that the correct profile is displayed for your download purpose, and select the **Licensed Products** tab.
7. In the search box under **Filter Products** , enter Client Management, and then click **Go** . The BMC Client Management link is displayed in the right pane.
8. Click the BMC Client Management link and on the BMC Client Management page, click the **Products** tab.
9. From the **Version** list, select the 12.5 version.
10. Select the platform to download.
11. Click **Download (FTP)** or **Download Manager** :
    - **Download (FTP)** - Places the selected items in an FTP directory. The credentials and FTP instructions are sent to you in an email message.
    - **Download Manager** - Enables you to download multiple files consecutively, and to resume an interrupted download, if the connection drops. This method requires a one-time installation of the Akami NetSession client program on the target computer and is usually the faster and more reliable way to transfer files. A checksum operation is used to verify file integrity automatically.

Upgrading database

The new version of BMC Client Management requires new tablespaces. Depending on your database, upgrade the corresponding tablespaces using one of the following methods:

- Upgrading the Oracle tablespaces
- Upgrading the PostgreSQL tablespaces
- Upgrading the SQL Server tablespaces

Upgrading the Oracle tablespaces

> If your master server is on version 12.0 or later, the installer automatically runs the script to upgrade the database.
>
> If you master server is on version 11.7 or earlier, follow the steps in this topic.

If you are upgrading from version 11.7 or earlier to the current version, you first need to upgrade your database by executing the **support/database/oracle/dbtablespaces_1170_1200.oracle.sql** script of the downloaded archive. Proceed as follows:

1. Copy the file **support/database/oracle/dbtablespaces_1170_1200.oracle.sql** to the temp directory of the machine on which the BMC Client Management database is installed.
2. Open the script in a text editor and replace the placeholder **&1** with the path to the tablespaces subdirectory (for example, **Oracle/OraData/BmcClientManagement**), **&2** with the name of the name of the Oracle account with which you connect to the BMC Client Management database, and **&3** with the corresponding password.
3. Launch the database tool of your choice and log on with the following parameters:

System_Password	The password to the Oracle system.
Net_Service_Name	The name of the Oracle service.

4. Launch the **support/database/oracle/dbtablespaces_1170_1200.oracle.sql** script.

The tablespaces are now upgraded and you can continue with the master server upgrade.

Upgrading the PostgreSQL tablespaces

> If your master server is on version 12.0 or later, the installer automatically runs the script to upgrade the database.
>
> Ifyoumaster server isonversion 11.7 or earlier, follow the steps in this topic.

If you are upgrading your master from version 11.7 or earlier to the current version, you first need to upgrade your database by executing the **support/database/postgres/dbtablespaces_1170_1200.postgres.sql** script of the downloaded archive. Proceed as follows:

1. Copy the file **support/database/postgres/dbtablespaces_1170_1200.postgres.sql** to the temp directory of the machine on which the BMC Client Management database is installed.
2. Open the script in an editor.
3. Replace the placeholder **&1** with the path to the tablespaces subdirectory (for example, **/usr/pgsql-9.2/data/facdb**) and **&2** with the name of the BMC Client Management database user.
4. Launch the database tool of your choice, log on as the BMC Client Management database user or administrator.
5. Launch the **support/database/postgres/dbtablespaces_1170_1200.postgres.sql** script.

The tablespaces are now upgraded and you can continue with the master server upgrade.

Upgrading the SQL Server tablespaces

> f your master server is on version 12.0 or later, the installer automatically runs the script to upgrade the database.
>
> If you master server is on version 11.7 or earlier, follow the steps in this topic.

If you are upgrading your master from version 11.7 or earlier to the current version, you need to upgrade your database by executing the following script: **support\database\sqlserver\dbtablespaces_1170_1200.sqlserver.sql** of the downloaded archive. Proceed as follows:

1. Open the **SQL Query Analyzer** and select the device on which the BMC Client Management database is located (for example, **local** , if it is on the local device).
2. Open the file **support/database/sqlserver/dbtablespaces_1170_1200.sqlserver.sql** of the downloaded archive in the **SQL Query Analyzer** window.
3. In the script replace the placeholder **&2** with the name of the BMC Client Management database (for example, **bcmdb**), and **&1** with the path to the tablespaces subdirectory (for example, **Microsoft SQL Server/MSSQL/Data/ bcmdb**).
4. Verify that the script works correctly by clicking **Parse Query** . If this is the case execute the script by clicking **Execute Query** .

The new tablespaces are now created and you can continue with the master server upgrade.

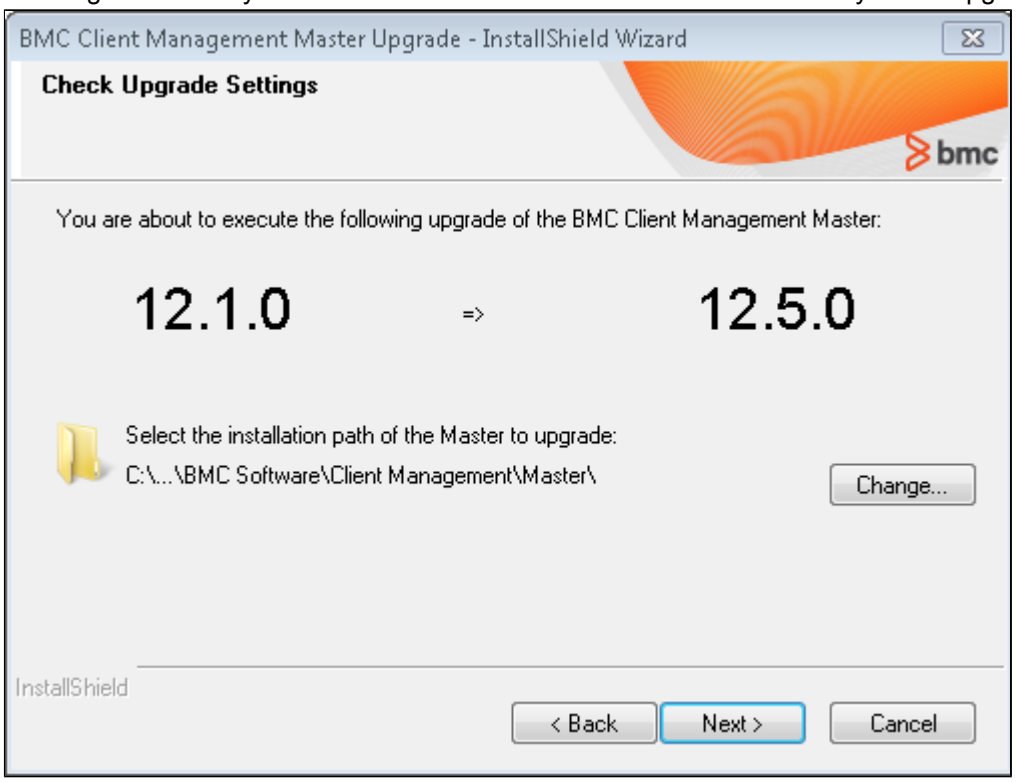
Upgrading the master and database on Windows systems

A setup program takes you through the steps for the master and database upgrade.

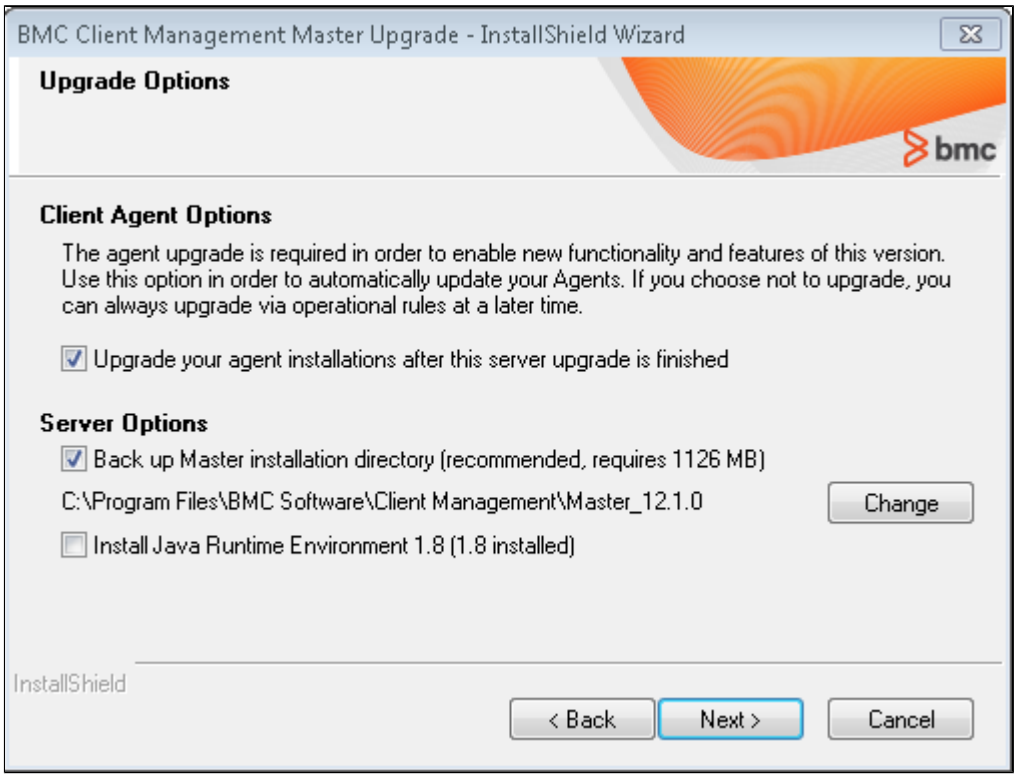
Note:

The new version of BMC Client Management requires new tablespaces. For more information, see Preparing for upgrade. If you have an SQL database, the tablespace upgrade is included in the master upgrade process. However, in specific situations, you still must upgrade the tablespaces manually. For example, if you renamed the tablespaces from their default values. For more information on updating tablespaces, see Preparing for upgrade.

1. Go to the **upgrade/master** directory.
   This directory contains the master upgrade packages for all supported platforms.
2. Launch the **Upgrade.exe** file to start the upgrade wizard.
   A **Choose Setup Language** pop-up requests you to select your language for the installation procedure.
3. Select your language (in this case, probably *English*), and then click **OK** .
4. Wait a few moments while InstallShield prepares the Windows Installer installation and the configuration of BMC Client Management .The **Check Upgrade Settings** screen appears showing the currently installed version number and the version to which you are upgrading.



5. *(Optional)* If it is not installed in the default directory, select the installation directory of the master, and click **Next**.
   The installation directory is provided by the Registry by default.
6. In the **Upgrade Options** window, you have several choices:

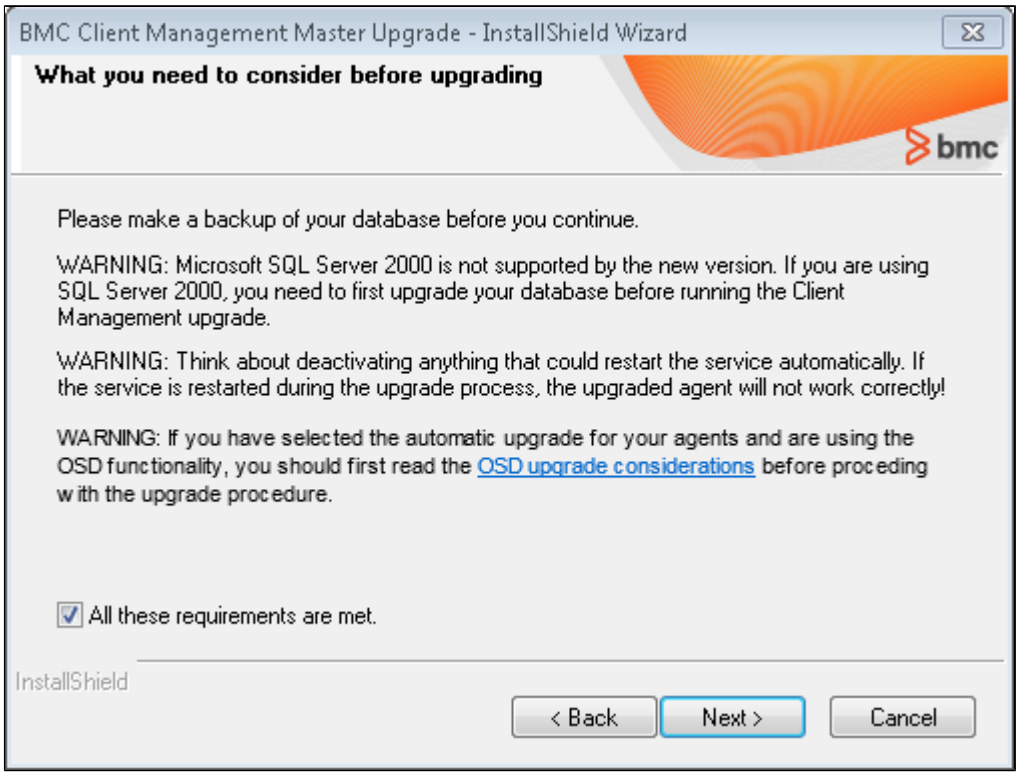


- *(Optional)* If you do not want to automatically upgrade all your clients after the master is upgraded to the new version, clear the **Client Agent Options** box.
- *(Optional)* Clear the check box if you do not want to create a backup of the currently installed master.

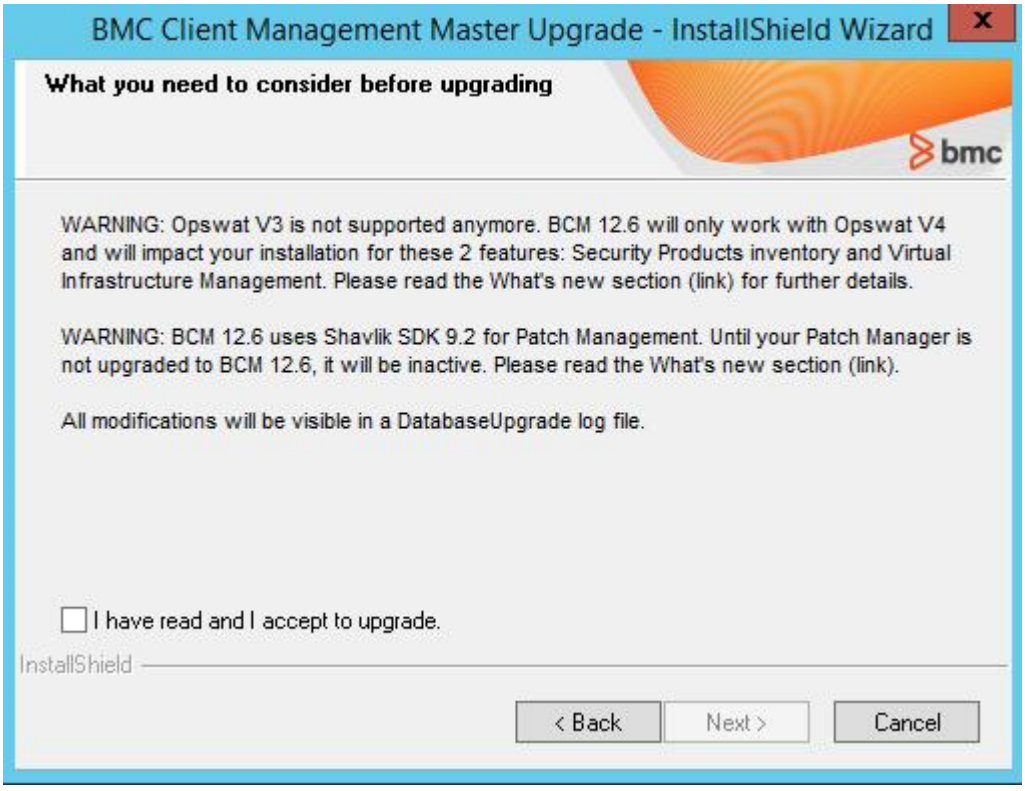
> **Note**
>
> To save the backup in a directory other than the one shown, click the **Change** button and select it from the window that appears.

- *(Optional)* Clear the check box to not upgrade to the newer JRE.

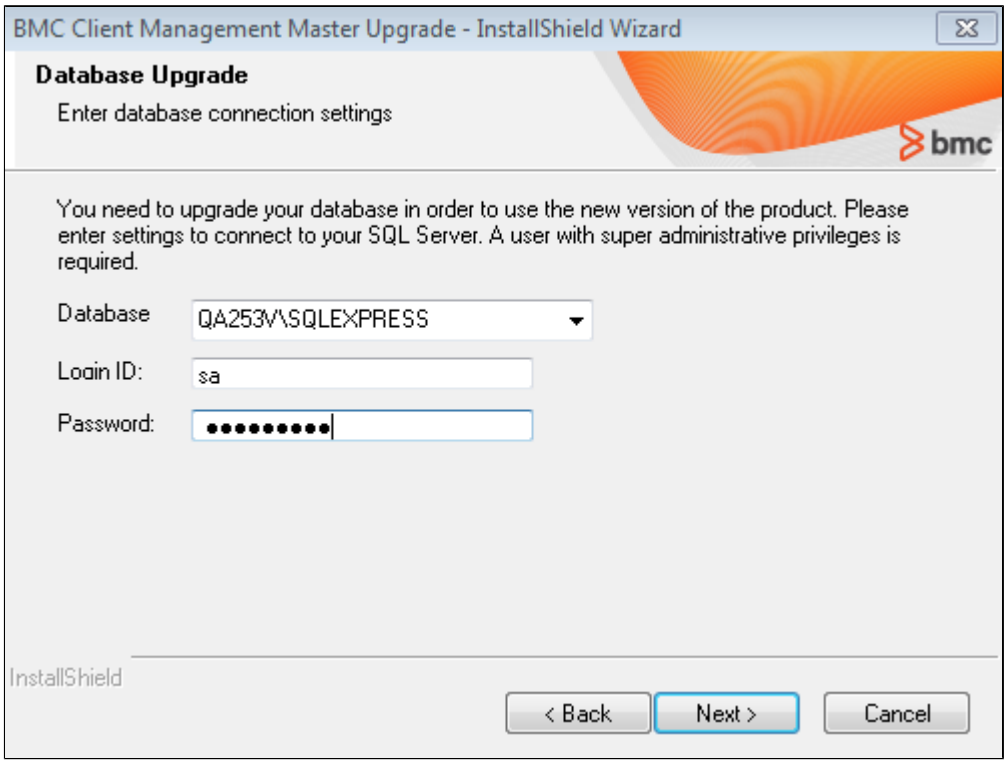
7. Click **Next** .
   The next window lists all requirements that need to be fulfilled before you can start the actual upgrade process. If appropriate, select the **All these requirements are met** box, otherwise abandon the upgrade and execute the necessary options before relaunching the process.



8. Click **Next**.



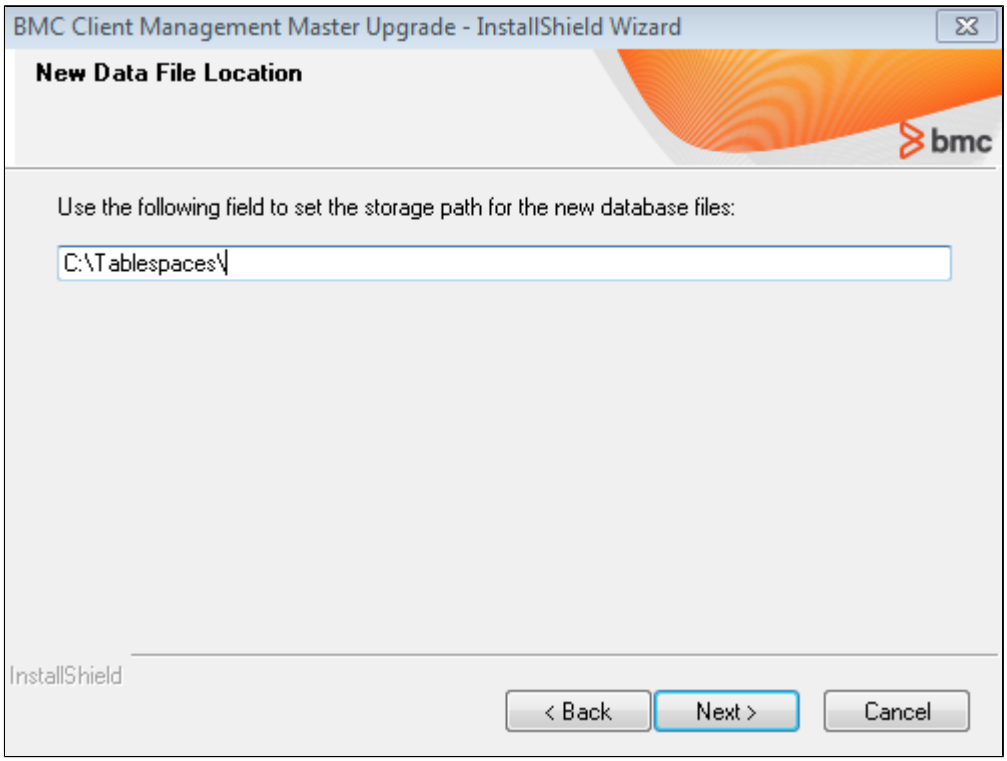
   a. Select **I have read and I accept to upgrade** checkbox.
9. Click **Next**.
   The **Database Upgrade** window appears on the screen.



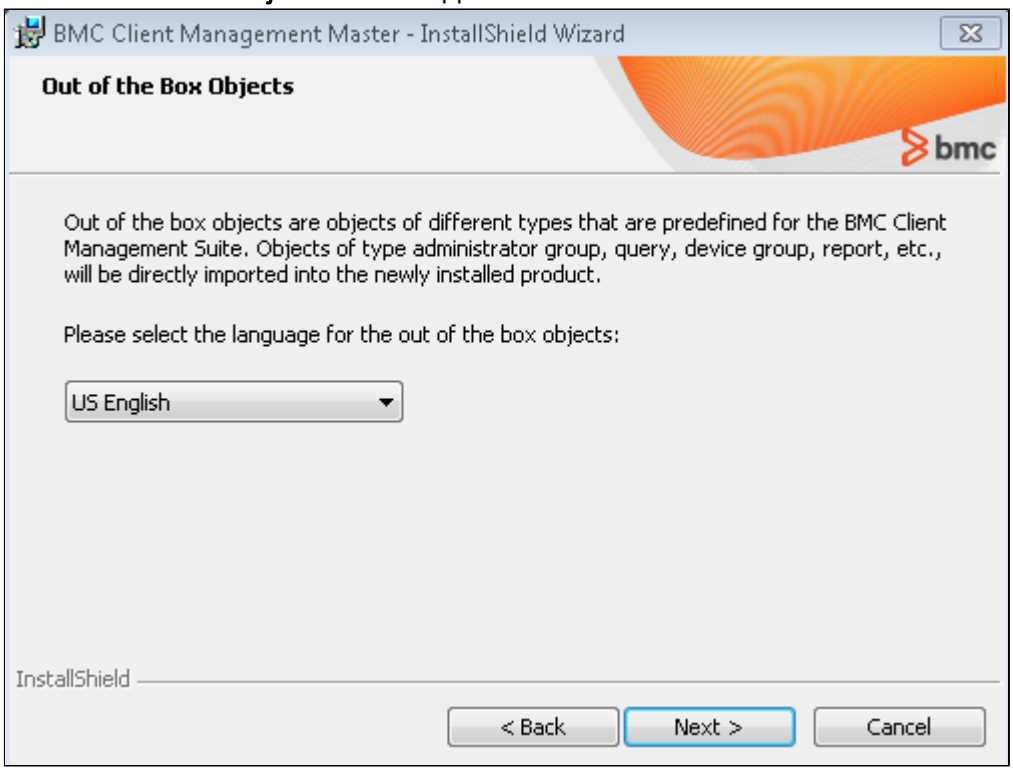
- *(Optional)* If the prepopulated value is incorrect, select the database server from the **Database** list.
- *(Optional)* If the prepopulated value is not correct, enter another administrator account and password with which to upgrade the database.

> **Note**
>
> The account must have superadministrator privileges.

10. Click **Next**.
    If you are upgrading with an SQL database, the **New Data File Location** window appears on the screen. If you work with an Oracle database, this window is not displayed.

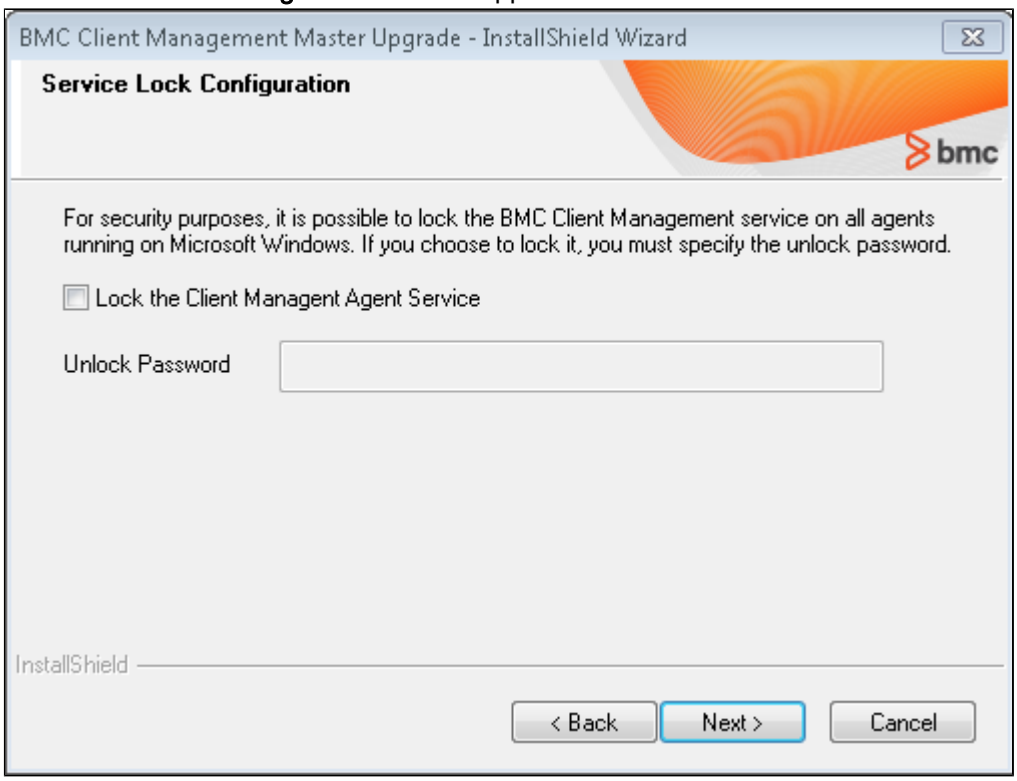


11. Enter the path to the tablespaces directory in the field and click **Next**.
    The **Out of the box Objects** window appears on the screen.

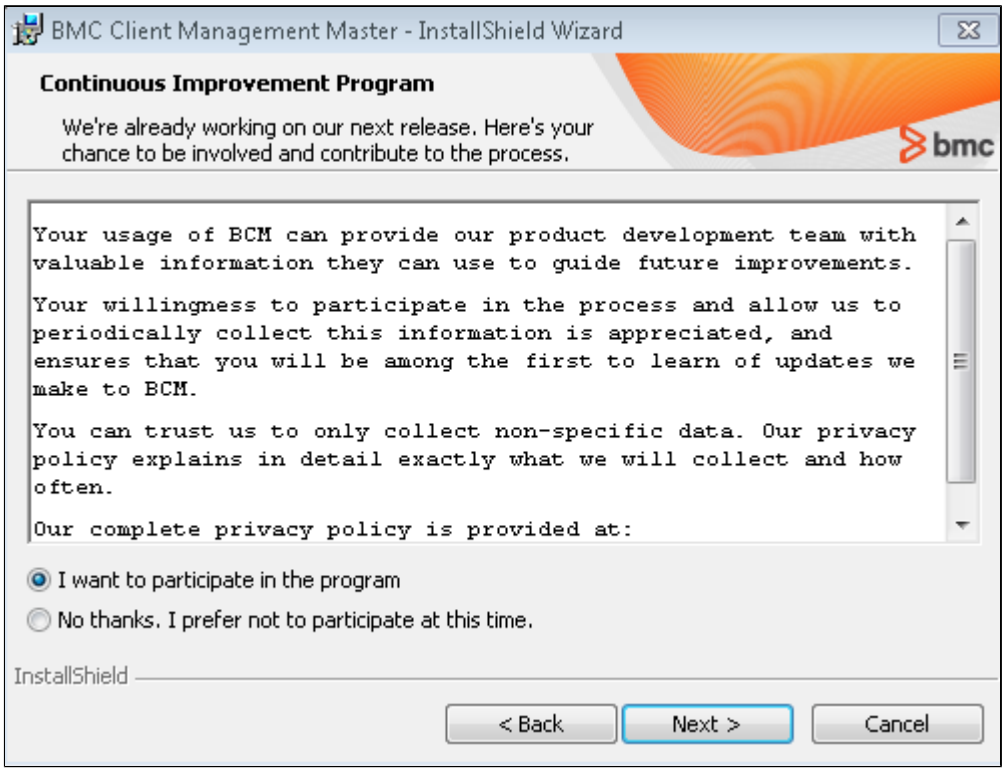


12. Select the language in which to update your predefined objects from the list box.
    You can also manually update the predefined objects at another time (see Upgrading the predefined objects).

13. Click **Next**.
    The **Service Lock Configuration** window appears on the screen.



    (*Optional*) Select the **Lock the Client Management Agent Service** option to prevent local administrators from stopping or starting the service. If you select this option, you have to also specify **Unlock Password**.
14. Click **Next**.
    The **Continuous Improvement Program** window appears on the screen.



(Optional) If you do not want to participate in the Continuous Improvement Program, select **No thanks. I prefer not to participate at this time.** option.

15. Click **Next** .
    If the connection credentials are correct, a new window appears to remind you of the prerequisites and specific considerations. If the connection credentials are not correct, an error message is displayed. You need to acknowledge it, return to the window and retry entering your credentials.
16. Click **Next** .
17. If you do not want to participate in the amelioration of the product and let BMC know your thoughts and ideas about BMC Client Management, select the **I want to participate in the program** option in the **Continuous Improvement Program** window.
18. The next window displays a review of the selected options. If all upgrade settings are to your satisfaction, click the **Upgrade** button to launch the upgrade process.
    The upgrade first stops the agent (that is, the blue icon in the system tray disappears) and then upgrades all components that you have selected to upgrade.
19. In the wizard complete window, click **Finish**.
    To not display the upgrade log, clear the respective button. This is not recommended, however, because it delivers important information should a problem arise during the upgrade.

The upgrade process is now terminated.

Upgrading the master and database on Linux

The update processes of the master and the database are closely linked together and consist of the operations described in the following topics.

1. Open the **/root/BMC/upgrade/master** folder.
2. Open a terminal window, and change directory to **/root/BMC/upgrade/master**.
3. Add executable rights on the script by running the following command:

```
chmod +x linux-master-upgrade.sh
```

4. Execute this command:

```
sh linux-master-upgrade.sh
```

5. The upgrade executable first stops the agent.
6. Answer the questions that appear in the terminal window.

> This upgrade process automatically updates all operational rule steps, report templates, and predefined objects. If you want to manually update the predefined objects at another time, see Upgrading the Predefined Objects.

7. The upgrade process restarts the agent.

Upgrading the common components

The following information leads you through the upgrade process for the common components of BMC Client Management - the console and the predefined (out-of-the-box) objects for all supported platforms. This topic includes:

- Upgrading the console
- Upgrading the predefined objects
- Performing an automatic upgrade of the client agent on all platforms

Upgrading the console

To upgrade a console to the current version you have the following possibilities:

- Automatically upgrading via the console parameters
- Manually upgrading via the console Download page

If you applied a master hotfix, the console is upgraded by this process as well; therefore, you can skip the following sections.

Automatically upgrading via the console parameters

Before upgrading the console, you need to have already upgraded the master. The upgrade process for the console is then configured so that it is executed automatically when the console is launched for the first time after the master upgrade.

Manually upgrading via the console Download page

The **Console Download Page** is available on the master server and provides the links to download the different versions of the BMC Client Management console. This page is only accessible via a browser through the following address: `http://<master name>:<master port>/console`; it cannot be accessed through the regular agent interface.

The BMC Client Management console exists for the different operating systems as well as Java Web Start. To download and install a specific console version, click the link of the desired version under the respective section. To install the console as Java Web Start with the master, click the respective icon on the page.

Notes

- This installs a link on your desktop to the master and enables you to launch the console, which is not installed on the local device. The files required to launch the console are stored in the local cache memory and are updated every time a console update is available.
- Do not empty or delete the Java cache memory, because this deletes the files required for the console Web Start. If this happens, the Web Start Console must be reinstalled.

The download page also provides the current version of the Java Runtime Environment (JRE) that is required by the console as well as the master.

Upgrading the predefined objects

If you imported the out-of-the-box objects, you also need to upgrade them to the new version, if you chose to deactivate the automatic upgrade option. Proceed as follows:

1. Open the console and log on.
2. Select **Tools > Import Out-of-the-Box Objects** .
   The **Out-of-the-Box Object Import** window appears.

3. Select the language of the predefined objects from the list box.
   If you already imported a previous version of this file, the **Import Results** window appears. It lists all predefined objects that are contained in this new file with their object type.
4. Select all objects that are to be added or updated by marking the respective check box in the **Update** column.
5. To update all objects, select the following **Select All Objects** button.
6. Click **OK** to confirm the import and close the window.

The selected predefined objects are now imported: the selected new objects are added and those that already exist are updated. All selected predefined objects are now available in the console for use.

Performing an automatic upgrade of the client agent on all platforms

BMC Client Management agents can be upgraded automatically or manually. If you want to manually upgrade your agents, see the sections under the respective platforms.

Automatic upgrade of agents is specified during the master upgrade. To verify that you have defined automatic upgrade, proceed as follows (by default the automatic upgrade is deactivated):

1. In the console, open the **Global Settings > System Variables** node.
2. Select the **Connection Management** tab.
3. Check that the **Automatic Agent Version Upgrade** parameter is set to **Yes** .
4. If this is not the case, double-click the respective line in the table.
   The **Properties** window opens.
5. Check the box for the parameter.
6. Click **OK** to confirm and close the window.

The automatic agent upgrade is instantly activated. The next time the agents upload their identity to their parent, they are upgraded immediately, if an upgrade is available.

Manually upgrading the BMC Client Management client agents

This section provides information about upgrading the BMC Client Management agent on all supported platforms. Normally the upgrade is done automatically by the master after it was upgraded. If you deactivated the automatic upgrade option you must upgrade your environment manually.

There are two possible ways to manually upgrade the agents on the relays and clients.

Note:

Be aware that when doing so you must execute the operation for all different platforms individually.

You can upgrade the client in two different ways:

- Individually (one by one):
  - Upgrading client agents individually on Windows systems
  - Upgrading client agents individually on Linux systems
  - Upgrading the agents individually on MAC systems
- Via device groups
  - Upgrading client agents via device groups on Windows systems
  - Upgrading client agents via device groups on Linux systems
  - Upgrading client agents via device groups on MAC systems

Upgrading client agents individually on Windows systems

Installed BMC Client Management client agents can be upgraded from any previous version to the most recent version very easily via a semi-automatic upgrade which is executed through an operational rule.

The upgrade process for agents works as follows for all of the different platforms:

1. Log on to the console with a super administrator login or equivalent rights.

   To upgrade client agents via device groups instead of individually, see Upgrading client agents via device groups .

   One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* under the **Packages** / **Operational Rules** top nodes.

   Note:

   If you performed previous upgrades, for example, from 6.1.2 to 6.1.3, the operational rules and packages are placed under the previously created folder called, for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, for example:
   - *Win32Upgrade* / *Win32Oneoff* for agents on 32-bit Windows devices
   - *Win64Upgrade* / *Win64Oneoff* for all agents installed on 64-bit Windows systems.
3. Go to the **Assigned Objects > Devices** node below the selected package.
4. Select **Edit > Assign Device** .
   A pop-up window appears in which you can define if the operational rule is automatically activated with the default schedule.
5. Click **Yes** .

   > If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device** pop-up window appears.
6. Click the **All** button in the left window bar.
   The list in the right part of the window now displays all available devices of your infrastructure on which a BMC Client Management agent is installed.
7. Select all devices of the operating system type that require upgrading from the list, for example, all Windows 64-bit devices for the *Win64Upgrade* rule.
8. Click **OK** to confirm the assignment and close the window.
   The devices are added to the table of assigned devices with the default timer, which schedules the execution once and immediately.

When the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` is displayed in the **Status** box for the respective device in the table of all assigned devices.

To verify this go to a device node, either in the **Device Topology** or in a device group and select the device's **General** tab.

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Upgrading client agents individually on Linux systems

Installed BMC Client Management client agents can be upgraded from any previous version to the most recent version very easily via a semi-automatic upgrade which is executed through an operational rule.

The upgrade process for agents works as follows for all different platforms:

1. Log on to the console with a super administrator login or equivalent rights.

> To upgrade client agents via device groups instead of individually, see Manually upgrading client agents via device groups on Linux systems now.

One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* under the **Packages** / **Operational Rules** top nodes.

> **Note:**
>
> If you performed previous upgrades, for example, from 6.1.2 to 6.1.3, the operational rules and packages are placed under the previously created folder called, for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, for example:
   - *Linux32Upgrade* / *Linux32Oneoff* for agents on 32-bit Linux devices
   - *Linux64Upgrade* / *Linux64Oneoff* for all agents installed on 64-bit Linux systems.
3. Go to the **Assigned Objects > Devices** node below the selected package.
4. Select **Edit > Assign Device** .
   A pop-up menu appears in which you can define if the operational rule is automatically activated with the default schedule.
5. Click **Yes** .

> If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device** pop-up menu appears.
6. Click **All** in the left window bar.
   The list in the right part of the window now displays all available devices of your infrastructure on which a BMC Client Management agent is installed.
7. Select all devices of the operating system type that require upgrading from the list, for example, all Linux 64-bit devices for the *Linux64Upgrade* rule.
8. Click **OK** to confirm the assignment and close the window.
   The devices are added to the table of assigned devices with the default timer, which schedules the execution once and immediately.

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device in the table of all assigned devices.

To verify this go to a device node, either in the **Device Topology** or in a device group and select the device's **General** .

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Upgrading the agents individually on MAC systems

The installed BMC Client Management agents can be upgraded from any previous version to the most recent version very easily via a semi-automatic upgrade which is executed through an operational rule.

The upgrade process for agents works as follows for all of the different platforms:

1. Log on to the console with a super administrator login or equivalent rights.

   > To upgrade client agents via device groups instead of individually, see Manually upgrading the client agents via device groups on MAC systems now.

   One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* under the **Packages** / **Operational Rules** top nodes.

   > **Note:**
   >
   > If you performed previous upgrades, for example, from 6.1.2 to 6.1.3, the operational rules/packages are placed under the previously created folder called for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, for example: *MaxOsXUpgrade* or *MaxOsXOneoff* for agents on any version of MAC operating system.
3. Go to the **Assigned Objects > Devices** node below the selected package.
4. Select **Edit > Assign Device** .
   A pop-up window appears in which you can define if the operational rule is automatically activated with the default schedule.

5. Click **Yes** .

   > If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device** pop-up window appears.
6. Click the **All** button in the left window bar.
   The list in the right part of the window now displays all available devices of your infrastructure on which a BMC Client Management agent is installed.
7. Select all devices of the operating system type that require upgrading from the list, for example, all devices with a MAC operating system for the *MaxOsXUpgrade* rule.
8. Click **OK** to confirm the assignment and close the window.
   The devices are added to the table of assigned devices with the default timer, which schedules the execution once and immediately.

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device in the table of all assigned devices.

To verify this go to a device node, either in the **Device Topology** or in a device group and select the device's **General** .

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a oneoff, the **Agent Revision** number should have increased by one.

Upgrading client agents via device groups on Windows systems

Agents can be upgraded via device groups instead of individually. To use this type of upgrade, one or more Windows device groups must be created. While it is possible to create these groups during the upgrade procedure it, BMC recommends that you prepare them beforehand.

> **Note**
>
> To use this procedure to upgrade the client agents, you must have the newest version of the predefined objects installed (see Upgrading the predefined objects).

To upgrade client agents via device groups you need to execute the following two procedures:

1. Creating Windows target groups:
   For Windows systems, two different upgrade packages are available, one for 32 bit Windows and another for 64 bit Windows . Depending on the population of your network, you might therefore only need to create one of the following groups or both. These groups must contain all clients and relays that are running on the respective Windows operating system. To populate these groups, two queries must be created: One that finds all devices with the respective operating system version and a second one that finds either the clients or the relays. Both can be based on existing queries.
2. Upgrading the BMC Client Management agents on Windows devices via device groups.

This topic includes the following procedures:

- To create the 32-bit Windows group
- To create the 64-bit Windows group
- To upgrade the BMC Client Management agents on Windows devices via device groups

To create the 32-bit Windows group

1. Go to the **Queries** node.
2. Select the folder **Operating Systems** .
3. Select the **Windows** folder.
4. Select the query *32 Bit Windows Devices* .

> If you need to create a group for several types of Windows devices you can select more than one query in this folder by holding the CTRL key.

5. Click **Edit > Create Device Group** .
   The new group is automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *32 Bit Windows Devices* .
6. Find the query *Client Devices* , duplicate it and give it a new name, for example, *All Clients and Relays* .

> This query is located either in the folder *BMC Client Management Architecture* or *Numara Asset Management Platform Architecture* , depending on which version you have currently installed.

> **Note**
>
> If you already have a query that collects all client devices and all relays you can skip the following procedure and continue directly with step 17 .

7. Select the new query and go to its **Criteria** tab.
8. Select **OR** as the **Query Operator** above the criteria table.
9. Select **Edit > Add Criterion** .
   The **Select Criterion** pop-up window appears.
10. Select the criterion **Topology Type** .
11. Click the **Find** button.
    The **Search Criteria** pop-up dialog appears.
12. Select the **Relay** topology type and click **OK** .
13. Change the **Operator** to **Equal to** .
14. Click the **Add** button to add the criterion to the list.
15. Click **OK** to confirm the new query content and to close the window.
16. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** box above the table.
17. Go to the **Device Groups** top node and select the query_32 Bit Windows Devices_ .
18. Select its **Dynamic Population > Queries** subnode.
19. Click the **Assign Query** icon.
20. Find the newly created query *All Clients and Relays* or your existing query, select it and click **OK** .
    A **Properties** window appears.
21. Select the option **Only Devices with an Agent** as the **Device Type** and click **OK** .
    The second query is directly assigned to the group.

The new group is now created using both queries to find its population and is ready to be used for upgrading all Windows 32-bit agents.

To create the 64-bit Windows group

1. Select the query *64 Bit Windows Devices* .
2. Click **Edit > Create Device Group** .
   The new group is automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *64 Bit Windows Devices* .
3. Find the query *Client Devices* , duplicate it and give it a new name, for example, *All Clients and Relays* .

> This query is located either in the folder *BMC Client Management Architecture* or *Numara Asset Management Platform Architecture* , depending on which version you have currently installed.

> **Note:**

If you already have a query that collects all client devices and all relays you can skip the following procedure and continue directly with step 14.

4. Select the new query and go to its **Criteria** tab.
5. Select **OR** as the **Query Operator** above the criteria table.
6. Select **Edit > Add Criterion** .
   The **Select Criterion** pop-up window appears.
7. Select the criterion **Topology Type** .
8. Click the **Find** button.
   The **Search Criteria** pop-up dialog appears.
9. Select the **Relay** topology type and click **OK** .
10. Change the **Operator** to **Equal to** .
11. Click the **Add** button to add the criterion to the list.
12. Click **OK** to confirm the new query content and to close the window.
13. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** list box above the table.
14. Go to the **Device Groups** top node and select the group *64 Bit Windows Devices*.
15. Select its **Dynamic Population > Queries** subnode.
16. Click the **Assign Query** icon.
17. Find the query *All Clients and Relays* or your existing query, select it and click **OK** .
    A **Properties** window appears.
18. Select the option **Only Devices with an Agent** as the **Device Type** and click **OK** .
    The second query is directly assigned to the group.

The new group is now created using both queries to find its population and is ready to be used for upgrading all Windows 64-bit agents.

To upgrade the BMC Client Management agents on Windows devices via device groups

Now that all necessary groups have been created, the upgrade packages can be created, assigned and distributed to these target groups. Proceed as follows:

1. In the console select the **Tools > Create Upgrade Packages** menu item.
   One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* or *BMC Client Management Oneoff* under the **Packages** / **Operational Rules** top nodes.

Note:

If you performed previous upgrades, for example: 6.1.2 to 6.1.3 the operational rules and packages are placed under the previously created folder called, for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, for example,
   - *Win32Upgrade* / *Win32Oneoff* for agents on 32-bit Windows devices
   - *Win64Upgrade* / *Win64Oneoff* for all agents installed on 64-bit Windows systems.
3. Go to the **Assigned Objects > Device Groups** node below the selected package.
4. Select the **Edit > Assign Device Group** icon.
   A pop-up window appears in which you can define if the operational rule is automatically activated with the default schedule.
5. Click **Yes** .

   If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device Group** pop-up window appears.
6. Click the **All** button in the left window bar.
   The list in the right part of the window now displays all available device groups of your infrastructure on which a BMC Client Management agent is installed.
7. Select the group of the operating system type and that require upgrading from the list, for example, *64 Bit Windows Devices* for the *Win64Upgrade* rule.
8. Click **OK** to confirm the assignment and close the window.
   The device group is assigned with the default timer, which schedules the execution once and immediately.
9. Go to the **Assigned Objects > Devices** subnode.

   This view lists all devices that are a member of the assigned group and information on the upgrade process.

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device.

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Upgrading client agents via device groups on Linux systems

Agents can be upgraded via device groups instead of individually. To use this type of upgrade one or more Linux device groups need to be created. While it is possible to create these groups during the upgrade procedure it, BMC recommends that you prepare them beforehand.

> **Note:**
>
> To use this procedure to upgrade the client agents you must have the newest version of the predefined objects installed (see topic Upgrading the predefined objects).

To upgrade client agents via a device group, you need to execute the following two procedures:

1. Creating the Linux target groups:
   For Linux systems, two different upgrade packages are available, one for 32-bit Linux and another for 64-bit Linux . Depending on the population of your network, you might therefore only need to create one of the following groups or both. These groups must contain all clients and relays that are running on the respective Linux operating system. To populate these groups, two queries need to be created: One that finds all devices with the respective operating system version and a second one that finds either the clients or the relays. Both can be based on existing queries.
2. Upgrading the BMC Client Management agents on Linux devices via device groups.

This topic includes the following procedures:

- To create the 32-bit Linux group
- To create the 64-bit Linux group
- To upgrading the BMC Client Management agents on Linux devices via device groups

To create the 32-bit Linux group

1. Go to the **Queries** node.
2. Select the folder *Operating Systems* .
3. Select the folder *UNIX* .

> **Note:**
>
> If you already have a query that collects all 32-bit Linux devices you can skip the following procedure and continue directly with step 14.

4. Select the query *Linux Devices* , duplicate it and give it a new name, for example, *32 Bit Linux Devices* .

5. Select the new query and go to its **Criteria** tab.
6. Select **AND** as the **Query Operator** above the criteria table.
7. Select **Edit > Add Criterion** .
   The **Select Criterion** pop-up menu appears.
8. Select the criterion **Operating System Name** .
9. Change the **Operator** to **Contains** .
10. Enter *32* in the **Value** box.
11. Click **Add** to add the criterion to the list.
12. Click **OK** to confirm the new query content and to close the window.
13. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** list box above the table.
14. Now select the new query in the hierarchy to the left, right-click and select the **Create Device Group** menu option.
    The new group is automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *32 Bit Linux Devices* .
15. Find the query *Client Devices* , duplicate it and give it a new name, for example, *All Clients and Relays* .

> This query is located either in the folder *BMC Client Management database* or *Numara Asset Management Platform Architecture* , depending on which version you have currently installed.

> **Note:**
>
> If you already have a query that collects all client devices and all relays you can skip the following procedure and continue directly with step 26.

16. Select the new query and go to its **Criteria** tab.
17. Select **OR** as the **Query Operator** above the criteria table.
18. Select **Edit > Add Criterion** .
    The **Select Criterion** pop-up menu appears.
19. Select the criterion **Topology Type** .
20. Click **Find** .
    The **Search Criteria** pop-up window appears.
21. Select the **Relay** topology type and click **OK** .
22. Modify the **Operator** to **Equal to** .
23. Click **Add** to add the criterion to the list.
24. Click **OK** to confirm the new query content and to close the window.
25. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** list box above the table.

26. Go to the **Device Groups** top node and select the group *32 Bit Linux Devices* .
27. Select its **Dynamic Population > Queries** subnode.
28. Click **Assign Query** .
29. Find the newly created query *All Clients and Relays* , select it and click **OK** .
    A **Properties** window appears.
30. Select the **Only Devices with an Agent** option as the **Device Type** and click **OK** .
    The second query is directly assigned to the group.

The new group is now created using both queries to find its population and is ready to be used for upgrading all 32-bit Linux agents.

To create the 64-bit Linux group

1. Go to the **Queries** node.
2. Select the folder *Operating Systems* .
3. Select the folder *UNIX* .

> **Note:**
>
> If you already have a query that collects all 64-bit Linux devices you can skip the following procedure and continue directly with step 14.

4. Select the query *Linux Devices* , duplicate it and give it a new name, for example, *64 Bit Linux Devices* .
5. Select the new query and go to its **Criteria** tab.
6. Select **AND** as the **Query Operator** above the criteria table.
7. Click **Edit > Add Criterion** .
   The **Select Criterion** pop-up menu appears.
8. Select the criterion **Operating System Name** .
9. Change the **Operator** to **Contains** .
10. Enter *64* in the **Value** box.
11. Click **Add** to add the criterion to the list.
12. Click **OK** to confirm the new query content and to close the window.
13. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** list box above the table.
14. Now select the new query in the hierarchy to the left, right-click and click the **Create Device Group** menu option.
    The new group is automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *64 Bit Linux Devices* .
15. Find the query *Client Devices* , duplicate it and give it a new name, for example, *All Clients and Relays* .

This query is located either in the folder *BMC Client Management database* or *Numara Asset Management Platform Architecture* , depending on which version you have currently installed.

Note:

If you already have a query that collects all client devices and all relays you can skip the following procedure and continue directly with step 26.

16. Select the new query and go to its **Criteria** tab.
17. Select **OR** as the **Query Operator** above the criteria table.
18. Select **Edit > Add Criterion** .
    The **Select Criterion** pop-up menu appears.
19. Select the criterion **Topology Type** .
20. Click **Find** .
    The **Search Criteria** pop-up window appears.
21. Select the **Relay** topology type and click **OK** .
22. Modify the **Operator** to **Equal to** .
23. Click **Add** to add the criterion to the list.
24. Click **OK** to confirm the new query content and to close the window.
25. Activate the query by selecting the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** list box above the table.
26. Go to the **Device Groups** top node and select the group *64 Bit Linux Devices* .
27. Select its **Dynamic Population > Queries** subnode.
28. Click **Assign Query** .
29. Find the newly created query *All Clients and Relays* , select it and click **OK** .
    A **Properties** window appears.
30. Select the **Only Devices with an Agent** option as the **Device Type** and click **OK** .
    The second query is directly assigned to the group.

The new group is now created using both queries to find its population and is ready to be used for upgrading all 64-bit Linux agents.

To upgrading the BMC Client Management agents on Linux devices via device groups

Now that all necessary groups have been created, the upgrade packages can be created, assigned and distributed to these target groups. Proceed as follows:

1. In the console select the **Tools > Create Upgrade Packages** menu item.
   One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* or *BMC Client Management Oneoff* under the **Packages** / **Operational Rules** top nodes.

> **Note:**
>
> If you performed previous upgrades, for example, 6.1.2 to 6.1.3, the operational rules/packages are placed under the previously created folder called, for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, for example,
   - *Linux32Upgrade* / *Linux32Oneoff* for agents on 32-bit Linux devices
   - *Linux64Upgrade* / *Linux64Oneoff* for all agents installed on 64-bit Linux systems.
3. Go to the **Assigned Objects > Device Groups** subnode.
4. Select **Edit > Assign Device Group** .
   A pop-up window appears in which you can define if the operational rule is automatically activated with the default schedule.
5. Click **Yes** .

> If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device Group** pop-up window appears.
6. Click the **All** button in the left window bar.
   The list in the right part of the window now displays all available device groups.
7. Select the device group created in the preceding step, which contains all devices of the operating system to be upgraded, for example:

- *32 Bit Linux Devices* all Linux 32-bit devices
- *64 Bit Linux Devices* all Linux 64-bit devices

1. Click **OK** to confirm the assignment and close the window.
   The device group is assigned with the default timer, which schedules the execution once and immediately.
2. Go to the **Assigned Objects > Devices** subnode.

This view lists all devices that are a member of the assigned group and information on the upgrade process.

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device.

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Upgrading client agents via device groups on MAC systems

Agents can be upgraded via device groups instead of individually. To use this type of upgrade, a specific Mac device group needs to be created. While it is possible to create this group during the upgrade procedure, BMC recommends that you prepare it beforehand.

Note:

To use this procedure to upgrade the client agents you must have the newest version of the predefined objects installed (Upgrading the predefined objects).

To upgrade MAC agents via a device group, you need to execute the following two procedures:

- To creating the target group
- To upgrading the BMC Client Management agents on Mac OS X devices via device groups

To creating the target group

1. Go to the **Queries** node.
2. Select the folder *Operating Systems* .
3. Select the *Mac OS X* folder.
4. Select the query *Mac OS Devices* .
5. Click **Edit > Create Device Group** .

The new group is automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *Mac OS Devices* .

To upgrading the BMC Client Management agents on Mac OS X devices via device groups

Now that the necessary group has been created, the upgrade packages can be created, assigned and distributed to these target groups. Proceed as follows:

1. In the console click **Tools > Create Upgrade Packages** .
   One custom package (**.cst**) per **.zip** file is created in the same location together with its respective operational rule and is placed in a specifically created folder called *Client Management Upgrade* or *BMC Client Management Oneoff* under the **Packages** / **Operational Rules** top nodes.

   > **Note:**
   >
   > If you performed previous upgrades, for example, 6.1.2 to 6.1.3, the operational rules/packages are placed under the previously created folder called, for example, *PrecisionUpgrade* , *NumaraAssetManagementPlatformUpgrade* or *FootprintsAssetCoreUpgrade* . No new folder is created.

2. Go to the **Operational Rules > Client Management Upgrade** node and select the operational rule to upgrade the agents, *MaxOsXUpgrade* or *MaxOsXOneoff* .
3. Go to the **Assigned Objects > Devices** node below the selected package.
4. Click **Edit > Assign Device Group** .
   A pop-up window appears in which you can define if the operational rule is automatically activated with the default schedule.
5. Click **Yes** .

   > If you select **No** here, the operational rule must be specifically activated afterwards.

   The **Assign to Device Group** pop-up window appears.
6. Click the **All** button in the left window bar.
   The list in the right part of the window now displays all available device groups.
7. Select the device group created in the preceding step, which contains all devices of the operating system to be upgraded, in this case *Mac OS Devices* .
8. Click **OK** to confirm the assignment and close the window.
   The device group is assigned with the default timer, which schedules the execution once and immediately.
9. Go to the **Assigned Objects > Devices** subnode.

   > This view lists all devices that are a member of the assigned group and information on the upgrade process.

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device.

The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Verifying the upgrade

There are two parts of verifying the upgrade process:

- Verifying the master and database upgrade
- Verifying the client agent upgrade

Verifying the master and database upgrade

When the upgrade process is finished, a terminating window appears and the agent is restarted.

You can see that the upgrade process was successful, when the agent icon reappears in the status bar. During its initialization process the icon is gray  , and it is shown in blue  when the agent is up and running again.

If an error occurred during the upgrade process, the agent icon stays gray. To check for the errors, open the upgrade log, located in the **/log** directory.

Verifying the client agent upgrade

After the assignment process is finished and the upgrade package has arrived at the targets, the agents are automatically upgraded.

This is the case when the status is green and `Executed` displays in the **Status** box for the respective device in the table of all assigned devices.

To verify this proceed as follows:

- Go to a device node, either in the **Device Topology** or in a device group and select the device's **General** tab.
  The attributes **Agent Version Major** and **Agent Version Minor** should display the values `12` and `0` now. If you are applying a hotfix, the **Agent Revision** number should have increased by one.

Integrating

External integration in BMC Client Management is set up to allow for data exchange between BMC Client Management and other applications, such as BMC Remedyforce, BMC FootPrints Service Core, BMC Atrium CMDB, and Remedy with Smart IT.

Whenever a specific event is generated in BMC Client Management, a notification is sent to the target software to create an incident ticket in the target application. This allows the administrators of the target application to follow up on the progress of these events.

This section explains how to define and set up external integrations with other applications and how to track these events in BMC Client Management. For information about how set up the target applications for external integration with BMC Client Management and how to use the information made available by BMC Client Management in the target applications, see the respective product documentations. The BMC Client Management sections of the BMC Remedyforce, BMC FootPrints Service Core, and Remedy with Smart IT online helps.

The following table provides links to the relevant topics based on your goals:

Goal	Instructions
Understand product compatibility matrix	• Product matrix compatibility
Integrate and exchange data between BMC Client Management and ITSM applications	• Integrating with BMC ITSM applications • Configuring the Web Service • Setting up external integration with BMC Remedyforce • Setting up external integration with BMC FootPrints Service Core • Tracking shared events • Events defined for notification
Integrate and exchange data between BMC Client Management and BMC Atrium CMDB	• Integrating with BMC Atrium CMDB • Supported versions • Atrium installation • Configuring the SQL database for Atrium CMDB integration • Filters • Working with the integration maintenance tool
Integrate BMC Client Management and Remedy with Smart IT to automate incident generation	• Before you begin • Identify events for monitoring assets in BCM • Creating an integration with Remedy with Smart IT • Results • Track notification events and alerts in BCM • Updating notification events in BCM • Troubleshooting • Where to go from here

Product matrix compatibility

The following table provides the product compatibility matrix for BMC Client Management integration with other BMC products. At the time of release, the product versions listed in the table were tested as compatible.

Product	Version	BMC Client Management 12.0 compatibility	BMC Client Management 12.1 compatibility	BMC Client Management 12.5 compatibility
FootPrints	11.5x	Yes	Yes	Yes
FootPrints	11.Current	Yes	Yes	Yes
FootPrints	12.0.0	Yes	Yes	Yes
FootPrints	12.Current	Yes	Yes	Yes
BMC Remedyforce	Earlier than summer 2014	Yes	Yes	Yes
BMC Remedyforce	Current	Yes	Yes	Yes
BMC Atrium CMDB	7.6.04	Yes	Yes	Yes
BMC Atrium CMDB	8.x	Yes	Yes	Yes
BMC Atrium CMDB	9.0		Yes	Yes
BMC Atrium CMDB	9.1		Yes	Yes
Remedy with Smart IT	1.5.01			Yes (with Patch 3)

Integrating with BMC Remedy Single Sign-On

BMC Remedy Single Sign-On (BMC Remedy SSO) is an authentication system that supports various authentication protocols such as LDAP and provides single sign-on for users of BMC products. For more information about BMC Remedy Single Sign-On, including installation and configuration, see BMC Remedy Single Sign-On overview in the BMC Remedy Action Request System 9.1 online documentation.

Integrating BCM with BMC Remedy SSO enables Remedy with Smart IT technicians to remote control BCM managed endpoints through the BCM browser-based console.

The BMC Remedy SSO administrator typically provides the parameters needed to apply Remedy SSO settings in BCM. As a BCM administrator, ensure that the mandatory settings are met to ensure a successful integration.

To integrate with BMC Remedy SSO, a BCM administrator must configure Remedy SSO parameters in the BCM console. After successfully configuring Remedy SSO with BCM, the Remedy with Smart IT administrator gets access to the BCM browser-based console to search for and remote control BCM managed devices.

Before you begin

As a BCM administrator who is integrating BCM with Remedy SSO, ensure that the following settings are met:

- Remedy SSO parameter details
  - RSSO URL
  - Realm
  - Certificate Authority
  - Server Certificate

Mandatory settings

- The minimum supported version of BMC Remedy SSO is 9.1.01 and later.
- The BCM master and the BMC Remedy SSO server must be in the same domain. For example, if the BCM master server domain name is bcm.calbro.com, then the BMC Remedy SSO domain name must be rsso.calbro.com.
- BCM and the BMC Remedy SSO server must use the same LDAP server. Otherwise, BCM is unable to check user permissions even if the user has successfully logged in through BMC Remedy SSO.
- The BCM master server must have a reservation in DNS and must be accessed using that DNS name; otherwise, the integration fails and the following message is displayed: **Forbidden request! Goto** url **is wrong**.
- The same user must be present on both BMC Remedy SSO and BCM master server; otherwise, the integration fails. For example, if **AllenBrooks** is authenticated through Remedy SSO, then a user **AllenBrooks** should be present on the BCM master server as well.

Considerations for configuring certificates

Communication between BCM and BMC Remedy SSO can take place only over secured protocol (HTTPS). To enable communication by using HTTPS, you must obtain the HTTPS certificate from the Remedy SSO server.

You can supply a CA bundle that is trusted by your organization, pin the certificate downloaded from BMC Remedy SSO, or use both.

A pinned certificate is more secure than a CA bundle; however, pinned certificates require more frequent renewal. BMC recommends that you use both a pinned certificate and a trusted CA bundle to verify the identity of the Remedy SSO server.

BMC Remedy SSO parameters

As a BCM administrator, you must get the following settings from a Remedy SSO administrator. The following parameters are required to configure Remedy SSO with BCM.

Parameter	Description
Enabled	Defines whether the Remedy SSO server authentication is activated.
RSSO Server URL	Enter the URL for the BMC Remedy SSO server. The Remedy SSO server URL must begin with https and have the same domain as the BCM master server. For example, use *bcm.calbro.com* and *rsso.calbro.com*.
RSSO Realm ID	A realm is a virtual identity provider used to authenticate a domain. Contact your Remedy SSO administrator for the Realm ID. This field must not be empty. The Realm ID must exist on the Remedy SSO server.
Product Identifier	Defines the identifier for BMC Client Management. The identifier must be unique for each application that provides authentication through Remedy SSO server.
RSSO Token revalidation period	Enter the revalidation period in seconds. For more information, contact your Remedy SSO administrator.
Certificate Authority Bundle	Configures the list of certificate authorities that BMC Client Management must trust when connecting to a Remedy SSO server.
Server Certificate	Defines the server certificate to accept when connecting to the Remedy SSO server. This certificate is taken from the Remedy SSO server and it must be pinned to use the certificate.

Note: You must configure a certificate on the BMC Client Management console using one of the options for security purposes.

Configuring BCM to integrate with BMC Remedy SSO

As a BCM administrator, you need the required parameters to configure Remedy SSO in BCM.

To apply the BMC Remedy SSO settings, perform the following steps:

1. In the BCM console, go to **Global Settings** > **System Variables**.
2. In the **RSSO** tab, enter the parameter values.
    a. Enable RSSO
    b. RSSO URL
    c. RSSO Realm ID
    d. Product Identifier
    e. RSSO Token revalidation period
    f. Certificate Authority
    g. Server Certificate
3. Click **OK**.

Troubleshooting

Issue	Cause (s)	Resolution(s)
BCM integration with Remedy SSO not successful	Incorrect Remedy SSO parameters Remedy SSO server down	Contact Remedy administrator
Cannot authenticate into BCM browser-based console	Remedy SSO server down Incorrect Remedy SSO credentials Incorrect configuration in BCM	Contact Remedy administrator to ensure Remedy server is up and running Contact BCM administrator to check whether Remedy SSO is correctly configured

Next steps

Connect to the BCM browser-based console using Remedy SSO credentials

Integrating with BMC ITSM applications

Integration with ITSM applications in BMC Client Management is set up to allow for data exchange between BMC Client Management and ITSM applications, such as BMC Remedyforce and BMC FootPrints Service Core. Whenever a specific event is generated in BMC Client Management, a notification is sent to the target application to create an incident ticket. This allows the administrators of the target application to follow up on the progress of these events.

This section explains how to define and set up external integrations with other ITSM applications - BMC Remedyforce and BMC FootPrints Service Core - and how to track these events in BMC Client Management.

This topic includes:

Configuring the web service

For the external integration with other products to work, the web service module is required. You need to add those devices to the Web Service Configuration view. Also, for the BMC Client Management integration with other ITSM applications, an SSL certificate issued by a trusted authority is required.

Configuring the device web service for use with the external integrations consists of the following steps:

Adding an SSL certificate

To secure the transactions and encrypt the information passing between the BMC Client Management server and BMC ITSM applications, you must install a Secure Socket Layer (SSL) certificate on the BMC Client Management server. For more information about SSL, see http://en.wikipedia.org/wiki/Secure_Sockets_Layer. You must purchase an SSL certificate from an SSL vendor, such as Go Daddy or Symantec . After purchasing the SSL certificate, you must prepare the certificate by creating a private key and Certificate Signing Request (CSR). When you created the private key and the CSR, you are ready to install the SSL certificate.

This process is divided into the following steps:

Preparing the CSR

When purchasing an SSL certificate, the certification authority will request you to provide a Certificate Signing Request (CSR). A CSR is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private 2048-bit key will also be created at the same time which you should store in a safe place.

To prepare your certificate proceed as follows:

1. Click **Prepare Certificate Request**  .
   The **Prepare Certificate Request** appears.
2. Enter the required information into the following fields:

Parameter	Description
Domain Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser or you receive a name mismatch error. For example *.google.com, mail.google.com .
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC, for example My Spy Company, Inc..
Department	The division of your organization handling the certificate.
City	The city where your organization is located.
State/Province	The state/region where your organization is located. This should not be abbreviated, for example Califiornia.
Country	Select the country in which your organization is located from the dropdown list.
Private Key Password	Enter the password that encodes the private key. This is not mandatory but recommended.
Private Key Password Confirmation	Reenter the password for confirmation.

3. Click **1 Save Private Key** .
4. Browse to the location where you want to save the private key.

> BMC recommends that you save the private key in the same folder where you saved the SSL certificate.

   The private key is now saved in a text file on your computer.
5. Click **2 Save CSR** .
   The CSR is saved in a text file on your computer. It is this file that needs to be sent to your certificate provider.

> **Note:**
>
> BMC recommends that you save the CSR in the same folder where you saved the SSL certificate and the private key.

6. Click **Close** to close the window.

Your private key and all required information are now saved on your computer. Now you need to send the saved CSR file to your certificate provider who normally will send you the final certificate in an email that should also contain download links to the root and intermediary certificates required for installing the SSL certificate on BMC Client Management .

> **Note:**
>
> Be aware that it might take quite a while for you to receive the certificate and can thus continue to install it.

Installing the SSL certificate

After you received the certificate you need to install it in BMC Client Management before it can be used for the external integration:

1. Click **Install Certificate** .
   The **Install Certificate** window appears.
2. Enter into the **Give a name to your certificate** field a unique name for the new SSL certificate.
3. To enter the required data into the **Root Certificate** field click **Browse** .
   An **Open** window appears.
4. Select the file that contains the root certificate.
5. Click **Open** .
   The content of the selected file is copied to the respective field.

> **Note:**
>
> You can also enter the required data into these fields by opening the respective files in a text editor and copying their content into the respective fields. For this you need to copy the content from the `----BEGIN CERTIFICATE---` to the `---END CERTIFICATE----` markers.
> Ensure that you copy `----BEGIN CERTIFICATE---` and `---END CERTIFICATE----` too. Some certificate providers might give you the root and intermediate certificates in one file. You can verify if you added the correct certificate after pasting the content and clicking **Details** . A root authority is self-signed. Therefore, the **Issuer** and **Subject** fields must have the same value.

6. Repeat the preceding steps for the **Intermediate Certificates** and **Final Certificate** fields.

> The **Intermediate Certificates** is optional and can remain empty if no **Intermediate Certificates** exists.

7. To display the details of a certificate, for example to verify if the selected certificate is the correct one click **Details** .
   A **Certificate Details** window appears showing the contents of the certificate in readable format.
8. Repeat the preceding steps for the **Private Key** field.

> If you are manually copying the private key you need to copy the content from the `----BEGIN RSA PRIVATE KEY---` to the `---END RSA PRIVATE KEY----` markers, including the markers themselves.

9. If a password was defined for the private key in the certificate request preparation you need to enter it here as well. If not password was defined this field can remain empty.
10. After all data is filled in the **Install Certificates** button becomes available. Click it.
    A **Information** window appears, with the result of the certificate installation. This can either be *The SSL certificate was successfully installed.* or an error message displays detailing the issue causing the error.

The required SSL certificate is now installed and BMC Client Management is ready for integration with BMC Remedyforce.

Adding devices for web services and external integrations

To add a device for use with the external integrations, its web services module must be loaded and configured as follows:

1. Click **Add Device** .
   The **Enable Web Service Module on Selected Device** window appears.
2. Select the desired device from one of the available lists and click **OK** .
   The device is now added to the list of web service enabled devices.
3. To specifically configure the web service for the device select it in the left window pane.
4. Now double-click an entry in the table or click **Properties** .
   The **Properties** window appears.
5. Fill the required information into the respective fields:

Parameter	Description
Web Service Port	Defines the TCP port dedicated to the web services.
Listening Addresses	Comma separated list of local addresses (ipv4 and/or ipv6) on which we will listen. By default, addresses are 0.0.0.0,::, which means listen on all IPV4 and IPV6 addresses.
Trusted Address	Defines a number of IP addresses from which the agent is to accept incoming Web service requests. Trusted addresses may be entered as single IP addresses or in form of address ranges:Dotted notation, for example, 94.24.127.24 or 2001:db8:85a3::8a2e:370:7334CIDR notation, for example, 94.24.127.0/24

Parameter	Description
	or 2001:db8:85a3::8a2e:370:152/896With the short or complete network name such as scotty or scotty.enterprise.comA mixture of both: 94.24.127.24, 2001:db8:85a3::8a2e:370:152/896, scotty.enterprise.com. Several ranges must be separated by a comma (,).

6. Click **OK** to confirm the web service configuration.

Setting up integration with BMC Remedyforce

Defining an integration to BMC Remedyforce allows the administrators to define a number of events for which they want to receive notifications and for which, at the same time, incident tickets are created in BMC Remedyforce that can be followed in that software.

When setting up integration between BMC Client Management and BMC Remedyforce you need to execute some specific configurations for both applications. This paragraph guides you through the necessary steps in BMC Client Management. For information about how to configure BMC Remedyforce for integration refer to section Integrating BMC Remedyforce with BMC Client Management.

The following topics guide you through the setting up external integration with BMC Remedyforce:

- Creating a new external integration to BMC Remedyforce
- Defining external integration for BMC Remedyforce

Creating a new external integration to BMC Remedyforce

To create a new integration with BMC Remedyforce proceed as follows:

1. Select **Edit > Create BMC Remedyforce Integration**  .
   The **Properties** dialog box appears on the screen.
2. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC Remedyforce integration for helpdesk tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called. For example, http://localhost:8080/footprints/servicedesk/ or

Parameter	Description
	:8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress:8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.

3. In the list below check the boxes for all events for which an incident ticket is to be created in BMC Remedyforce .

> You will also receive an event notification by email for each incident ticket that is created.

4. Click **OK** to confirm.

Defining external integration for BMC Remedyforce

You can define the external integration for the following different aims:

- Defining one-way integration
- Defining two-way integration
- Defining event-specific integration

Defining one-way integration

To create a new integration with BMC Remedyforce for one-way-integration, that is, with the aim of only recovering information from BMC Client Management , the administrator needs to be defined via whom the calls are executed:

1. Go to the **Global Settings > External Integration** node.
2. Select **Edit > Create BMC Remedyforce Integration** .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC Remedyforce integration for helpdesk tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.

4. Click **OK** to confirm.

BMC Client Management is now set up for sending alert notifications to BMC Remedyforce and creating incident tickets there, as well as closing tickets in BMC Client Management, once they are resolved in BMC Remedyforce.

Defining two-way integration

To create a new integration with BMC Remedyforce for two-way-integration, that is, with the aim of recovering as well as providing information from/to BMC Client Management, proceed as follows:

1. Go to the **Global Settings > External Integration** node.
2. Select **Edit > Create BMC Remedyforce Integration** .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC Remedyforce integration or BMC FootPrints Service Core integration.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called, for example, http://localhost:8080/footprints/servicedesk/ or :8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress:8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.

4. In the list below check the boxes for all events for which an incident ticket is to be created in BMC Remedyforce .

> You will also receive an event notification by email for each incident ticket that is created.

5. Click **OK** to confirm.

BMC Client Management is now set up for sending alert notifications to BMC Remedyforce and creating incident tickets there, as well as closing tickets in BMC Client Management , once they are resolved in BMC Remedyforce.

Defining event-specific integration

If in the list of all available alerts and events you find that you need integration for a specific alert, you can also set up the external integration for the alert in question directly from this node.

1. Select the event in the table for which a new external integration is to be defined.
2. Select **Edit > Create BMC Remedyforce Integration** .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC Remedyforce integration or BMC FootPrints Service Core integration.
Application Type	The product for which to create the integration. In this case this field is preselected and cannot be modified.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called, for example, http://localhost:8080/footprints/servicedesk/ or:8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress: 8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.

4. In the list below the notification box for the selected event is already pre-checked.

> If required you can check further events for notification for this integration.

5. Click **OK** to confirm.

The new external integration to BMC Remedyforce will immediately created and activated. This means that from now on the administrator will receive a notification whenever this type of event occurs and an incident ticket will automatically be created in BMC Remedyforce.

Setting up integration with BMC FootPrints Service Core

Defining an integration to BMC FootPrints Service Core allows the administrator to receive notifications for a number of events and for which at the same time incident tickets are created in BMC FootPrints Service Core , that can be followed in that software.

When setting up integration between BMC Client Management and BMC FootPrints Service Core you need to execute some specific configurations for both applications. This paragraph guides you through the necessary steps in BMC Client Management. For information about how to configure BMC FootPrints Service Core for integration, see Integrating BMC Client Management with BMC FootPrints Service Core.

The following topics guide you through the setting up external integration with BMC FootPrints Service Cord:

- Creating a New External Integration to BMC FootPrints Service Core
- Defining the external integration for BMC FootPrints Service Core

Creating a New External Integration to BMC FootPrints Service Core

To create a new integration with BMC FootPrints Service Core proceed as follows:

1. Select **Edit > Create BMC FootPrints Service Core Integration**  .
   The **Properties** dialog box appears on the screen.
2. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC FootPrints Service Core integration for helpdesk tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called, for example, http://localhost:8080/footprints/servicedesk/ or :8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress:8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right. In this case all Service Core data is now available.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.
Workspace	Select the Service Core workspace in which to create the alerts. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. Once you select the desired workspace the field below will become available with all its options.
Item Definition	Select the Service Core item definition to which to add the alert. Once you have selected the desired workspace this list is automatically populated with the values available in BMC Footprints Service Core. Once you select the desired workspace the fields below will become available with all their options.

Parameter	Description
Sub-Category	Select the category for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty. This field is optional.
Severity	Select the severity for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty. This field is optional.

3. In the list below check the boxes for all events for which an incident ticket is to be created in BMC FootPrints Service Core .

> The events available for notification are sorted according to their functionality. To access the individual events click the arrow icon to the right of the heading and then check the boxes of the events to activate.

> You will also receive an event notification by email for each incident ticket that is created.

4. If you want to integrate the event into a BMC FootPrints Service Core template select it from the **Item Template:** drop-down list next to the event.

> This field remains dimmed if no item templates are available.

5. Repeat the preceding steps for all different event types.
6. Click **OK** to confirm.

Defining the external integration for BMC FootPrints Service Core

You can define the external integration for the following different aims:

- Defining one-way integration
- Defining two-way integration
- Defining event-specific integration

Defining one-way integration

To create a new integration with the BMC FootPrints Service Core (FPSC) for one-way-integration, that is, with the aim of only recovering information from BMC Client Management, the administrator needs to be defined via whom the calls are executed:

1. Go to the **Global Settings > External Integration** node.

2. Select **Edit > Create BMC FootPrints Service Core Integration**  .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC FootPrints Service Core integration for helpdesk tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.

4. Click **OK** to confirm.

BMC Client Management is now set up for exporting data to BMC FootPrints Service Core.

Defining two-way integration

To create a new integration with Service Core for two-way-integration, that is, with the aim of recovering as well as providing information from/to BMC Client Management, proceed as follows:

1. Go to the **Global Settings > External Integration** node.
2. Select **Edit > Create BMC FootPrints Service Core Integration**  .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC FootPrints Service Core integration for helpdesk tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called, for example, http://localhost:8080/footprints/servicedesk/ or :8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress:8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right. In this case all Service Core data is now available.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.
Workspace	

Parameter	Description
	Select the Service Core workspace in which to create the alerts. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. Once you select the desired workspace the field below will become available with all its options.
Item Definition	Select the Service Core item definition to which to add the alert. Once you have selected the desired workspace this list is automatically populated with the values available in BMC Footprints Service Core. Once you select the desired workspace the fields below will become available with all their options.
Sub-Category	Select the category for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty. This field is optional.
Severity	Select the severity for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty. This field is optional.

4. In the list below check the boxes for all events for which an incident ticket is to be created in BMC FootPrints Service Core.
   The events available for notification are sorted according to their functionality. To access the individual events click the arrow icon to the right of the heading and then check the boxes of the events to activate. You will also receive an event notification by email for each incident ticket that is created.
5. If you want to integrate the event into a BMC FootPrints Service Core template select it from the **Item Template:** drop-down list next to the event.
   This field remains dimmed if no item templates are available.
6. Repeat the preceding steps for all different event types.
7. Click **OK** to confirm.

BMC Client Management is now set up for exporting data to BMC FootPrints Service Core and creating incident tickets there, as well as closing tickets in BMC Client Management , once they are resolved in Service Core.

Defining event-specific integration

If in the list of all available alerts and events you find that you need integration for a specific alert, you can also set up the external integration for the alert in question directly from this node.

1. Select the event in the table for which a new external integration is to be defined.
2. Select **Edit > Create BMC FootPrints Service Core Integration** .
   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example, BMC Remedyforce integration or BMC FootPrints Service Core integration.
Application Type	The product for which to create the integration. In this case this field is preselected and cannot be modified.

Parameter	Description
Integration Administrator	Specify the administrator for whom the integration is created by clicking the Select Administrator icon to the right.
Application Login	Enter the name of the administrator for which the integration is created. Be aware that the administrator must be a valid Service Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services is called, for example, http://localhost:8080/footprints/servicedesk/ or :8080/footprints/servicedesk/" class="external-link" rel="nofollow">https://ServiceCoreServerIpAddress:8080/footprints/servicedesk/. To verify that the entered link is valid click the Check Connection button to the right.
Language	Select the language in which the incidents is created in the application. All Console languages are available for this choice.
Sub-Category	Select the category for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty.
Severity	Select the severity for the alert. If you have verfied the connection this list should have been automatically populated with the values available in BMC Footprints Service Core. If none of the available values are appropriate leave the field empty.

4. In the list below the notification box for the selected event is already pre-checked.
   If required you can check further events for notification for this integration.
5. If you want to integrate the event into a BMC FootPrints Service Core template select it from the **Item Template:** drop-down list next to the event.
   This field remains dimmed if no item templates are available.
6. Click **OK** to confirm.

The new external integration to Service Core will immediately created and activated. This means that from now on the administrator will receive a notification whenever this type of event occurs and an incident ticket will automatically be created in Service Core .

Tracking shared events

BMC Client Management administrators can track all events that are shared with other software products via the **Alerts and Events** node. All events that are available for external integration are part of the **Alert & Event** event log model.

This view provides the following selection options which can be combined for the display. When opened the table of this node is empty. To launch the display click **Find** :

Parameter	Description
Model Name	Select from this list the type of event log model for which to display the logged events, for this case you always need to select the **Alert & Event** option.
Status	Select in this field the status value for which the logged events are to be displayed.

Parameter	Description
Start Date	Select in this field the date from which on the logged events are to be displayed.
End Date	Select in this field the date up to which the logged events are to be displayed.

The table displays the following information for all alerts and events that are shared and tracked with other applications.

Alert & Event

The **Alert & Event** model logs agent operation events, such as events and alerts generated by operational rules, by the inventory module, security alerts, and so on. It shows the following information for each event:

Parameter	Description
Device Name	This column is not displayed under the **Alerts and Events** of a device.
Event Date	The date and time the alert occurred in the default time format.
Status	An event is closed either automatically by the BMC Client Management master, because an automatic solution was applied and the agent found the device to be now compliant. If this automatic solution is not possible the alert can only be closed manually from the target application after it was manually resolved.
Severity	Defines the severity of the selected alert, **Error, Information** or **Warning** .
Category	Defines the type of event that is being logged.
Sub-category	The alert sub-category to which the alert/event was assigned. This value can be freely defined by the administrator.
Description	Displays the textual description of the alert/event.
Shared	Indicates if this alert is shared with other applications such as BMC Remedyforce or BMC FootPrints Service Core via the external integration. It only appears after the ticket was actually created in the target integration.
Acknowledged by	The name of the administrator who acknowledged the event.
Last Modified By	Displays the name of either the last person that last modified the object or its contents, such as the administrator, or it may be the system that last executed any modifications.
Notes	This free text field can contain additional information concerning the selected object.

Filtering alerts and events

This view always only shows the alerts and events logged for a specific event log model. To display the events and alerts of another model or to further limit the displayed list to those of a specific status or timeframe, proceed as follows:

1. Select the desired event log model from the **Model Name** drop-down box.

> To filter for a specific status of the current model do not modify this selection.

2. You can further filter the alerts and events of the selected model according to the following criteria:
   - Select a specific status value from the **Status** drop-down box to display only alerts /events of a specific status type.
   - To filter for events of a specific timeframe select the start and end date of the desired timeframe in the calendar boxes.

   > You can use only one criteria for filtering or you can use a combination of them.

3. Click **Find** .

The table will refresh and display only those alerts/events that comply with the selected criteria.

Acknowledging alerts

After you access the **Alerts and Events** node the alert icon in the status bar disappears. However the status of the alerts themselves has not yet changed. To acknowledge specific alerts, proceed as follows:

1. Mark the alerts to be acknowledged in the table in the right window pane.
2. Select **Edit > Acknowledge Alerts** .
   A confirmation windowdisplays.
3. Select **Yes** to confirm and proceed with the action.

The status of the selected alerts will now be changed from `Unnotified Alerts` to `Acknowledged Alerts` .

Purging alerts and events

Alerts and events can be purged. Be careful when using this operation, ALL alerts and events of this event log model for the current device/device group will be irrevocably deleted from the database.

1. Click **Purge** .
   A confirmation window appears.
2. Click **Yes** to confirm.
   Another confirmation window appears if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce or BMC FootPrints Service Core .
3. If the incident tickets that were created in BMC Remedyforce should be closed at the same time click **Yes** , otherwise click **No** .

All alerts and events will be deleted from the database and, if requested, the status of the connected incident ticket(s) in BMC Remedyforce or BMC FootPrints Service Core will be changed to `Closed` .

Deleting individual alerts and events

It is possible to delete individual alerts and events that are no longer required.

1. Select the alert(s)/event(s) to delete in the table to the right.
2. Click **Edit > Delete** .
   A confirmation window appears.
3. Click **Yes** to confirm.
   Another confirmation window appears if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce .
4. If the incident tickets that were created in BMC Remedyforce should be closed at the same time click **Yes** , otherwise click **No** .

All selected alerts and events will be deleted from the database and, if requested, the status of the connected incident ticket(s) in BMC Remedyforce will be changed to `Closed` .

Events defined for notification

The following events are defined for notification:

- BMC Client Management Application
- Discovery and Inventory
- Applications and Application Licensing
- Compliance
- Agent-based Monitoring

BMC Client Management Application

The events and alerts of this section are concerned with the general workings of the BMC Client Management agents and licensing problems.

Parameter	
Error detected on BCM Agent	The agent on a client or relay has a problem executing correctly or has stopped working. The alert is automatically closed once the agent is executing again properly.
Error detected on BCM Master	The agent on the master has a problem executing correctly or has stopped working. The alert is automatically closed once the agent is executing again properly.
BMC Client Management license expired	A BMC Client Management license that you have purchased passed its expiry date. The alert is automatically closed once the respective license is valid again.
BMC Client Management license exceeded	A BMC Client Management license that you have purchased exceeds its number of allowed objects created in the database. The alert is automatically closed once the respective license is valid again.

Discovery and Inventory

The events and alerts of this section are concerned with the individual devices in the network and their agent and connection status.

Parameter	
New device without agent discovered	A new device on which no BMC Client Management agent is installed was discovered in your network.
A computer or device lost contact	A device in your network has lost contact with its parent or is in general not reachable. The alert is automatically closed once the device is contactable again.

Applications and Application Licensing

The events and alerts of this section are concerned with application license monitoring and prohibited managed applications.

Parameter	
Software license count maximum exceeded	An application is newly installed on a device but there are no more licenses for it available. The alert is automatically closed once the respective application license is valid again, that is, additional licenses are purchased or the application is removed from the device.
Software license expiration date exceeded	An application with a time license is found on at least one device in your network of which the final license date has expired. The alert is automatically closed once the respective application license is valid again.
Underinstalled licensed software	An application is found for which there are still licenses available, that is it can still be installed on more devices. The alert is automatically closed once all available licenses of the application are installed.
Software license count threshold exceeded	The installed application base approaches the specified threshold at which notification is required. For example, if 100 licenses are available and the threshold is set to 80%, an alert is generated when the application is installed for the 80th time. This might be the time to consider purchasing additional licenses. The alert is automatically closed once the installed application base falls below the respective application license threshold again, that is, additional licenses are purchased or applications are uninstalled, for example, from devices on which they are no longer required.
A prohibited application was started	An application is started on a device on which its execution is prohibited.

Compliance

The events and alerts of this section are concerned with compliance.

Parameter	
All Defined Custom Compliance Alerts	An alert that was defined for device compliance is generated. Many of these alerts can be closed automatically once the criterion that caused the alert on the device matches its requirements. For more information about the available alerts and how to define them refer to the *BMC Compliance Manager* manual.

Agent-based Monitoring

In this section you can select which operations rule steps are to send event notifications when they are generating alerts.

Parameter	
Check URL Availability	The step finds that the URL that it verified is not reachable. Once the step finds the URL reachable again the alert is closed automatically. If the URL in the step is changed, the first alert is closed automatically and a new alert is generated if the new URL is not reachable either.
Check Windows Events	The step finds a Windows event entry that contains either the specified string or has the specified event ID.
Check Running Process	The step either does not find the specified process or could not terminate it, if this was requested. The alert is automatically closed once the process can be found (and terminated).
Advanced Process Execution Check	The step does not find the specified process. The alert is automatically closed once the process can be found.
Generate Custom Alert	A custom alert is generated by the step.
File Analysis via Regular Expression	The step finds a match for the specified regular expression in the listed files.
Check Installed Software	The step does not find the specified software installed on the target. The alert is automatically closed once the specified software is found installed on the target.
Advanced Installed Software Check	The step does not find the specified software installed on the target. The alert is automatically closed once the specified software is found intalled on the target.
Service Execution Check	The step finds that a process that it has verified is not running. The alert is automatically closed once the specified service is found executing.
Low Disk Space	The step finds that the free disk space has fallen under the defined percentage limit on the target device. The alert is automatically closed once the step finds enough free disk space.
Check Disk Space	The step finds that there is less free disk space on the target device than defined in the step. The alert is automatically closed once the step finds enough free disk space.
The total size of the memory has changed	The total size of the memory on a specified device has changed.

Setting up integration with Remedy with Smart IT to automate incident generation

Integrating Remedy with Smart IT with BMC Client Management (BCM) enables administrators to automate incident generation in Remedy with Smart IT based on events defined in BCM. An event in BCM is a significant action or occurrence in a system or application that needs to be reported to

administrators. When an event occurs that administrators need to know about, an alert is generated in BCM console. Such alerts cause Remedy with Smart IT to automatically generate incidents and notify administrators about these incidents. An i ncident is a type of ticket that is generated in Remedy with Smart IT.

For example, a Remedy with Smart IT administrator can subscribe to an event when an error happens on BCM agent. When this event occurs, BCM generates an alert which causes a new incident to be created in the Remedy with Smart IT application. The application notifies Smart IT service desk technicians about these incidents.

It is a two-way integration between BCM and Remedy with Smart IT applications.

This section lists the necessary steps required to integrate Smart IT in BCM.

Before you begin

As a BCM administrator who is integrating BCM with Remedy with Smart IT, you need to have the following information:

- Login credentials of the Remedy with Smart IT administrator
- Remedy with Smart IT server URL to integrate with BCM
- Identify notification events that the Remedy with Smart IT administrator wants to monitor in BCM

Identifying events for monitoring assets in BCM

If you are a Smart IT administrator for your organization, you need to identify events that can be monitored by BCM. To identify events that can be monitored by BCM, see Events defined for notification.

Request a BCM administrator to define these events when integrating these applications.

Creating an integration with Remedy with Smart IT

To create a new integration with Remedy with Smart IT:

1. From the BCM console, select **Global Settings** > right-click **External Integration** > **Create Integration**.
2. In the BMC Integration wizard, enter data into the following fields:

Parameter	Description
Instance Name	Enter a name to identify the integration. For example, ***Remedy with Smart IT integration***.
Application Type	Select **Remedy with Smart IT**.
User name	Enter a valid Remedy with Smart IT administrator name.
Password	Enter the administrator password.
Application URL	Enter the URL to access the Remedy with Smart IT web server. `http://<midtier_server>:<port>/arsys/services/ARService?server=<servername>` To verify that the URL is valid, click **Check Connection**.
Language	Select the language in which incidents will be created. All console languages are available.

> **Note**
>
> If **Check Connection** action fails, BCM cannot integrate with Remedy with Smart IT and the **Next** button is not enabled.

3. Click **Next** to view the **Event Subscriptions** window.
4. From the available event types, click an event type and select alert notifications for which you want an incident ticket to be created in the Remedy with Smart IT application.

> You will receive an event notification by email for each incident ticket that is created in Remedy with Smart IT.

5. Repeat step 4 to change alert notifications.
6. Click **Finish**.

After you integrate BCM with Remedy with Smart IT, the integration details are populated as a new integration link in **Global Settings** > **External Integration**.

Results

The integration results in one of the following possibilities:

- A successful integration is created under the **Global Settings** > **External Integration**.
- Connection tests do not pass because of incorrect web server URL, incorrect URL syntax, incorrect server names. Contact the Remedy with Smart IT administrator.

- Cannot complete integration because Remedy with Smart IT administrator credentials is incorrect. Contact the Remedy with Smart IT administrator.
- An integration is created without enabling any notification events for BCM.

Tracking notification events and alerts in BCM

BCM administrators can track all the events and alerts generated for other products. For example, if you subscribe to an event that detects an error on BCM agent, the **Alerts and Events** window in the BCM console captures the alert generated for this event. For more information on tracking events and alerts, see Tracking shared events.

Updating notification events in BCM

Events are classified into different functional areas managed by BMC Client Management, such as **BCM Application**, **Discovery and Inventory**, **Applications and Application Licensing**, **Compliance**, and **Agent-based Monitoring**. Based on your organization needs, you can change notifications.

To update notification events:

1. On the console menu, select **Global Settings** > **External Integration** > ***Remedy with Smart IT integration***.
2. On the **Notification Events** tab, double-click an event to open the **Event Subscriptions** window.
3. Select new or clear existing notification events.
4. Click **Finish**. The **Notification Events** tab refreshes to show latest updates.

Creating an assignment record in Remedy ITSM

As a Remedy with Smart IT administrator, you must ensure that an assignment record is created in Remedy with ITSM. Also ensure that auto-assignments are configured so that the system automatically assigns records, such as problem investigations or change requests, to the appropriate support group.

For more information, see

Creating assignments

Assigning requests with the Assignment Engine

Troubleshooting

The following table lists possible issues when integrating with Remedy with Smart IT.

Issue	Cause(s)	Solution(s)
Cannot connect to Remedy with Smart IT server	• The URL to access Remedy with Smart IT is incorrect. • The server instance cannot be accessed. • The server is down.	Possible solutions: • If the URL is incorrect, ensure that URL follows this format, `http://<midtier_server>:<port>/arsys/services/ARService?server=<servername>`

Issue	Cause(s)	Solution(s)
	• The user name and or password is incorrect.	• If the server instance cannot be accessed or credentials are incorrect, check with Remedy with Smart IT administrator.
Incidents are not generated in Remedy with Smart IT	• Notification events are not defined in BCM • Assignment configuration and auto-assignments are not configured correctly in Remedy with ITSM	• Contact BCM administrator to verify whether the required notification events are defined in BCM. • Contact a Remedy with ITSM or Smart IT administrator to verify whether ITSM is configured to automatically generate inicidents in Remedy with Smart IT
Cannot integrate BCM with Remedy with Smart IT	• Integration issues in BCM	• Review the **mtxagent.log** file that can be accessed from `C:\Program Files\BMC Software\Client Management\Master\log`

Where to go from here

When setting up an integration between BCM and Remedy with Smart IT, you need to configure both the applications. As a Smart IT administrator or a Smart IT service desk technician, you need to perform specific configurations in Remedy with Smart IT. For more information on integration steps on Smart IT, see Integrating Smart IT with BMC Client Management: 1.5.01 and later

Related topics

Integrating with BMC ITSM applications

Resolving tickets with the help of Client Management actions: 1.5.01 and later

Integrating with BMC Atrium CMDB

BMC Client Management discovers hardware and software inventory of desktops and maintains in its database, whereas BMC Atrium CMDB is a configuration management database (CMDB) used by enterprise IT organizations to document, store, and manage details of the configuration items (CI) in their IT infrastructure.

BMC Client Management - BMC Atrium CMDB integration allows you to retrieve data from the BMC Client Management database, transform it into data in the format required by the Atrium CMDB , and finally insert this data into the Atrium database. Now the data discovered by BMC Client Management is ready to be used by other BMC applications which share the Atrium CMDB data.

The following video (4:28) describes the steps to integrate BMC Client Management with BMC Atrium CMDB.

https://youtu.be/73QhTxOik0s

For the complete list of components added during BMC Client Management - BMC Atrium CMDB Integration installation, see topic Components Installed during Installation.

This topic includes:

- Supported Versions
- Atrium Installation
- Configuring the SQL database for Atrium CMDB integration
- Filters
- Working with the Integration Maintenance Tool

Supported Versions

The BMC Client Management - BMC Atrium CMDB Integration version 1.6.00 supports:

- BMC Client Management version 12.1 and later
- Footprints Asset Core version 11.7 (requires specific updates, see BMC Client Management version 11.7 and version 12.0 installation prerequisites for more information)
- BMC Client Management version 12.0 (requires specific updates, see BMC Client Management version 11.7 and version 12.0 installation prerequisites for more information)
- BMC Atrium CMDB version 9, 9.0.1, and 9.1
- BMC Remedy AR System version 9, 9.0.1, and 9.1
- BMC Atrium Integrator version 9, 9.0.1, and 9.1
- BMC Atrium CMDB version 8.x
- BMC Remedy AR System version 8.x
- BMC Atrium Integrator version 8.x
- BMC Atrium CMDB version 7.6.04 SP5 and later
- BMC Remedy AR System version 7.6.04 SP5 and later
- BMC Atrium Integrator version 7.6.04 SP5 and later

Atrium Installation

This section describes the system requirements and prerequisites and provides worksheets that you can use to gather the information needed to install the BMC Client Management - BMC Atrium CMDB Integration. The following topics are available:

- Downloading the Installer
- Installation Prerequisites
- User Permissions
- Installation Worksheet
- Installing BMC Client Management - BMC Atrium CMDB Integration
- Components Installed during Installation
- BMC Atrium CMDB - BMC Client Management class mapping

Downloading the Installer

The BMC Client Management - BMC Atrium CMDB Integration installer version 1.6.00 is available for download from the BMC Electronic Product Distribution (EPD) website.

You can access this website at http://webapps.bmc.com/epd . To use the website, you need the user name and password that you obtained when you registered and subscribed to Customer Support. To subscribe, you must have a valid Support Contract ID. If you do not know your Support Contract ID, contact customer_care@bmc.com.

If you do not have a current license for the product, contact your BMC sales representative or your local BMC office or agent. If you cannot download the product, you can request a physical kit.

1. Create a directory to save the downloaded files to.

   > On Microsoft Windows computers, ensure that the directory is only one level into the directory structure. The EPD package creates a directory in the temporary directory when you extract the files, and the directory that contains the installation image should not be in a directory deeper than two levels into the directory structure.

2. Go to https://webapps.bmc.com/signon/content/logon.jsp .
3. Enter your user ID and password, and click **Submit** .
4. Click **Download Product** .
5. On the **Export Compliance and Access Terms** page, provide the required information, agree to the terms of the agreements, and click **Continue** .
6. If you are accessing this site for the first time, create an EPD profile; otherwise continue directly with the next step:
   a. Under **Localized Languages** , select the language for the product.
   b. Under **Install Platforms** , select the platforms to download for the product.
   c. Click **Save Profile** .
7. Verify that the correct profile displays for your download purpose, and select the **Licensed Products** tab.
8. Locate the product:
   a. Locate the product name and expand its entries to show the available version numbers. For example, to download the BMC Client Management - BMC Atrium CMDB Integration installer, select BMC Client Management .
   b. Expand the version number to show the available versions.
   c. Select the check boxes next to the products and documents to download.
9. To download the selected items, click **Download (FTP)** or **Download Manager** :
   - **Download (FTP)** places the selected items in an FTP directory, and the credentials and FTP instructions are sent to you in an email message.

- **Download Manager** enables you to download multiple files consecutively and to resume an interrupted download if the connection drops. This method requires a one-time installation of the AkamiNetSession Client program on the target computer and is usually the faster and more reliable way to transfer files. A checksum logic is used to verify file integrity automatically.

Installation Prerequisites

This section provides information about how to plan for your installation and prepare your environment before the installation. The topic includes:

- Linux Installation Prerequisites for Atrium CMDB Version 8.0 and later
- Linux Installation Prerequisites for Atrium CMDB Version 7.6.04 SP5 and later
- Client Management version 11.7 and version 12.0 installation prerequisites
- Java Runtime Environment Prerequisites
- Client Management SQL Server Windows Authentication Prerequisites

> **Note:**
>
> On both Windows and Linux systems, the files and folders extracted from the downloaded archive should not be renamed or modified.
>
> The installer for the Atrium CMDB / BMC Client Management integration components should be run on the system where Atrium CMDB is installed.

Linux Installation Prerequisites for Atrium CMDB Version 8.0 and later

In order to install the Atrium CMDB components on a Linux system, the following prerequisites must be met:

- The system where the integration component must have a GUI installed.
- All files and folders provided with the installer must be marked as executable. From the directory where the installation files were extracted to, run `chmod -R +x *` to mark the files as executable.
- The `BMC_AR_SYSTEM_HOME` environment variable must be set to the location where the `AR System` is installed. This can usually be set by running `export BMC_AR_SYSTEM_HOME=/opt/bmc/ARSystem` (this example assumes that the `AR System` is installed in `/opt/bmc/ARSystem`) .

Linux Installation Prerequisites for Atrium CMDB Version 7.6.04 SP5 and later

In order to install the Atrium CMDB components on a Linux system, the following prerequisites must be met:

- The system where the integration component must have a GUI installed.

- Ensure that you provided execution rights to the installer folder, all its subfolders, and files. All files and folders provided with the installer must be marked as executable. From the directory where the installation files were extracted to, run `chmod -R +x *` to mark the files as executable.
- Ensure that you set the environment variable for the installed location of BMC Atrium Integrator, `export ATRIUMINTEGRATOR_HOME=/opt/bmc/AtriumIntegrator` .

Client Management version 11.7 and version 12.0 installation prerequisites

To make sure your installation will also work with future versions of Client Management , you need to upgrade the database your current Client Management installation with the respective script, which is provided separately to the installer:

- Oracle database: Atriumviews.sql.oracle
- SQL Server database: Atriumviews.sql.sqlserver
- PostgreSQL database: Atriumviews.sql.postgresql

To execute the script proceed as follows:

1. Copy the script in the `<InstallDir/master/data/Vision64Database/sql>` directory.
2. Stop your master.
3. Open the `Vision64Database.ini` file in the `<InstallDir/master/config>` directory.
4. Find the section `SqlRunOnce` .
5. Below the explanation enter the name of the script corresponding to your database type preceded by the relative path, for example:
   `name=../data/Vision64Database/sql/Atriumviews.sql.oracle`

```
[SqlRunOnce]

; List of SQL scripts to run once at startup time. After being executed, each
; line is re-written with a ';' prefix to disable it in the future. The order
; of file execution is as listed.
name=../data/Vision64Database/sql/Atriumviews.sql.oracle


[SqlRun]
```

6. Start the master.
   The script is executed and creates all required new tablespaces.

Java Runtime Environment Prerequisites

Depending on your BMC Atrium CMDB version, the following Java Runtime Environment (JRE) must be set as default JRE verseion:

- BMC Atrium CMDB 9 or earlier: Java 1.7.0_55 or later
- BMC Atrium CMDB 9.0.1 or later: Java 1.8.0_45 or later

Client Management SQL Server Windows Authentication Prerequisites

BMC Atrium Integrator 1.6 installer uses Java Database Connectivity (JDBC) driver to connect to a relational database management system (RDBMS). To handle the Windows Authentication, the SQL Server JDBC driver must be available in the Java Runtime Environment (JRE) installation folder.

The following are the prerequisites for using Windows Authentication:

- BMC Atrium CMDB 8 or later (with Pentaho 4.x or later)
- JDBC driver installed in JRE installation directory

> **Note**
>
> Download a version of the JDBC driver that is compatible with the JRE and SQL Server versions. If you have multiple versions of JRE, ensure that you have copied the JDBC driver in the correct JRE folder.

To install JDBC driver, download the JDBC driver file (*sqljdbc_4.0.2206.100_enu.exe* in this example), extract it locally, and copy the files as the following example for SQL server 2012 and 2014:

- Copy *Microsoft JDBC Driver 4.0 for SQL Server**sqljdbc_4.0**enu**sqljdbc4.jar* to *<JRE Path>**lib**ext* directory
- Copy \ *Microsoft JDBC Driver 4.0 for SQL Server**sqljdbc_4.0**enu**auth**x64 (or x86 depending on you JRE version)*\ *sqljdbc_auth.dll* to *<JRE Path>**bin* directory
  where, `<JRE Path>` is your JRE installation directory (for example, *C:**Program Files (x86)**Java*).

> **Note**
>
> For using Windows Authentication, the SQL Server port value is mandatory.

User Permissions

When you run the installation program, you must be logged on to the destination computer as the administrator or as a user with administrator rights and permissions.

Installation Worksheet

Before installing the BMC Client Management - BMC Atrium CMDB Integration , you must gather the parameter information that the installer requires for each product. This section has a worksheet you can use to do so to complete the installation process. To avoid installation errors, print the worksheet, fill it in with the relevant information, and refer to it during the installation.

The following sections are provided:

- Directory selection
- BMC Client Management connection validation settings
- BMC Remedy AR System user inputs

Directory selection

Panel name and setting	Default value and notes	Your value
Destination Directory	Default value: • Windows: **C:\Program Files\BMC Software\BCMCMDBIntegration** • Linux: **/opt/bmc/BCMCMDBIntegration** **Note** If you are reinstalling the Atrium Integrator, the installation directory selected during the last installation is displayed as default destination directory. However, you can select a different directory.	

BMC Client Management connection validation settings

Panel name and setting	Default value and notes	Your value
Database Type	Supported database types: • SQL Server (selected by default) • Oracle • PostgreSQL	
Authentication	• SQL Server Authentication (selected by default) • Windows Authentication	
Database Server or IP	The SQL Server name IP or DNS name including SQL Server\Instance name	
System Administrator User		
System Administrator Password		
Database Name/Service	If you used the default values for the Client Management installation, this is **bcmdb**.	
Database Port	Dafault database ports: • SQL Server (1433) • Oracle (1521) • PostgreSQL (5432) **Notes**	

Panel name and setting	Default value and notes	Your value
	• Leave as is if you are using an instance name for SQL Server. • For using Windows Authentication, database port is mandatory.	
Database Owner	If you used the default values for the Client Management installation, this is **bcmdbuser** .	

BMC Remedy AR System user inputs

Panel name and setting	Default value and notes	Your value
AR System Server Administrator Name		
AR System Server Administrator Password		
AR System Server TCP Port	Default value: 0 **Note** Note: A value of 0 indicates use of the port mapper service. If a fixed port is being used, specify the port number.	
AR System Server Name Alias	The name of the computer on which Atrium is installed.	

Installing BMC Client Management - BMC Atrium CMDB Integration

The following section provides information about installing BMC Client Management:

- Windows Installation
- Linux Installation
- Installing BMC Client Management

Note

On both Windows and Linux systems, the files and folders extracted from the downloaded archive should not be renamed or modified.

The installer for the Atrium CMDB / BMC Client Management integration components should be run on the system where Atrium CMDB is installed.

Windows Installation

On Windows systems, the installation is started by running the `setup.exe` file provided with the installer. You are then presented with on-screen instructions to complete the installation.

> **Note:**
>
> Be aware, that the installer does not support network paths. To launch it remotely you must map the network drive.

Linux Installation

Once all prerequisites listed under Linux Installation Prerequisites are met, start the installation by executing the `setup.bin` script. The installation script launches a GUI, which will walk you through the installation process.

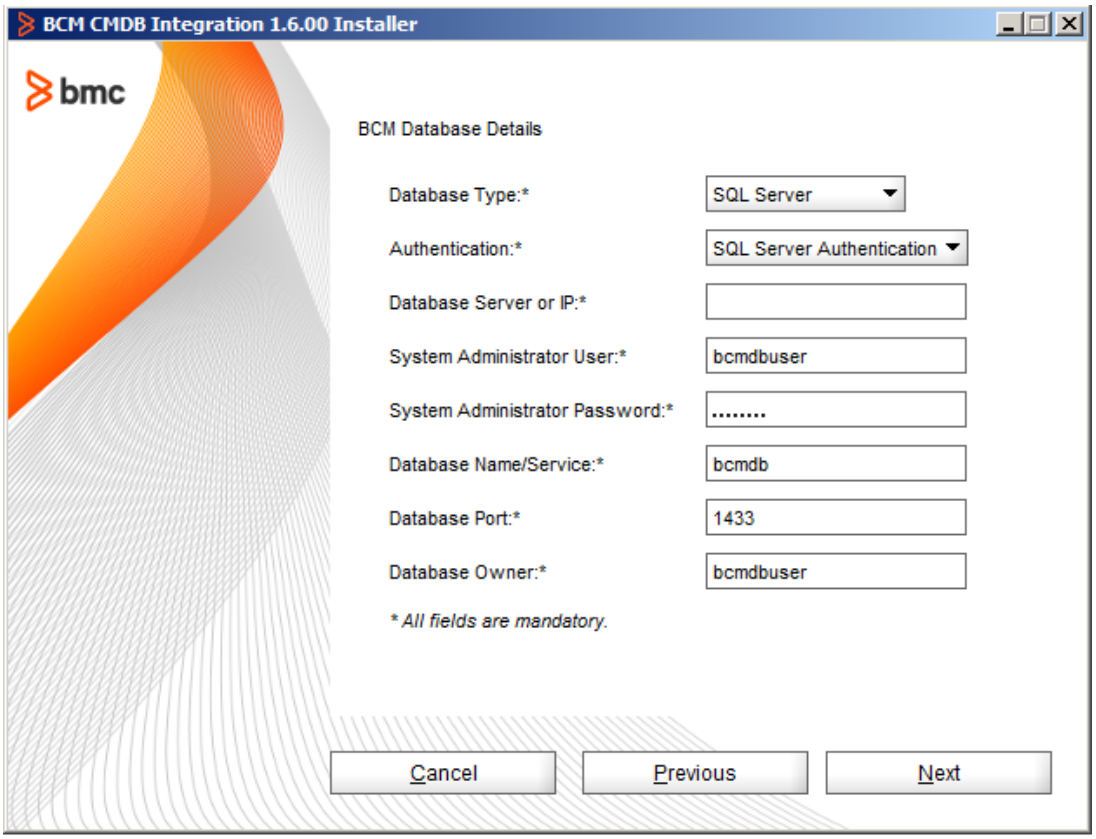
Installing BMC Client Management

1. On the **Welcome** page, click **Next** .
2. Review the license agreement, select **I agree to the terms of license agreement** , and then click **Next** .
3. On the **Directory Selection** page, navigate to the directory in which you want to install the BMC Client Management - BMC Atrium CMDB Integration software.

   > The default location is:
   > - Windows: **C:\Program Files\BMC Software\BCMCMDBIntegration**
   > - Linux: **/opt/bmc/BCMCMDBIntegration**

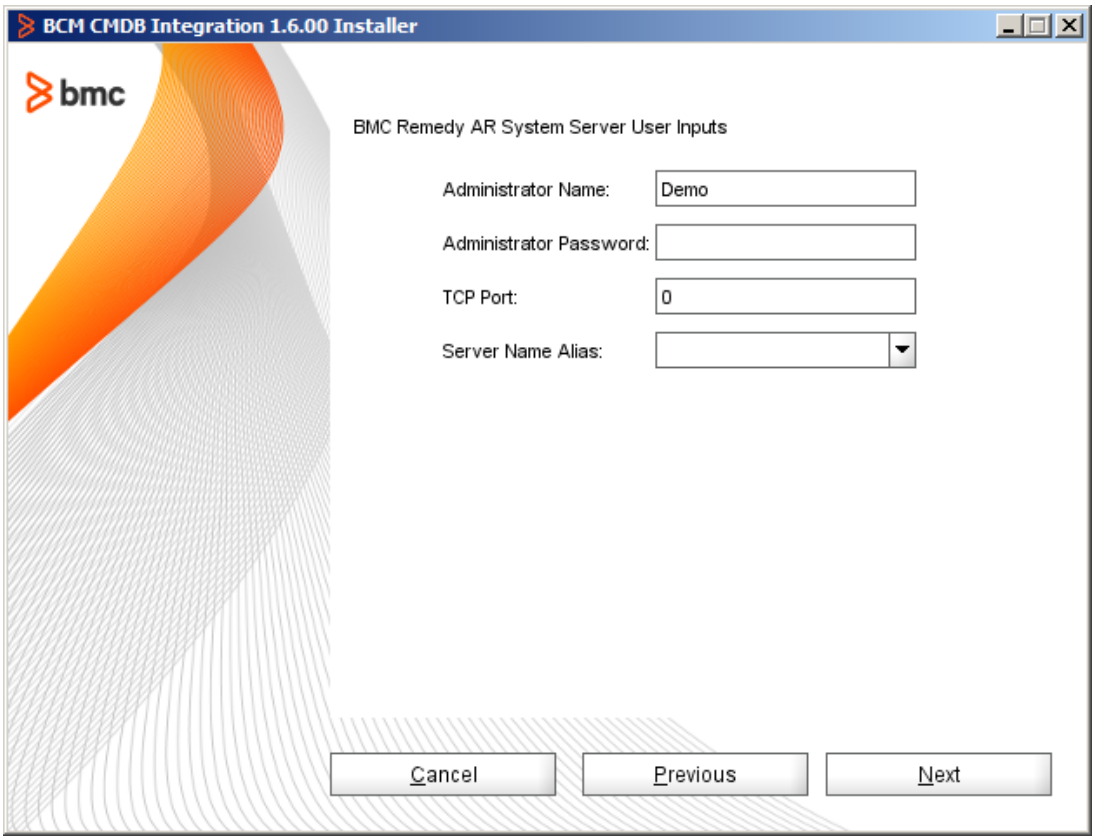
4. Click **Next** .
5. On **BCM Database Details** page, specify the database type and server, the system administrator user and password, and the database name and port on which the BMC Client Management database is listening.

   > The database owner will be configured in the **BCMConfig.properties** file and is used for the transformations. This field is applicable only to SQL Server and is mandatory.



6. Click **Next** .
7. On the **BMC Remedy AR System User Inputs** page, specify the AR System Server Administrator user credentials, AR System Server TCP Port, and AR System Server Name Alias.

> The default AR System Server TCP Port is 0. A value of 0 indicates use of the port mapper service. If a fixed port is being used, specify the port number.



8. Click **Next** .
9. On the **Installation Preview** page, click **Install** .
10. On the **Installation Summary** page, click **View Log** to review any messages.
11. Click **Done** to exit the installer.

Components Installed during Installation

The following components are installed by the BMC Client Management - BMC Atrium CMDB Integration installation:

Component	Description
Dataset	`BMC.FP.ASSETCORE` dataset is created in the BMC Atrium CMDB .
FPIntegrationID	The `FPIntegrationID` attribute is added to the `BMC_BaseElement` class.
Config File	The **BCMConfig.properties** file is created in the **<InstallDir>\bcmcmdbintegration\config** directory.
Logs folder	Installation logs are created in the `<InstallDir>\Logs` folder.
Atrium Integrator jobs	Atrium Integrator jobs are imported into the Atrium Integrator repository in the `BCM_1_6` folder.
KJBs	Atrium Integrator jobs are imported into the Atrium Integrator repository in the `BCM_1_6` folder. Four Jobs are created: • `BCM_Hardware_Input` to insert/update Hardware Inventory • `BCM_Hardware_Delete` to delete Hardware Inventory • `BCM_Software_Input` to insert/update Software Inventory • `BCM_Software_Delete` to delete Software Inventory

KTRs	KTRs are imported into the Atrium Integrator repository in the `BCM_1_6` folder.
BMC Client Management connection	KTRs are updated with the proper BMC Client Management database connection details.
CMDB database connection	KTRs are updated with Atrium CMDB database connection details.
Normalization Engine jobs	NE jobs are created in the BMC Atrium Core CMDB.
Reconciliation Engine jobs	RE jobs are created in the BMC Atrium Core CMDB.

BMC Atrium CMDB - BMC Client Management class mapping

This topic lists mapping between BMC Atrium CMDB and BMC Client Management classes. It also lists the BMC Atrium CMDB class attributes and corresponding BMC Client Management stream fields for each class.

The following class mapping is available:

- BMC_ComputerSystem : BCM_Software_ComputerSystem
- BMC_Product : BCM_Software_Product
- BMC_ComputerSystem : BCM_Hardware_ComputerSystem
- BMC_Processor : BCM_Hardware_Processor
- BMC_OperatingSystem : BCM_Hardware_OperatingSystem
- BMC_IPEndpoint : BCM_Hardware_IPendpoint

BMC_ComputerSystem : BCM_Software_ComputerSystem

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	DeviceName
Description	Description
ShortDescription	ShortDescription
ManufacturerName	ManufacturerName
Model	ModelName
SerialNumber	SerialNumber
Domain	Domain
HostName	HostName
TotalPhysicalMemory	PhysicalMemory
isVirtual	isVirtual
OwnerName	PrimaryUserLogin
CITag	AssetTag
TokenId	GenTokenID (Generated Token ID)

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Category	Category (depending on the BCM Device type)
Type	Type (depending on the BCM Device type)
Item	Item (depending on the BCM Device type)
NameFormat	NameFormat
VirtualSystemType	GenVirtualSystemType (Generated from BCM VirtualSystemType value to fit BMC Atrium CMDB)
PrimaryCapability	PrimaryCapability
CapabilityList	PrimaryCapability

BMC_Product : BCM_Software_Product

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	Name
ManufacturerName	ManufacturerName
Model	Model
MarketVersion	MarketVersion
VersionNumber	VersionNumber
Category	"Software"
Type	"Software Application/System"
Item	"BMC Discovered"
NameFormat	"ProductName"

BMC_ComputerSystem : BCM_Hardware_ComputerSystem

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	DeviceName
Description	Description
ShortDescription	ShortDescription
ManufacturerName	ManufacturerName
Model	ModelName
SerialNumber	SerialNumber
Domain	Domain
HostName	HostName
TotalPhysicalMemory	PhysicalMemory

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
isVirtual	isVirtual
OwnerName	PrimaryUserLogin
CITag	AssetTag
TokenId	GenTokenID (Generated Token ID)
Category	Category (depending on the BCM Device type)
Type	Type (depending on the BCM Device type)
Item	Item (depending on the BCM Device type)
NameFormat	NameFormat
VirtualSystemType	GenVirtualSystemType (Generated from BCM VirtualSystemType value to fit BMC Atrium CMDB)
PrimaryCapability	PrimaryCapability
CapabilityList	PrimaryCapability

BMC_Processor : BCM_Hardware_Processor

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	InstanceName
Description	Description
ShortDescription	ShortDescription
ManufacturerName	ManufacturerName
FPAssemblyId	DeviceID
Category	"Hardware"
Type	"Component"
Item	"CPU"
NumberOfLogicalProcessors	NumberOfLogicalProcessors
MaxClockSpeed	MaxClockSpeed
NameFormat	"ProcessorName"
ProcessorFamily	GenProcessorFamily (Generated processor family to fit CMDB; default **Other**)

BMC_OperatingSystem : BCM_Hardware_OperatingSystem

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	OSName

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Description	Description
ShortDescription	ShortDescription
ServicePack	ServicePack
VersionNumber	VersionNumber
BuildNumber	BuildNumber
FPAssemblyId	DeviceID
Category	"Software"
Type	"Operating system software"
Item	"Operating system"
NameFormat	"OSName"

BMC_IPEndpoint : BCM_Hardware_IPendpoint

BMC Atrium CMDB Class Attribute	BMC Client Management Stream Field
Name	IPAddress
NameFormat	"IP"
Address	IPAddress
ShortDescription	ShortDescription
FPAssemblyId	DeviceID
Category	"Network"
Type	"Address"
Item	"IP Address"

Configuring the SQL database for Atrium CMDB integration

The configuration for the integration component is stored in a file named **BCMConfig.properties**, and an example configuration file is included in the `<InstallDirectory>\bcncmdbintegration\config` folder.

If your BMC Client Management database resides on a Microsoft SQL server, some database specific configuration will be required. Follow the ensuing steps to add this configuration to the **BCMConfig.properties** file.

For Microsoft SQL databases, the database owner name, and schema prefix will need to be added to the **BCMConfig.properties** file. Follow the ensuing steps to locate this information, and add it to the configuration file.

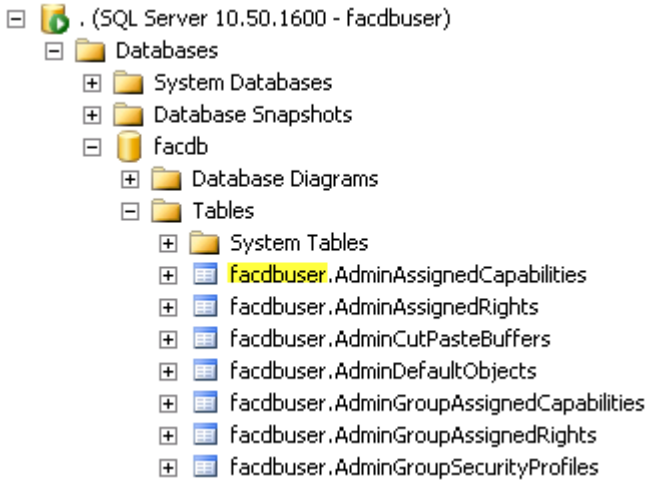
The following topics are provided:

Configuring the database owner

1. On the BMC Client Management master, navigate to the directory where BMC Client Management is installed (typically `\Program Files\BMC Software\Client Management\Master`).
2. Open the `Vision64Database.ini` file from the `\Master\config` directory.
3. Locate the `User=` line, the `username` specified here is the database owner.

Configuring the schema prefix

1. Open **SQL Management Studio** on the SQL server where the BMC Client Management database resides.
2. After logging into **Management Studio**, in the **Object Explorer** section on the left side of the window, expand **Databases > Your Database > Tables** (replace *Your Database* with the name of your BMC Client Management database, typically **bcmdb**).
3. Note the name appearing to the left of the dot in the table `names` ; this is the schema owner. As an example, in the following screenshot, we can see that the schema owner is **bcmdbuser** :



After identifying the database owner, and schema prefix, please add these values to the `SQLDBOWNER` and `SQLSCHEMAPREFIX` parameters in the **BCMConfig.properties** file. For example, if the schema prefix and database owner are both `bcmdbuser`, these parameters should be entered as shown (note the dot at the end of the `SQLSCHEMAPREFIX` parameter, please ensure this dot is entered in your configuration file also):

```
SQLDBOWNER=bcmdbuser
SQLSCHEMAPREFIX=bcmdbuser.
```

Filters

The following topics are provided:

- Hardware jobs
- Software jobs
- Identifying device group IDs
- Best practices with reconciliation

Hardware jobs

The integration component can be configured to import data only from selected device groups by entering the device group IDs into the `HARDWARE_GROUPID` parameter in the **BCMConfig.properties** file. For example, to retrieve data from groups whose IDs are `100,101,` and `200` , this parameter should be entered as follows:

```
HARDWARE_GROUPID=100,101,200
```

If you are not sure which group IDs correspond to the groups you would like to import, see topic Identifying device group IDs for further instructions on identifying group IDs.

Software jobs

The integration component can also filter software inventory data based on device group ID in a similar way to the filtering for the hardware job, using the `SOFTWARE_GROUPID` parameter in the **BCMConfig.properties** file. The syntax for filtering a software import by group ID is the same as that for the hardware import, and as an example, we will also show the filter configured to collect data only from devices in groups with IDs of `100,101,` and `200`:

```
SOFTWARE_GROUPID=100,101,200
```

In addition to the device group ID filtering, the software import can also be filtered based on the status of the software which was set via the BMC Client Management console . The possible statuses which can be filtered are:

- `Managed - Supported`
- `Managed - Unsupported`

For example, to import both `Managed - Supported` and `Managed - Unsupported` software, you would use the following filter line in the **BCMConfig.properties** file:

```
SOFTWARE_STATUS='Managed - Supported', 'Managed - Unsupported'
```

Identifying device group IDs

Assuming the name of the device group is known, the group ID can be identified using a simple SQL statement (replace YOUR_GROUP with the name of the group whose ID you would like to find):

```
select groupid from groups where GroupTypeID=101 and GroupName='YOUR_GROUP'
```

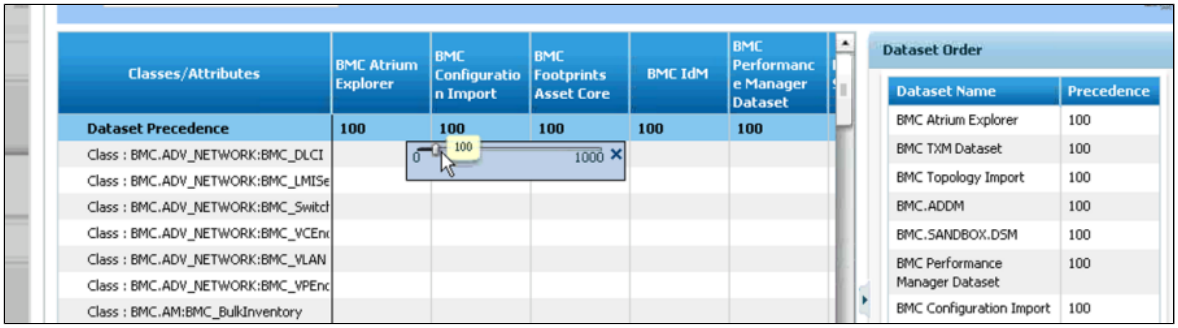
The group ID which is returned can then be used in either a hardware or software group filter.

Best practices with reconciliation

The jobs created by the installer should be run sequentially and not concurrently, because this may cause duplication of records.

Within the Atrium reconciliation engine, the default dataset precedence is 100 for any new database, it is recommended that BMC ADDM has a higher precedence set than BMC Client Management for the various tasks.

For more information on setting the precedence, please review the Atrium documentation.



Working with the Integration Maintenance Tool

This section provides instructions for using the BMC Client Management - BMC Atrium CMDB Integration Maintenance Tool.

The Maintenance Tool provides a common tool to access diagnostics and utilities. You can use the Maintenance Tool to review logs or configuration parameters. The Maintenance Tool also provides the Log Zipper utility that collects and archives log files and operating system information that BMC Customer Support might need to help you troubleshoot problems.

The following topics are provided:

- Executing the maintenance tool
- Viewing the installation logs
- Zipping logs for customer support

Executing the maintenance tool

1. From the installation directory of the product, open the **<Installdir>/ bcmcmdbintegration** folder.

   > The default installation directory is as follows:
   > - Windows: **C:\Program Files\BMC Software\BCMCMDBIntegration**
   > - Linux: **/opt/bmc/BCMCMDBIntegration**

2. Execute the following file to open the Maintenance Tool:

Windows: `BCMCMDBIntegrationMaintenanceTool.cmd`

Linux: `BCMCMDBIntegrationMaintenanceTool.sh` The following tabs are displayed:

- Logs
- Configuration
- Health Check
- Encrypt

> **Note**
>
> BMC Client Management - BMC Atrium CMDB Integration only uses the **Logs** tab. The other tabs are for other applications such as BMC Remedy Atrium. For more information, see the documentation for those products.

Viewing the installation logs

When you run the BMC Client Management - BMC Atrium CMDB Integration installer or uninstaller a log file is created in the BMC Client Management - BMC Atrium CMDB Integration Maintenance Tool. To view these logs proceed as follows:

1. Open the Maintenance Tool.
2. Click the **Logs** tab.
3. To view the installation log, click **Install Log** .

> This action is required when you want to see the messages generated during installation or search the installation logs to identify issues. Search for rows highlighted in red (errors) or yellow (warnings).

4. To view the installation log, click **Uninstall Log** .

   > This action is required when you want to see the messages generated during uninstallation or search the uninstallation logs to identify issues. Search for rows highlighted in red (errors) or yellow (warnings).

   > Click the column header to sort columns. To reverse sort a column, press the **Shift** key while clicking the column header.

5. To view the configuration log, click **Configuration Log** .
6. To open the folder that contains the log files, click **Browse to Log** .

Zipping logs for customer support

Installation issues and application issues can occur during installation or application use. You can use the Log Zipper, which is part of the BMC Client Management - BMC Atrium CMDB Integration Maintenance Tool, to zip all the log files that are necessary to debug issues. This action is required when you want to send the logs to Support for error investigation.

1. Open the Maintenance Tool.
2. Click the **Logs** tab.
3. To zip all log files for Support, click **Zip Logs** .

   > This action is required when you want to send the log files to Support for error investigation.

4. To zip all registered product logs on the computer, click **Zip All Logs** .

   > This action is required when you want to send the logs to Support for error investigation.

5. Send the `BCMCMDBIntegrationLogs.zip` output file from the `temp` directory to BMC Customer Support.

Using

This section provides information on how the IT administrator can successfully achieve organization's infrastructure management goals using BMC Client Management.

The following table provides links to relevant topics for each goal:

Goal	Instructions
Understand BMC Client Management console	• Navigating through the console • Understanding common functionalities • Understanding common objects • Managing console preferences • Managing the BMC Client Management agent • Viewing autodiscovered objects • Managing dynamically populated user and device groups • Managing devices and device groups • Managing users and user groups
Scan a complete network or parts of a network for all existing devices	• Managing asset discovery scans • Managing discovered devices • Viewing result of the last scan • Discovering the assets via the wizard
Understand the process of agent rollout	• Agent rollout overview • Getting started with agent rollout • Rolling out your first agent • Automatically rolling out agent using a wizard • Downloading and installing rollout from a server • Scheduling a rollout • Alternative rollout methods • Uninstalling the client agent via rollout
Understand and apply operational rules	• Operational rules overview • Getting started with operational rules • Adding packages to operational rules • Adding dependencies to operational rules • Advertising an operational rule • Assigning targets to operational rules • Leveraging operational rule steps • Operational rules wizards • Examples of operational rules
Collect and manage inventory of a device or a device group	• Managing inventory of a device • Managing inventory of a device group • Purging • Collecting inventory remotely via USB for unconnected device • Getting started with custom inventory
Monitor and manage installed applications	• Overview of Application Management • Getting started with application monitoring • Defining an application for usage monitoring via the software catalog

Goal	Instructions
	• Defining an application for prohibited launch detection via the software catalog • Uploading application monitoring events to the master • Generating application monitoring reports • Defining applications to use in application management • Configuring application monitoring • Adding an application from a device • Managing application lists • Managing custom applications • Managing licensed software • Managing schedule templates • Managing software catalog
Track and manage usage of software licenses	• Getting started with managing software licenses • Creating a licensed software • Evaluating the Licensed Software for Authorized Software Installations • Modifying the Evaluation Schedule • Software License Management Wizard
Track and manage financial data of IT assets	• Overview of financial asset management • Financially assessing your devices • Evaluating a device group's financial data • Creating Relations between Assets • Adding Additional Information via Files • Editing the financial information of a device • Viewing calculated values
Evaluate compliance of your IT environment with necessary rules and regulations	• Overview of Compliance management • Getting started with custom compliance • Evaluating your Environment for Compliance with a Basic Rule • Assigning the compliance rule to a device group and evaluating its members • Creating a Device Group of Non-compliant Devices • Reporting compliance • Managing compliance dashboards • Compliance Rules for Compliance Management • Dynamic Groups in Compliance Management • Overview of SCAP compliance • Managing SCAP Jobs • Scap job wizard • SCAP Implementation Statement
Manage, update, and download patches across your network	• Getting started with patch management • Prerequisites • Patching Your First Device • Automating Patch Management • Regularly scanning a device group for missing patches • Deploying a Bulletin to Affected Devices

Goal	Instructions
	• Scheduling Deployment • Generating Patch Group Reports • Automatically Downloading Patches • Viewing the Patch Detection dashboard • Managing patch inventory • Working with patch groups • Managing patch jobs • Managing bulletins • Managing service packs • Managing dynamic downloader • Locally accessing patch management • Patch Service Pack Distribution Wizard
Automate distribution, installation, and configuration of all enterprise software	• Software distribution overview • Distributing your first package • Creating an MSI Package and making it available • Assigning an existing package to the targets for distribution • Killing Firefox before starting the distribution • Distributing only to devices with a minimum amount of RAM • Using multicast distribution (predefined bandwidth) • Rebooting the device at the end of the distribution • Scheduling distribution • Distributing with Wake-On-LAN enabled • Managing Packages • Software distribution wizards
Deploy and manage operating systems	• Prerequisites for OSD • Executing your first operating system deployment • Performing advanced OSD tasks • Managing OSD Managers • Managing Image Repository • Configuring Network Boot Listener • Managing OSD Drivers • Managing OSD Images • Managing OSD Disk Configurations • Managing OSD target lists • Managing targets • Managing OSD Projects • Managing OSD multicast sessions • Creating an OSD PXE Menu • Managing OS Deployment via the wizards
Manage devices effectively and lock unauthorized devices	• Creating your first device rule • Monitoring local events • Monitoring the results on the master
Monitor all systems on a network remotely	• Remote management overview • Remotely controlling a device

Goal	Instructions
	• Directly accessing a device
Implement power management on client systems	• Power management overview • Generating the Power Management inventory • Monitoring the Power Management events • Power Management reporting • Defining an upload schedule for Power Management • Regularly generating (update) the inventory • Regularly uploading events • Creating or modifying power scheme • Changing active power scheme • Managing Power Management Inventory • Viewing alerts and events • Power management step reference
Use diagnostic tools for verifications and checks	• Launching a diagnostic • Viewing device diagnostic results • Viewing device group diagnostic results • Canceling a running diagnostic • Deleting diagnostic results • Repairing corrupted data in the database • Filtering for specific diagnostic results • Filtering for specific status values • Importing new diagnostic scripts
Remotely configure and manage iOS mobile devices	• Managing mobile devices • Enrolling mobile devices • Viewing information about managed mobile devices • Managing mobile applications • Managing configuration profiles for managed mobile devices • Performing remote operations on managed mobile devices

Working with BMC Client Management console

The BMC Client Management console is the most important part of BMC Client Management. All the tools necessary for managing your clients on a day-to-day basis can be found in the console. The most important aspect of the console is its capability to manage any of the object types supplied by BMC Client Management and execute all types of action on these.

This topic includes:

- Launching the console
- Logging on to the console
- Related topics

Launching the console

The console is a Java application and can thus be launched using the generally available startup options provided by Java, such as `-Xmxn` to extend the maximum size of the memory allocation (n must be a multiple of 1024, for example, `Xmx80m` or `Xmx81920k`). By default the anti-aliasing option is used for the console. To switch it off, open the console shortcut's **Properties** window and modify the `-Dswing.aatext` option from `true` to `false` . To launch the console with its standard options proceed as follows, depending on the operating system on which your console is installed:

Platform	Description
Windows	To launch your newly installed Console, select **Start > Programs > BMC Software > Console** or double-click the console desktop icon.
Linux	To start the console, type `BMCClientManagementConsole` , then press **Enter** .
Mac OS	To start the console, double-click the icon for the console on the desktop.

Logging on to the console

In the the Login window, enter the required information and click **Login**.

Notes

- If the console is installed on the master server, this text box is filled in with the default value`localhost:1610` . If you are connecting via Java Web Start, this text box is filled in with the master information (that is, either the master's name or IP address).
- If you are accessing the console from a device other than the master, r eplace the prepopulated *localhost* entry with the name of the master server you want to connect to and its port number separated by a colon (:) in the **Server:Port** box. You can enter the host name either as its short or full network name such as **scotty** or **scotty.enterprise.com**, or in the form of its IP address. Be aware that when you use IPv6 you need to put square brackets around the IP address, for example, **[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611**.
- If you need to connect to Client Management via the Internet and you have installed your console separately from your master, you must provide the public IP address of the master to be able to connect.

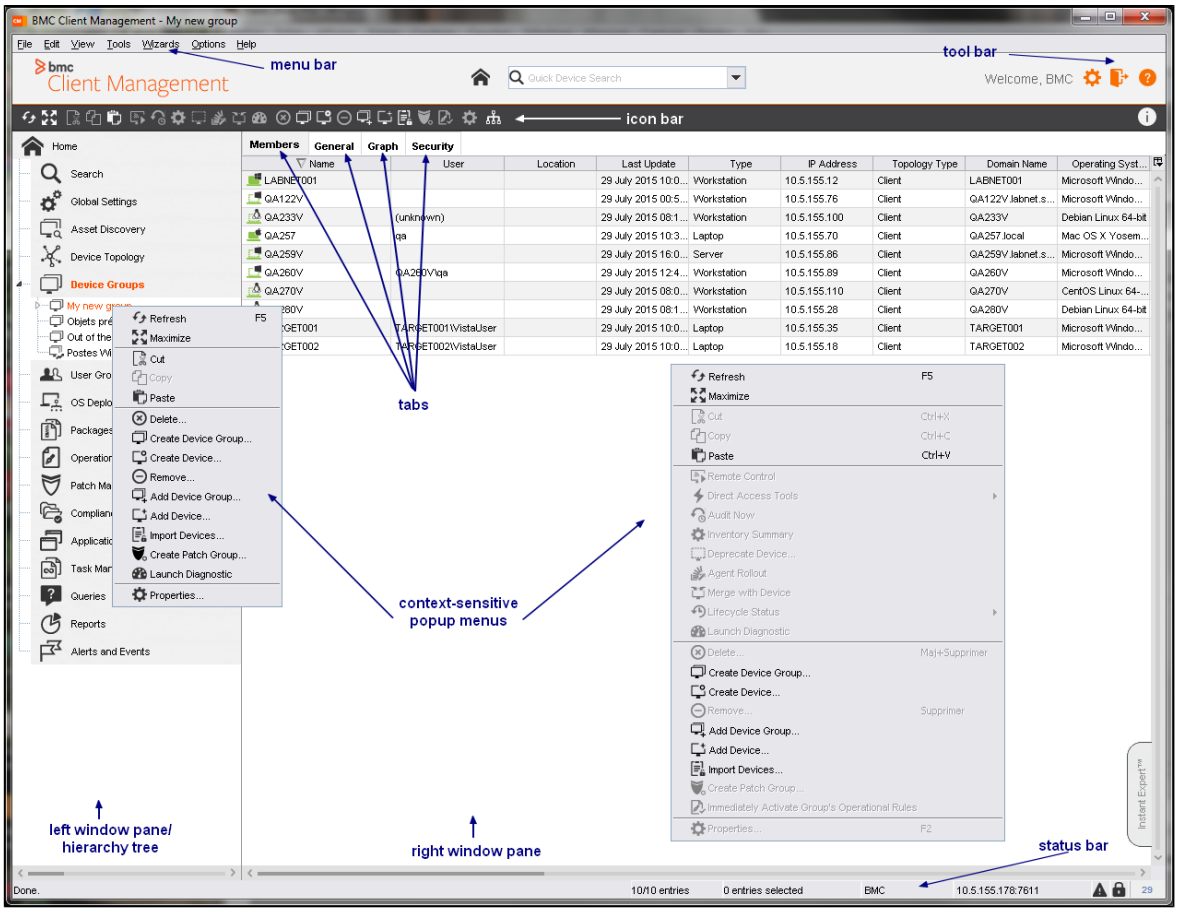
Related topics

- Navigating through the console
- Understanding common functionalities

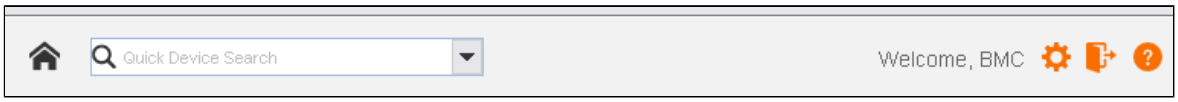
- Understanding common objects
- Managing console preferences
- Managing the BMC Client Management agent
- Viewing autodiscovered objects
- Managing dynamically populated user and device groups
- Managing devices and device groups
- Managing users and user groups

Navigating through the console

There are seven main areas on the console screen. The title bar at the top, the menu bar right below, followed by the graphical icon bar and the tool bar right below and at the bottom of the window the status bar. The main window is divided into the left and right window panes. Both the left and right window panes offer context sensitive pop-up menus to access node or tab specific information or actions.



The tool bar is always available below the icon bar and provides general tools usable at all locations in the console, such as a quick search functionality, direct access to the logged users' preferences and the possibility to switch on/off the guided tasks functionality.



The tool bar is composed of the following elements:

Element	Description
Quick Device Search	This field allows you to quickly find one or more devices. For more details on how to use this search see Quick Search.
Preferences	This item is a shortcut to the **Preferences** window which allows you to define specific settings for the currently logged user. For more details on this topic see Managing console preferences.
Help	This button is a shortcut to the online help. If you click it a browser window opens and displays the complete online help.

Understanding common functionalities

BMC Client Management provides a number of functionalities which are common to many elements and can be applied to most of your database objects:

- Searching objects
- Viewing object properties
- Selecting object
- Saving, exporting, importing, and printing
- Duplicating objects
- Using keyboard shortcuts
- Managing bookmarks within console
- Using Instant Expert™

Searching objects

This topic introduces the **Search** functionality of the BMC Client Management console . It describes how to create and apply a search and explains the presentation of the search results.

This topic includes:

- Quick search
- Advance search
- Related topics

Quick search

To quickly access a specific device in your network the **Quick Search** functionality provides you with an easy to use syntax to find anything. You can search for any information that can be found in the device's identity, and its hardware or software inventory. This type of search is limited to devices, any other object can only be found via the **Advanced Search** .

1. To search for devices enter the criteria in the text box above the table, for example, *windows* to find any device with a Windows operating system, or *Linux* for all Linux devices.
   - The search is not case sensitive, therefore *WINDOWS, Windows* and *windows* will all find the same devices.
   - You can use wildcard characters for the search, that is, `192.168.15.` **to find all devices of a specific subnet. The accepted wildcard characters are ? and {}** .
2. Click **Find** next to the text box.
   The following table will then display all devices matching the search criteria with the following information:

Parameter	Description
Rating	Displays the matching percentage of the entered criteria with the search expression found on the device, for example, 100 for a full match (100%).
Hits	Displays how often the search expression was found for the device, for example, Hits: 4, indicates that the search expression was found 4 times in different fields of the device.

3. Select a device.

The **Result Details** box below the list will now display the context in which the search criteria was found, with all occurrences of the criteria being highlighted per device.

The following operations are available for a device found by the search from this location:

- Remote Control
- Direct Access Tools
- Audit Now
- Inventory Summary
- Deprecate Device
- Agent Rollout
- Purge
- Merge with Device
- Delete Device
- Update Index
- View Node

Advance search

The BCM database typically contains large numbers of objects. The **Advanced Search** functionality is designed to let you quickly locate and view information about a particular object, group or folder of objects that meet the search criteria you specify.

To execute a search define the following criteria:

Parameter	Description
Object	

Parameter	Description
	Select the type of the object to find from the list box. You can search for any main object type that exists in the database. If *Device* is selected as the type a new drop-down list box appears to the right, in which you can define if the search is to be executed in the **Topology** , in the **Device Group Hierarchy** , only for **Objects Found** (among the objects under the **Lost and Found** node) or for **All** objects in the database.
Criterion	Select in this list the object attribute on which the search is to be executed, for example, the object name or the object notes, and so on.
Operator	Select the operator for the search, possible values are **Contains** , **Ends with** , **Equal to** , **Greater than** , **Greater than or equal** , **Less than** , **Less than or equal** , **Like (SQL)** , **Not equal to** , **Not like (SQL)** , **Starts with** , **Is Null** and **Is Not Null** .
Value	Enter the value to search for into this text box or select it from the list box. Depending on which operator you chose you can also use the following wildcard characters in this text box: • % to indicate any number and type of character to return the maximum number of objects matching the operator criterion. • If the value to search for is of type Boolean, you need to enter 0 for is not equal to the criterion, and 1 for fulfils the criterion condition.

To execute the defined search click **Find** to the right. The results of the search will be displayed in the lower half of the right console pane in the form of a list, which displays the icon and the location of the object found.

For example, the result for administrators lists all administrators found directly under the **Administrators** node and under the groups to which they are assigned. The result of a search for specific devices lists all devices found at their location within their groups and within their actual location in the topology, for example, the device group hierarchy: Device Groups/Bridge/KirkDevice Groups/Bridge/OhuraDevice Groups/Engine/ScottyDevice Groups/Commanders/Kirk

and the topology hierarchy: Topology/Enterprise/BridgeRelay1/Kirk Topology/Enterprise /EngineRelay1/Scotty Topology/Enterprise/BridgeRelay1/Kirk/Ohura

If no objects can be found for the defined criteria the value **No Result** will be displayed next to the button. If an error occurred during the search the message **Search Failed** will be displayed next to the **Find** button.

The following further operations are available for a device found by the search:

- Find node
- View Node
- Remote control

Related topics

- Search Syntax and Search Requests
- Update Index
- Cleaning up the Search Results

Search Syntax and Search Requests

The following rules apply for the quick search:

- Fields to search
- Search Requests

Fields to search

The following fields can be searched. They refer to either a device, a user or financial asset management data:

Parameter	Description
Name	The name of the device, for example, scotty.enterprise.com, PC1, M60-ITA.
os	The name of the operating system composed of its name, its major version, minor version, revision and build numbers, for example, Microsoft Windows XP Professional 32-bit 5.1 rev:Service Pack 3 build:2600.
fpac	The agent version, composed of its major version, minor version, revision and build numbers, for example, 10.0.0 build:100415c.
ip	The IP address in its dotted notation, for example, 194.50.68.255.
domain	The domain name of the device, for example, LABNET/PC2:
netbios	The NetBIOS name of the device, this field is not applicable for Linux and Mac OS devices, for example, M60-ITA.
macaddress	The MAC, that is, the hardware address of the device, for example, 00:01:02:AF:7D.
serialnumber	The serial number of the hard disk of the device, for example, 0001657879.
type	The topology type of the device, for example, master or client.
currentuser	The name of the user who was logged when the last hardware inventory was generated, for example, LABNET /Administrator.
user	The name of the user who was logged when the last hardware inventory was generated, for example, LABNET /Administrator.
vendor	The name of the vendor of the asset.
po	The purchase order number of the asset.
support	The name of the support provider of the asset.
dept	The name of the department to which the asset belongs.
sku	The SKU vendor name of the asset.
status	The current life cycle status of the asset.
contact	The name of the administrator to contact for anything about the asset.
owner	The name of the user of the asset.

Search Requests

The Quick Search supports the following types of search requests:

- The search is *not* case sensitive, for example, hardware inventory, Hardware Inventory and HARDWARE INVENTORY will all return the same results.
- The wildcard characters ? and * can be used.
- An "any words" or "natural language" search is any sequence of text, like a sentence or a question. In an "any words" search, use quotation marks (") around phrases, put + in front of any word or phrase that is required, and - in front of a word or phrase to exclude it.
  Examples

Search Request	Explanation
apple +pear	*Apple* must be present and *pear* .
apple -pear	*Apple* must be present but not the word *pear* .
+apple	Only the word *apple* must be present, not its plural, composed term or synonyms.
apple * pear	The words *apple* and *pear* separted by one or more words

- A boolean search request consists of a group of words, phrases, or macros linked by connectors such as AND, *not* and OR that indicate the relationship between them.
  Examples

Search Request	Explanation
apple and pear	Both words must be present.
apple or pear	Either word can be present.
"apple or pear"	The exact phrase *"apple or pear"* must be present.
apple w/5 pear	*Apple* must occur within 5 words of *pear* .
apple not w/5 pear	*Apple* must not occur within 5 words of *pear* .
apple pre/5 pear	*Apple* must occur 5 or fewer words before *pear* .
apple and not pear	Only *apple* must be present.
apple w/5 xfirstword	*Apple* must occur in the first five words.
apple w/5 xlastword	*Apple* must occur in the last five words.

  If you use more than one connector, you should use parentheses to indicate precisely what you want to search for. For example, apple and pear or orange juice could mean (apple and pear) or orange, or it could mean apple and (pear or orange).
- Noise words, such as if and the are ignored in searches.
- To search in a specific database field the following syntax options are available:
  Syntax `(name contains (M60 OR ITA)) and (macaddress contains 00:01:02:AF:7D)`
  or `(name::M60 or ITA)) and (macaddress::00:01:02:AF:7D)`
  Explanation
  The database field "name" must contain either the value "M60" or "ITA" and the field "macaddress" must contain the value "00:01:02:AF:7D".

Update Index

If the search provided no results maybe the index was not yet created or is not up to date. To immediately launch a new indexation click **Update Index** . The new indexation will be started immediately, however, depending on the size of your database this might take a few moments to finish.

Cleaning up the Search Results

Found objects can be selected and displayed directly under the main **Search** node. They will be displayed in the order of selection, not replaced. To remove all objects displayed under the main **Search** node, proceed as follows:

1. Select the **Search** node in the left window hierarchy.
2. Right-click the mouse on it.
3. Select **Clean up** from the pop-up menu.

All displayed objects will be removed immediately from the view.

Viewing object properties

All objects in the console provide you with specific information about their properties.

A number of these properties are already displayed in the **General** tab of each object as explained in the preceding paragraph, but some objects offer more detailed information in their properties window, the **Properties** dialog box. This dialog box usually only has one tab which displays the general information about the selected object; exceptions to this rule are mentioned in the respective object topics. In the **General** tab, you may view or modify some or all properties, depending on the object.

Selecting object

In the console objects are selected to be added or assigned through the Object Selection dialog box. This is applicable in all situations where an object can be added to a new relation or can be assigned to another object. Depending on the object location from which it is called it can have three or four of the following tabs represented by icons:

- Hierarchy ( )
- All ( )
- Search ( )
- Topology ( )

To select an object to add or assign it, select it in one of the tabs and click **OK** at the bottom of the window. You can also add or assign several objects at the same time by holding the CTRL key while selecting the objects. Multiple object selection, however, is only possible within one tab not across tabs.

Other items that are not database objects and which are displayed in the console window, such as operational rule steps or query criteria, will be added through their own specific dialog boxes, which will be explained in the respective topics.

Hierarchy

The **Hierarchy** tab displays all existing objects of a type in hierarchical order in tree form, that is, the selectable objects and their parents or children. As you can see in the graphic to the right, the example displays all device groups with their contents, that is, all other device groups and devices the group contains, even though the dialog box is called to assign a device not a device group as you can see from its title.

If this window is called by an administrator without read access on the Device Groups top node, this tab will not be displayed.

All

The **All** tab of this dialog box appears a flat list of all objects which are selectable. As you can see to the right, the table shows only the list of all devices that exist in the database and no device groups.

Search

The **Search** tab allows you to search for one or more specific objects in the database, such as devices, device groups or administrators. The **Search** tab needs the following parameters to be specified for the search:

Parameter	Description
Criterion	Select in this list the object attribute on which the search is to be executed, for example, the object name or the object notes, and so on.
Operator	Select the operator for the search in the second drop-down box. The possible values are: **Contains** , **Ends with** , **Equal to** , **Greater than** , **Greater than or equal** , **Less than** , **Less than or equal** , **Like (SQL)** , **Not equal to** , **Not like (SQL)** and **Starts with** .
Value	Enter the value to search for into this box. Depending on which operator you chose you can also use the following wildcard character in this text box: % to indicate any number and type of character after the already entered characters. You can also leave the text box blank, to return the maximum number of objects matching the operator criterion.

To execute the defined search click **Find** to the right. The results of the search will be displayed in the lower half of the window in the form of a list.

Topology

The **Topology** tab displays your whole network, that is, all objects of this type which are in the database. In the example to the right, you can see that it displays all different types of devices that exist, masters, relays and clients.

This tab is only applicable when adding or assigning a device or when an object is assigned to a device.

Saving, exporting, importing, and printing

This topic includes:

Saving view

The console allows you to save the data displayed in the right window pane in a console window in a user-defined format to be accessible to other applications.

1. Select **Edit > Save View**.
   The **Save a View** dialog box appears.
2. Enter the following data into the respective boxes:

Parameter	Data
View Title	Enter into this text box the name or title of the view to be saved. You can use any character, including special characters. Also no maximum length is fixed. Do not add an extension to the name, it is automatically added when selecting the file format.
File Format	Click the arrow on the drop down box to display the list of available file formats and select the desired format. Possible values are csv, html and xml.
File Path	Enter the full path of the target file into the text box. Do not enter a name for the file, it is automatically generated, being a combination of the saved node and tab name.
Browse	You can also define the target location by clicking Browse. A new window appears in which you can browse your directory hierarchy and select a target directory for the file.
Pages	This option is only displayed if the (page) view you are saving is paged and might thus consist of more than one page. You can define to only save the "page" currently displayed by checking the Current radio button or to save all "pages" of the selected node by marking the All radio button.

3. Click **OK** to confirm, generate it and save it to the defined location.

Exporting

The BMC Client Management export option allows you to export specific data of the currently selected node to a file in a user specified format. You can make it then accessible to other console users, who can import this file to add these data to their console or to users of other applications to which these data might be of interest.

1. Select the node for which you want to export the data in the left window pane.
2. Select **Edit > Export**.
   The **Export the Current Node** dialog box appears.
3. Either enter the file path for the export directly into the **File Path** box or click the button next to it to call a list of all available drives and directories of your client.
   The path entered here must be a full path, it cannot be a relative path. Besides, you must enter a name for your export file with an extension.

4. Select the desired item(s) for the export from the following list.
   You can select more than one item by clicking the first item, pressing the CTRL key and holding it when selecting other items with your cursor.
5. Click **OK** to confirm.

> ⚠ For exporting packages, BMC Client Management exports an `.xml` file and a `.package` file.

The export will directly be created at the defined location.

Importing

The console enables you to import complete views saved from other console windows. When you import a view, the root node of the import will be imported with all its following hierarchical structure.

1. Select **Edit > Import**.
   The **Import a Node** dialog box appears in which you can select the file containing the data to import.
2. Select the type of file which contains the import data and select the file.
   The file can be located anywhere within your network on a drive to which you have access, it must not be located on your local client.
3. Click **Open** to confirm.

> ⚠ For importing packages, the import process verifies whether a .package file related to the selected .xml file exists.
> - If the .package and .xml files are related, the package is automatically copied in the package location.
> - If the .package and .xml files are not related, the package has to be manually copied.

The window will close and the contents of the file will be imported directly into your console.

Printing

The console also allows you to print the currently selected view and all its data and any graphics displayed in the view.

1. Select the node in the left and the tab in the right window pane that you want to print.
2. Select **Edit> Print**.
   If the page you intend to print is paged, the **Print Zone** dialog box appears on the screen. It provides you with the following option:
   - **Current**: Prints only the currently displayed page.

- **All:** Prints all pages of the selected node.

3. Select the desired option and click **OK**.
4. In the **Print** window, select a printer and any other printer-connected options, and then click **OK**.

Your view is printed.

Duplicating objects

You can duplicate objects of your console by using the **Copy** and **Paste** actions. Duplicating objects can save you the time to create a new object of the same type with just slightly different attributes or values, such as a query, for which only one criterion is different.

Any individual object, such as an administrator, a report or an operational rule can be copied, but not folders or groups. Be aware that you can only duplicate objects within their own object type node, that is, you can only duplicate a query with the **Queries** node, you cannot copy it and place it in the **Assigned Queries** node of a device group.

Some general and some object specific restrictions apply when objects are duplicated:

- No assignments, that is, device, device group, query or operational rule, are copied, with the exception of **Rollouts** , for which the device assignments will be duplicated as well.
- The **Scheduler** s of queries, operational rules and reports are duplicated.
- The security settings of the duplicated object, that is, the settings defined in the object's **Security** tab will be duplicated.
- For operational rules the steps and the list of the packages to which they are assigned are duplicated.
- Regarding reports all their subreports and their respective contents, that is, columns and formats are duplicated, and the defined exports.
- **Rollouts** can be duplicated but neither individual pull deployments nor push deployments.
- If a device is duplicated within the same device group, the same rules as those explained in the preceding paragraph apply. If the device is copied and put into another device group, the name will stay the same, as a device can have several parents.

To duplicate objects

1. Select the object to be duplicated in the table in the right window pane of its folder or group.
2. Select **Edit > Copy** .
   The selected object was copied into the clipboard.
3. Select **Edit> Paste** .

> If you duplicate an object several times, the number will be increased with each paste action. For example, the original object is *myquery*, then it will be duplicated into *myquery (1)*, *myquery (2)*, and so on.

The duplicated object displays in its location with the same name as the original object extended by a number, because the same object cannot exist more than once, except for devices.

Using keyboard shortcuts

A number of shortcuts were implemented on the contents of the console window for Windows and UNIX systems.

Shortcut	Description
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + A	Select all
CTRL + P	Print
DELETE	Remove
SHIFT + DELETE	Delete
ENTER	Confirm modifications in a dialog box and close it (**OK** / **Close** button)
ESC	Close a dialog box without applying any modifications made in it (**Cancel** / **Close** button)
F1	Context-sensitive on-line help
F2	Open the Edit Properties window
F5	Refresh the active window

Managing bookmarks within console

The console allows you to create bookmarks, the same as in any browser window. This functionality can be accessed through the **View** menu. Only objects such as devices, rules, and so on, can be bookmarked. You cannot bookmark nodes such as Inventory, Package Factory, and so on.

You can access your bookmarks from **View > Bookmarks > (Your Bookmark)**.

This topic includes:

- Adding bookmarks
- Organizing bookmarks

Adding bookmarks

1. Select the object you want to add to as a bookmark in the left window pane.
2. Select **View** > **Bookmarks** > **Add Bookmark** .
   The **Add a New Bookmark** dialog box appears.
3. Enter a the name and folder for the bookmark in the respective boxes.

By default, the name of the bookmark is the same as that of the selected object. You can add the bookmark directly under the main bookmark node or into an existing folder.

4. Click **OK** to confirm.

The new bookmark was added to the list of bookmarks.

Organizing bookmarks

1. Select **View** > **Bookmarks** > **Organize Bookmark**  .
   The **Organize Bookmarks** dialog box appears.
2. Perform the desired task:

Task	Steps
Create Folder	Right-click the parent for the new folder.A pop-up-menu appears. Select Create Folder.The Create New Bookmark Folder dialog box appears on the screen. Enter the name of the new folder into the text box. Click OK to confirm.
Rename Bookmark Folder	Right-click the desired object.A pop-up-menu appears. Select Rename Bookmark Folder.The Rename a Bookmark or Bookmark Folder dialog box appears on the screen. Enter the desired name for the selected object into the text box. Click OK to confirm.
Remove	Right-click the desired object.A pop-up-menu appears. Select Remove.A Confirmation dialog box appears on the screen. Click the Yes button to confirm.

The selected task is completed.

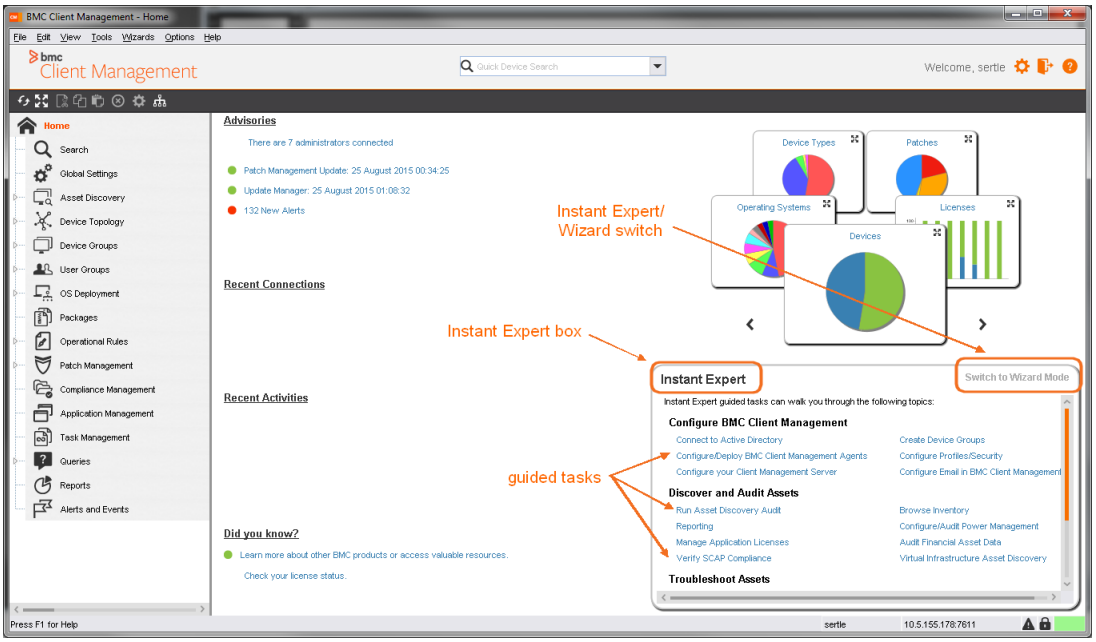
Using Instant Expert™

This topic includes:

- Instant Expert™ guided tasks
- Instant Expert™ Panel
- Maximizing or minimizing the Instant Expert™ panel

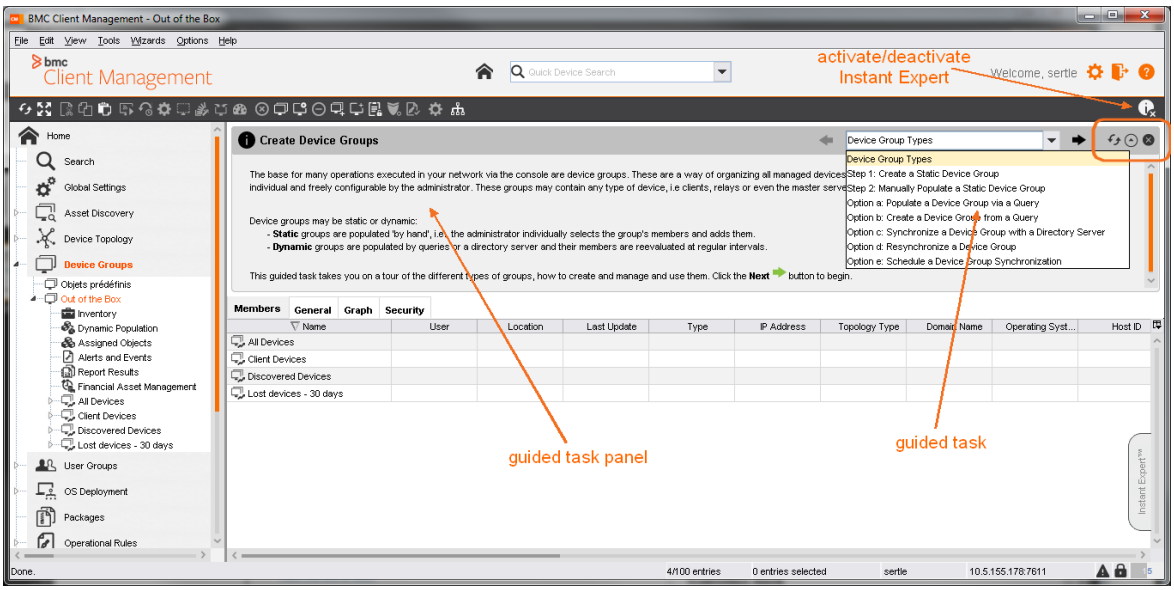
The **Instant Expert™** functionality in BMC Client Management provides you with two ways of working:

- Directly accessing a specific task from the dashboard or in a functionality.
- The **Instant Expert™** panel which is available for all the main nodes.



Instant Expert™ guided tasks

The CM console provides **Instant Expert™** guided tasks for a number of its functionalities that guide you through the first steps and examples of using it. These tasks are accessible from the Dashboard and from the main nodes of the individual functionalities.

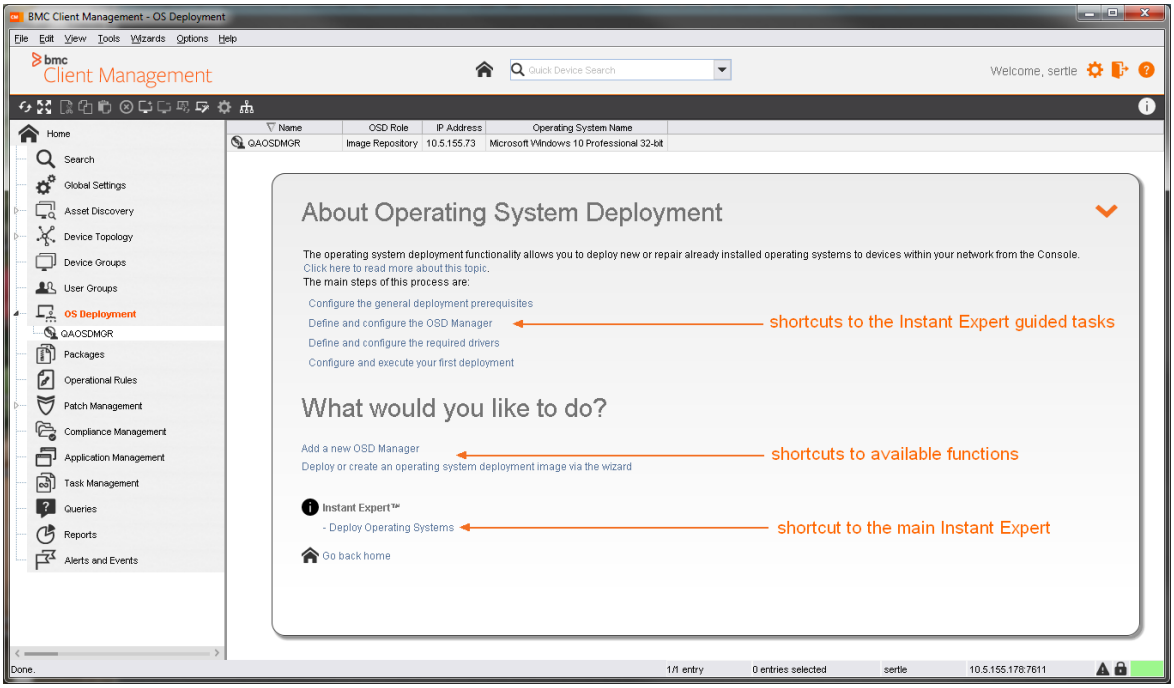


- You can switch the **Instant Expert™** mode on or off via the **Activate Instant Expert** / **Deactivate Instant Expert** button (/) in the icon bar which is accessible everywhere in the console.
- In the Dashboard the **Instant Expert™** is displayed alternately with the Wizards available via the console.

- Selecting a Task in the **Instant Expert™** panel moves the focus directly to the location of the task in the console window.
- The individual task steps then guide you through the respective functionality and its possibilities via different examples in the guided task panel of the functionality.
- Select the individual steps either from the list or advance/return (/) step-by-step via the respective buttons.
- The guided task panel can be refreshed ( ), collapsed and reopened (/) and closed ( ) via its respective icons.
- Some nodes have more than one Instant Expert guided task assigned. To switch to another task of the current node select the **Deactivate Instant Expert** icon ( ) and select it again ( ) to reactivate it. The **Select an Instant Expert Guided Task** window will be displayed in which you can select the task to execute now for the node.

Instant Expert™ Panel

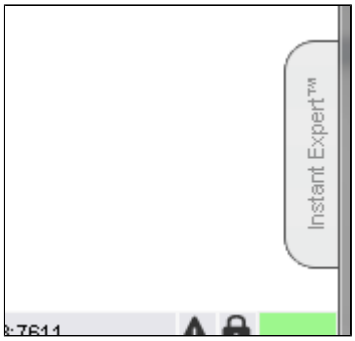
All nodes with the exception of the individual object nodes have an **Instant Expert™** panel, that is opened on top of the table in the right window pane when you select the node in the left hierarchy tree. This panel provides you with a short introduction to the functionality and its operating mode with shortcuts to existing **Instant Expert™** tasks. It also provides shortcuts to directly available functions under the second part and the direct access to the main **Instant Expert™** of the functionality.



Maximizing or minimizing the Instant Expert™ panel

The **Instant Expert™** panel is automatically minimized whenever an **Instant Expert™** task is called.

- To maximize, click the vertical **Instant Expert™** button on the bottom right hand side of the right window pane to maximize.



- To minimize,click the down arrow button on the top right hand side of the **Instant Expert™** panel.

When you minimize the **Instant Expert™** panel, it stays minimized until you maximize it again.

Understanding common objects

This topic explains the common objects such as users, devices or common nodes and tabs that are available for many of the different objects or have a general functionality.

While the information and options presented by these nodes and tabs are self-explanatory, you can perform a number of functions using these common objects:

- Managing assigned object types
- Managing schedule of an assigned object
- Managing dynamic groups
- Managing security of an object
- Managing graphs of an object

Object	Description
Assigned Objects	The Assigned Objects node provides the access points to all objects which can be assigned to a currently selected object and depending on the type displays different amounts of information. This information can be accessed via the subnodes of the assigned objects. In BMC Client Management, objects can be linked to other objects to execute specific operations, such as installing a software or monitoring the usage of an application on a group of specific devices. For more information, see Managing assigned object types.

Object	Description
Dynamic Population	In BMC Client Management any type of group can be either static or dynamic. Dynamic groups are populated and maintained through either a query or a directory server which was assigned to this group, or, if it is a device group, by a compliance rule, which collects the group's members according to their compliance, non-compliance or inability to be evaluated. Depending on the object it provides access to some of the following subnodes. These nodes display the objects which populate the group and allow you as well to define or modify the populator of the group: • Queries • Directory server • Compliance rule
Dynamic Groups	The Dynamic Groups node provides access to all types of groups which are dynamically populated by the currently selected object. For more information, see Managing dynamic groups.
General tab	The General tab is present in the right window pane in most of the console objects and it displays general information about the selected object. Some General tabs display some more object specific information, which will be explained in the respective topics. A number of the preceding explained values and object specific information detailed in the General tab are editable and can be modified through the Properties window.
Members tab	Being containers to collect members, all top nodes, folders or groups in the BMC Client Management have a Members tab to list all folders and individual objects which are members of the currently selected folder, group, or top node together with some further information depending on the type of the selected object.
Security tab	All database objects have a **Security** tab, which defines the specific access rights for administrators for that particular object. Be aware that only administrators assigned the capability **Manage Security** can edit the contents of this tab. **Administrators** who do not have the capability **View Security** will not be able to display the **Security** tab of any database object. For more information, see Managing security of an object.
Parameters tab	The **Parameters** tab provides access to all parameters and their values that can be defined for the respective module.
Bar Chart tab	The **Bar Chart** shows a graphical representation of the execution status of the distribution rule on the members of the assigned device group in the form of a bar chart. Double-clicking a grouped distribution rule status in either of the charts will set the filter for the displayed list of devices to the clicked status.
Pie Chart tab	The **Pie Chart** shows a graphical representation of the execution status of the distribution rule on the members of the assigned device group in the form of a pie chart. Double-clicking a grouped distribution rule status in either of the charts will set the filter for the displayed list of devices to the clicked status.
Graph tab	The graph is used to display the objects in the form of an image showing their direct connections. For more information, see Managing graphs of an object.

Managing assigned object types

The majority of the BMC Client Management object types can be assigned to devices and device groups. With the exception of some reports, you can see detailed explanations on these in the respective sections.

The following topics are provided:

- Assigned Groups
- Devices

Assigned Groups

The **Assigned Groups** node displays the list of individual device groups assigned to the selected object. Device groups can be assigned to:

- Inventory filters
- Application Monitoring (Monitored Applications, Prohibited Applications and Protected Applications)
- Operational Rules
- Packages
- Patch Groups
- Compliance Rules
- Device Groups assigned to transfer windows
- Commands

All objects assigned to a device group can have their assignments re-evaluated. To reevaluate assignment, select the device group and go to **Edit > Activate SCAP Job** . The agent will immediately re-evaluate the assignments of all objects of all object types for the selected device group.

Similarly, the following objects can be assigned to a device group:

- Operational rules
- Transfer windows
- Reboot windows
- Application lists
- Licensed software
- Inventory filters
- Reports
- Patch groups
- Patch jobs
- Compliance rules
- SCAP jobs
- Rollouts
- Commands

Devices

The **Devices** node displays the list of individual devices assigned to the selected object. Devices can be assigned to:

- Transfer Windows
- Inventory Filters
- Application Monitoring (Monitored Applications, Prohibited Applications and Protected Applications)

- Operational Rules
- Packages
- Patch Groups
- Compliance Rules
- Commands

Similarly, the following objects can be assigned to a device:

- Operational rule
- Transfer windows
- Reboot windows
- Application lists
- Licensed software
- Inventory filters
- Patch groups
- Patch jobs
- Compliance rules
- SCAP jobs
- Commands

Managing schedule of an assigned object

Objects which are in relation to other objects can also be scheduled to be assigned at a specific moment and they can be assigned a schedule at which their content is executed. When creating a relation between two objects it might not always be useful or possible to immediately apply this relation, that is, the assignment/execution must be postponed to another moment in time.

The schedule of an assigned object is defined in the **Scheduler** window by selecting options to answer the questions. Depending on the answer more options can become available. When the scheduler is first opened it displays in the top part the default schedule that is defined for execution. As you go along with your schedule specifications this line changes to show the execution schedule you define in verbal form. The **Scheduler** is accessed by clicking the **Properties** of a selected assigned object.

The **Scheduler** window provides you with the following possibilities:

1. First the assignment needs to be defined, make the necessary selections for the following parameters:
    - **Assignment Date** Define when a job or a rule is to be assigned. Possible options are:
        - **Assign Immediately** : the assignment is carried out immediately after defining the assignment.
        - **Specific Date** : the assignment of the job or rule will be carried out at a specific date and time.

- *Optional:***Wake-up Devices** Check this box if the agent is to wake up any devices which are currently switched off, to immediately execute the assignment instead of waiting for the next startup to do so.
- *Optional:***Run as Current User** Check this box if the distribution is to be executed and installed on the local device as the logged user and not as LocalSystem. If you are using environment variables in any of the step parameters you must check this box to make sure the variables of the local user are used and not the default values.
- *Optional:***Advanced** Click this link if you require more assignment options:
- *Optional:***Bypass Transfer Window** Check this box, if the distribution assignment is to be sent directly, ignoring any transfer window specifications which exist for the targets.
- *Optional:***Upload Intermediary Status Values** Define if only the final status values, that is, *Executed* or *Failed* are to be uploaded (unchecked), or if each and every status that the operational rule execution is passing through is uploaded (checked). This option is only available if the corresponding system variable is activated.
- *Optional:***Run while the execution fails** Defines if the operational rule /package is to be executed until its execution finally succeeds, that is, the final status *Executed* is uploaded.
- *Optional:***Upload status after every execution** Defines that the status value is uploaded after every execution of the rule, even if it has not changed.
- *Optional:***Assignment Activation** Defines the overall status of the software distribution rule for the respective device group. You can deactivate a group by unchecking the **Assignment Activation** box of the scheduler. By default this box is checked and the status is either *Activated* or *Paused* , if the default schedule was not selected during the assignment.
- *Optional:***Back to Previous** Click this link to return to the main assignment options and continue with the schedule definition.

2. Select one of the following options for the question **When do you want this rule to be run on devices?** to define when the actual execution is to be launched:
   Depending on the choice you make in this list box, additional options become available:
   - **Right now** Select this option to start the execution immediately.
   - **At Startup** Select this option if the object is to be executed every time the device is started.
   - **At Session Startup** Select this option if the object is to be executed every time the agent is started
   - **At Session Close** Select this option if the object is to be executed every time a session is closed.

- **Run repeatedly on a schedule** Check this option if if the execution is to be scheduled repeatedly.
- **Use Cronspec to Schedule** Select this option if the execution schedule is to be created via a cronspec.

3. *(Optional)* If you selected the **Run repeatedly on a schedule** option fill in the newly appeared boxes to create the execution schedule:
   a. Select if the schedule is to run every day, week or month.

> **Notes**
>
> - Be aware, that the weekly option is not available for agents of version 11.5.0 or earlier. If in your target groups there are agents of these versions, the final status is always `Sending impossible` .
> - If you already used previous versions of CM , be aware that it is not possible any longer to define a schedule that executes *on the nth day of the month*.

   b. If you select the weekly schedule you also need to select on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one weekday.
   c. If you selected a monthly schedule you also need to select in which week of the month by selecting the respective number and on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one week and one weekday.
   d. Select the **Once daily** radio button to only execute the object once per day. Then, in the list box next to it specify the time at which it is to be run.
   e. Select the **Multiple times** radio button to execute the object more than once per day. Then, in the boxes appearing below, specify the frequency and the unit for the frequency. Check the **between** box if in addition these multiple times are to occur within a specific timeframe and define the start and end time of this interval in the newly list that appears boxes.

4. *(Optional)* If you selected the **Use Cronspec to Schedule** option fill in the values that appeared for the cronspec definition:
   - **Minute** Enter the minute value, it can vary from 0-59.
   - **Hour** Enter the hour value, it can vary from 0-23
   - **Day** Enter the day value, it can vary from 1-31.
   - **Month** Enter the month value, it can vary from 1-12 (1 is January)
   - **Week Day** Enter the week day value, it can vary from 0-6 (0 is Sunday).
   - **Weeks of the Month** Enter the weeks of the month value, it can vary from 1-5.

> **Note**

Each set of ranges can be preceded by a % sign which changes the meaning from absolute to relative number. For instance if minutes equals 29 the timer gets fired each time the absolute time ends with a number of minutes equal to 29 (for example, 11:29) whereas %20 means every 20 minutes every hour, that is, at 13:00, 13:20, 13:40, 14:00, and so on.

- Ranges are comma-separated lists. A range is made of a number eventually followed by a '-' sign and another number
- The wildcard character asterisks (*) can be used to indicate any value.

5. *(Optional)* If the schedule is not to start immediately you need to select its starting moment from the **Do you want to configure a window in which this object can run?** box.
   - **Prevent this object from running on a schedule** Select this option if you want to disable a schedule.
   - **Start the schedule immediately** Select this option if you want to start the schedule immediately.
   - **Start the schedule at next startup** Select this option if you want to activate the schedule only after the next startup of the device.
   - **Start the schedule window on** Select this option if you want to start the schedule at a specific date and time.
6. *(Optional)* If you selected the **Start the schedule window on** option you now need to select the date and time at which the schedule is to start in the boxes that appear.
7. *(Optional)* Select after how many executions the schedule is to stop. To run it without any limits select the option **Unlimited** from the list box.
8. *(Optional)* If the execution is to stop at a specific date and time check the **End on** box and select the desired values from the list boxes next to it.

Managing dynamic groups

The **Dynamic Groups** node provides access to all types of groups which are dynamically populated by the currently selected object.

This topic includes:

- Dynamic device groups
- Administrator groups populated by a directory server
- Dynamic user groups

Dynamic device groups

Dynamic device groups are available for queries, directory servers, as well as compliance rules. Depending on their location, dynamic device groups node provides different information.

The following are the ways for populating dynamic device groups:

- Device groups populated by a query
- Device groups populated by a directory server
- Device groups populated by a compliance rule

Device groups populated by a query

The **Device Groups** node displays the list of device groups that is populated by the selected query. Under this node you can also either add groups to be populated or be removed from the automatic population by the query.

Parameter	Description
Group	This column displays the list of names of all device groups that the query populates.

Device groups populated by a directory server

The **Device Groups** node displays the list of device groups which are synchronized with the selected directory server.

The table in the right window pane shows the following information about the synchronized groups:

Parameter	Description
Group	This column displays the list of names of all device groups in the standard format `entry.full directory server name` that were synchronized with the selected server.
Entry	This field displays the DN Entry of the directory server.
Last Synchronization Time	Displays the date and time at which the device group was synchronized for the last time with the directory server.

Device groups populated by a compliance rule

The **Device Groups** node displays the list of device groups that a compliance rule populates.

The table in the right window pane shows the following information about the device groups:

Parameter	Description
Status	This field displays the evaluation status of the compliance rule, possible values are `Inactive` , `Evaluated` , `Evaluation Failed` , `Not Evaluated` , `Evaluating`, and `Evaluation Scheduled` .
Name	This column displays the list of names of all device groups that the compliance rule populates.
Compliance	This field displays the type of population for the group, that is, if the group contains all devices compliant to the rule, the non-compliant ones or those that could not be evaluated for specific reasons.
Last Evaluation	This field displays the date and time of the last compliance evaluation of the object.

Administrator groups populated by a directory server

The **Administrator Groups** node displays the list of administrator groups which are synchronized with the selected directory server.

The table in the right window pane shows the following information about the synchronized groups:

Parameter	Description
Group	This column displays the list of names of all administrator groups in the standard format `entry.full directory server name` that were synchronized with the selected server.
Entry	This field displays the DN Entry of the directory server.

Dynamic user groups

Dynamic user groups are available for queries and directory servers. Depending on their location, dynamic users groups node provides different information.

The following are the ways for populating dynamic user groups:

- User groups populated by a query
- User groups populated by a directory server

User groups populated by a query

The **User Groups** node displays the list of user groups to which the query is assigned for population. This node is only available for queries of type user. Be aware that a user group cannot be assigned by free and criterion queries at the same time. Also, it can only be assigned to one query if it is a free query; it can, however, be assigned to several queries if these are defined via criteria.

The table in the right window pane shows the following information about the assigned groups:

Parameter	Description
Group	This column displays the list of names of all user groups that the query is assigned to.
Create Time	This field displays the date and time at which the assignment between the query and the user group was created in the database.

User groups populated by a directory server

The **User Groups** node displays the list of user groups which are synchronized with the selected directory server.

The table in the right window pane shows the following information about the synchronized groups:

Parameter	Description
Group	This column displays the list of names of all user groups in the standard format `entry.full directory server name` that were synchronized with the selected server.
Entry	This field displays the DN Entry of the directory server.

Managing security of an object

When an object is created, only the administrator who created the object and the *superadministrator* have access to this object. To provide other administrators registered in the database with access to it, they must be added in the **Security** tab of the respective object with the

type of access defined. If no access is specifically defined, they will not be able to see or access it. Access can be added directly in the **Security** tab or it can be added through the Security Profile of the respective administrator.

The table of the **Security** tab displays the following information about the administrators and administrator groups with access to the specific object:

Parameter	Description
Administrators	This column lists the names of all administrators with access rights to this object.
Via Administrator Group	The fields in this column display if the access rights to this object are assigned to the administrator via a group membership. If this is the case, the column displays the name of the administrator group. If not, the field is empty. Access rights that are assigned through groups may not be modified.
Via Query Result	This column indicates if the access rights to this object are assigned via the result of a query, that is, a query collecting the administrators with access rights to the object. This field either displays the name of the query or an empty field. Access rights assigned through queries may not be modified.
As Member of	The fields in this column display if the access rights to this object are assigned to the administrator via a folder membership. If this is the case, the column displays the name of the administrator group. If not, the field is empty. Access rights that are assigned through folders may not be modified.
Read Access	This field shows if the administrator has read rights to the object. The possible values are **Allow** and **Deny** .
Write Access	This field shows if the administrator has write rights to the object. The possible values are **Allow** and **Deny** . With write access an administrator can manipulate the object in any way such as create new children, delete the object or modify it.
Assign Access	This access type defines if the selected administrator can assign this object to another object such as a operational rule or a transfer window. The possible values are **Allow** and **Deny** .
Direct Access Acknowledgement	Indicates if authentication is required when accessing the device via Direct Access.
Remote Control Acknowledgement	Indicates if authentication is required when accessing the device via Remote Control, and if yes for which specific situations.
On Dynamic Object	This column indicates if the access rights of the administrator are on the object itself or on the results /members of the object. The field is empty if the rights are on the object itself, otherwise it displays "Yes".

To add administrator or administrator group to assigned object

1. Select the **Security** tab of the object in the right window pane.
2. Select **Edit > Add Administrator** .
   The **Assign Administrators and Administrator Groups** dialog box appears and displays the list of all administrators and administrator groups to which you are granted at least read rights.
3. Select the administrator or administrator group to be added to the security settings of the object and click **OK** to add it.
   The **Properties** dialog box appears on the screen, displaying the possible access types for the selected administrator.
4. Select the respective radio buttons to either **Allow** or **Deny** read and write access of the selected administrator to the current database object.

5. Click **OK** to confirm the definitions and close the window.

Managing graphs of an object

The graph in BMC Client Management is used to display the objects in the form of an image showing their direct connections.

The graph shows the following types of connection:

- Network topology in the form of your BMC Client Management organization
- Network connections by IP addresses
- Physical network connections between the inventory assets
- Hierarchical connections between the devices and their different roles

The graph is available for the following objects and views:

- Device topology
- Device groups
- User groups
- OSD roles
- All types of inventory

This topic includes:

Device topology graph

The **Device Topology** graph works quite differently from the traditional interfaces. You see a great many objects, each one representing a piece of the hierarchical data, joined by lines or arcs called links. You can see objects linked to their children all the way out to a horizon and to their parents back to the root object.

The graph shows data structured as objects and links. The objects are the computers on your network and the links are the relationships between these in the hierarchy. The object information is conveyed most fundamentally through the text on the object label, that is, the name of the computer and the icon next to it identifying the computer's device type. Each displayed hierarchy has its unique root object, from which all other objects descend. The root object is defined through the computer that is currently selected in the left window pane, thus this can be **Device Topology**, if the main topology node is currently selected, or the master server, or any other relay or client which is selected.

The links, as already mentioned before, connect the objects and ensure their connectivity to the root. They make it clear which objects are grouped under one parent node. When a link is removed, the parent node is no longer related to the child node. If the child node has no other parents, it is removed from the tree.

This view is only available directly under the main **Device Topology** node in the **Graph** tab.

BMC Client Management topology

To display the network topology of your infrastructure, select the respective option from the **View** box at the top left of the right window pane.

In this view you can display different parts of your network in the same way as via the **Network Topology** graph. However in this view your devices are reflected according to their physical connections in the network. The view displays all devices that have an IP address, that is, it will also display printers, routers, switches, and so on. For more information about the options of this graph, refer to the **Network Topology** paragraph following.

Network Topology

Through the **Device Topology** / **Network Topology** graph you can browse very large amounts of hierarchically arranged data. You can also draw items of interest into focus without losing their context even in a tree with thousands of items. This graph makes accessing large datasets a far more intuitive experience than is available with more traditional interfaces such as the familiar expanding and collapsing vertical trees used in many Windows applications such as the Windows Explorer.

Connectivity Topology

The **Connectivity Topology** node represents the device topology by IP addresses for unmanaged devices via the graph view. It shows the physical connections of the inventoried devices with their parents and children, identified by their IP addresses. Connections with devices which were discovered during a scan but are now inactive, for example, the connection was unplugged, appear as dotted lines. To hide the children click the small minus symbol at the left bottom of the IP address, to show children click the small arrow at the same location. The discovered devices are identified as well by their type icon, that is, an orange device icon with the operating system of the device.

Graph for other BMC Client Management objects

The **Graph** displays all the objects of the current node found on the members in the selected view in the form of a hierarchy image. Most objects will be shown in this type of graph with three levels for each main object of the entry:

- Attributes
- Attribute values
- Device on which the attribute and its value was found

Actions on graphs

On a graph view, you can perform the following actions:

- Expanding and collapsing an object hierarchy
- Zooming and moving the graph view
- Locating an object in the graph view
- Dragging an object
- Viewing a node
- Finding a node in the tree
- Switching the layout

Notes

- By default, the graph view displays first level of nodes.
- If there are more than 20,000 nodes to display in a graph view, BMC Client Management console performance may slow down.

Expanding and collapsing an object hierarchy

- Double-click an object to expand the hierarchy and view its subnodes.
  The object is highlighted with a blue border and its subnodes are displayed.
- Double-click an object with expanded hierarchy view to collapse the hierarchy and hide its subnodes.

Tip

Double-click the root node to collapse all the subnodes in the hierarchy.

Zooming and moving the graph view

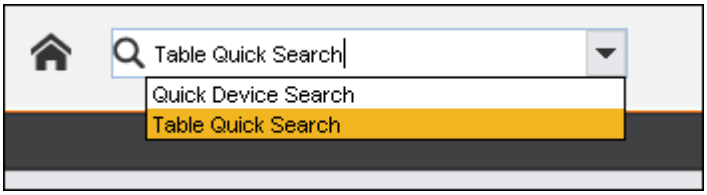
When you have a large network, the complete representation of it in the form of a graph can be very dense and difficult to interpret. The object, which is currently the focus of your attention, might be at the farther end of the hierarchy and thus only represented at the edge of your window. To have a closer look at it, you can zoom in the graph view to bring the desired object in the center.

- Click the zoom in ( ) button or use your pointing device to zoom in the view.
  After zooming in, if the object of your interest has moved out of the view, drag the graph to bring the object back in the view.
- Click the zoom out ( ) button or use your pointing device to zoom out the view.
  You can also click the **Reset** button to reset the graph to default view.

Locating an object in the graph view

To locate a specific object from a large network graph view, you might need to search a specific object. A node can be found only if the graph has been deployed before. For example, if a device to search is located under a relay and the user has not expanded the relay (double-clicked the relay) before to display the subnodes, the device will not be found.

1. Select the **Table Quick Search** option from the Search list.



2. Specify the starting letters or exact name of the object that you want to search and press **Enter**.
   All the objects matching the search string are highlighted in the graph with a red border. For example, searching for **10** in Network Topology view highlights all the objects that have IP address starting with **10**.

Dragging an object

To find a specific object in the graph, you can move the graph within the window to locate it, especially if the network represented is very large. The view will remember the position of your graph even when you access other objects and then come back to the topology tree. You can simply drag an object across the screen with your pointing device. The graph will follow the cursor across the screen. The objects located around the selected object will follow as well and adapt their position relative to the object and the current location in the window.

Viewing a node

If you spot a node in the graph for which you need more information, you can use this function to view all the information available on the specific node.

- To view details of a node, right-click the desired node in the graph and select **View Node** . Under the **Search** node in the left window pane, the selected node will be shown with all its available subnodes.

Finding a node in the tree

If you spot a node in the graph of which you want to know the location in the tree in the left pane, you can use this function to expand the tree up to the selected node.

- To find a specific node, right-click the desired node in the graph and select **Find Node** . Under the main node in the left pane, the tree will expand up to the desired node, thereby revealing its location and showing all its available subnodes.

Switching the layout

Depending on the final aim for which the graph displays, the graph can be shown in different types of layouts, to display the network hierarchy from different angles. The focus is preserved through these layout changes and the currently centered object remains the center of the focus. The following are the possible layouts:

Layout	Description
Left (Horizontal)	The root node is located at the left and the hierarchy extends to the right side of the window with the last children at the far right border.
Top (Vertical)	The root node is located at the top and the hierarchy extends below the master server towards the bottom of the window with the last children near the lower border.

- To switch from one type of layout to another, right-click anywhere in the graph view and select **Switch Layout** .
  The graph layout changes from your current layout to the next. Repeat this step until the layout you are looking for appears.

Managing console preferences

The **Preferences** window provides you options to individually configure the screen appearance and other default settings of your BMC Client Management console.

You can configure the preferences either via **Options > User Preferences** or directly from the tool bar.

You can manage the following preferences:

- Managing console appearance and general preferences
- Managing table preferences
- Managing object assignment preferences
- Managing email preferences
- Managing patch deployment preferences
- Managing alert preferences
- Managing miscellaneous preferences

Managing console appearance and general preferences

The following topics are provided:

- Managing general preferences
- Managing font preferences

Managing general preferences

In the **General** tab, you can configure the following preferences:

Parameter	Description
Console appearance	
Look'n Feel	The console comes with a number of predefined Look'n'Feel versions for the outward look of the console. Select your preferred look in this list.
Language	The console also provides a number of different languages. Currently available languages are French, German, Japanese, Spanish, UK English and US English. Select the desired language from the list. When the console is opened for the first time and no preference have been set yet, it will select the language of the local operating system, if it is one of the previously listed languages, if not the default language will be UK English.
Time Zone	The console provides you with the possibility to change the time zone for your console appearance. By default when the console is opened for the first time, the operating system time zone is used.
System Timezone	This option always will use the time zone which is selected for the local operating system. This is also the default option.
Custom Time Zone	Select the radio button to the left of the list box and then select the time zone you would like to use as a base for all CM operations via the console.
Date Format	This box defines the default date and time format which is used for any display of time (modification time, creation time, etc.) within the console.
Frequently Used Nodes	
Number of nodes to be remembered	Define in this box how many of the most frequently accessed nodes the console should remember. The default value is 10. You can access any of these nodes by selecting the **View > Frequently Used Nodes** menu item. The list next to the menu item displays the list of your most frequently used nodes.
Create new Object	
Open Properties Dialog Box	This check box defines if the **Properties** window is opened when you create any new object in the console. Through this window you can directly define the name and any other object specific data. By default the box is checked meaning the window is opened. If you clear the box new objects are created in the database and displayed in the respective table with their default name and settings.
System Settings	
Auto LockDown Delay (sec)	This entry defines the maximum time that can elapse without any input to the computer by the keyboard or mouse before the console is locked down for security reasons. If that time has elapsed the user/administrator must enter his login again to unlock the console. The default value for this number is 600 seconds.
Processing Window Delay (sec)	This entry defines how many seconds of processing must elapse before the processing window is displayed. This window informs the user that a process is currently executing. The default value for this option is 3 seconds. If you enter 0 the option is deactivated and no window will be displayed.

Managing font preferences

In the **Fonts** tab, you can set select the size and type of font to use.

Parameter	Description
Font Type	This list provides you with all fonts which are available to the console window. Click a font to select it.
Font Size	Select the size for the font in this list.

Parameter	Description
Font Preview	The **Font Preview** box appears a **Sample** for the selected font and size.

Managing table preferences

The **Tables** tab is for setting the properties of the tables in the right window pane of the console. This topic includes:

- Table-Row Settings
  - To modify the color of table elements
- Automatic Refresh
- Paging Settings
- Table elements colors settings

Table-Row Settings

In this section you can define the appearance of the tables in the console window. The following options are available:

Parameter	Description
Color of Odd Lines	The box next to this label displays the color of the first and each unevenly numbered row of the tables in the right window pane.
Color of Even Lines	The box next to this label displays the color of the second and each even numbered row of the tables in the right window pane.
Grid Color	The box next to this label displays the color of the table grid.
Row Height	This text box defines the height of the table rows in pixels. To modify the height simply change the displayed value to your desired value. The default row height is 9 pixels.

To modify the color of table elements

1. Click **Modify** next to the color box.
   The **Choose Color of Line** dialog box appears on the screen.

Tab	Description
Swatches	In this tab you can select the color by simply clicking one of the proposed colors. The **Recent** box appears the last choices that you made.
HSB	In this tab you can select your color by either entering the HSB code in the corresponding boxes to the right or by moving the pentagon to a color group and clicking to select a color. In the lower right side the RGB equivalent of the currently selected color appears.
RGB	In the RGB tab you can select the row color by either moving the three pentagons until the desired color is displayed or by entering the RGB code in the corresponding boxes to the right.

2. Select the desired color from one of the tabs.
3. Click **OK** to confirm.

The selected color is chosen for the selected table element.

Automatic Refresh

The preferences box provides each administrator with the possibility to define the refresh rate of the different console tables. Refreshing a view is not linked to the node but to the selected view. Its type of refresh is indicated through the color in the far right field of the status bar at the bottom of the console window.

The field is in the form of a progress bar, and the degree of filling indicates the rate at which the view is refreshed, that is, when the field has completely been filled in, the table in the right window pane will be automatically refreshed. If rows are selected in the table the auto-refresh is deactivated until the selection is removed.

Color	Description
	No automatic refresh is defined for this view.
	This view is refreshed via normal automatic refresh.
	This view is refreshed with fast automatic refresh.
	There is no connection to the master.

Static views such as the main console view or the **Managed Applications** node do not have automatic refresh, to manually refresh this view select the **View > Refresh** menu option.

Parameter	Description
Regular Automatic Refresh	In this section you can activate the regular refresh for dynamic tables such as the Events view or the Members view of the different objects.Check the **Enable Regular Automatic Refresh** box to enable the regular automatic refresh of dynamic tables. By default this option is enabled and set to automatically refresh the views every 30 seconds. You can modify the default value through the speed bar below the check box. To increase the refresh interval move the bar to the right. The selected value is indicated through the number displayed next to the **Enable Regular Automatic Refresh** check box. The colored field to its right indicates by which color the regularly refreshed tables can be recognized ().
Fast Automatic Refresh	In this section you can enable or disable the fast refresh for quickly changing dynamic tables, such as tables which contain a status, for example, Assigned Operational Rules and Assigned Devices.Check the **Enable Fast Automatic Refresh** box to define a personalized fast refresh rate for these console views. By default this box is checked and the value defined is 30 seconds. After checking this box you can modify the interval of the fast automatic refresh through the speed bar below the check box. To increase the refresh interval move the bar to the right. The selected value is indicated through the number displayed next to the **Enable Regular Automatic Refresh** check box. The colored field to its right indicates by which color the regularly refreshed tables can be recognized ( ).

Paging Settings

This part defines the volume of the content displayed in the tables of the console.

Parameter	Description
Table Rows per Page	The value in this text box defines the number of rows of the tables in the right window pane. This value is only applicable to the individual objects of the database, it does not include the subnodes that may be found under a node and will be listed in this table, too. For example. In the **Members** tab of the **Device Groups** node you will find the list of subnodes, which are **Inventory** , **Assigned Operational Rules** , **Assigned Queries** , **Directory Server** and

Parameter	Description
	Alerts and Events , plus all devices that are a member of this group. The number of rows defined in this text box will only affect the list of member devices displayed in this table. If you defined the number of rows to 5 and your group has 7 device members, the first page of the table in the right pane will only display the first five members. To see the remaining two members you must click **Next >** at the bottom of the pane.

Table elements colors settings

This task presumes that the **Preference** window is opened and the **Tables** tab is selected.

To change the color of table elements, proceed as follows:

1. Click **Modify** next to the color box.
   The **Choose Color of Line** dialog box appears on the screen.

Tab	Description
Swatches	In this tab you can select the color by simply clicking one of the proposed colors. The **Recent** box appears the last choices that you made.
HSB	In this tab you can select your color by either entering the HSB code in the corresponding boxes to the right or by moving the pentagon to a color group and clicking to select a color. In the lower right side the RGB equivalent of the currently selected color appears.
RGB	In the RGB tab you can select the row color by either moving the three pentagons until the desired color is displayed or by entering the RGB code in the corresponding boxes to the right.

2. Select the desired color from one of the tabs.
3. Click **OK** to confirm.

The selected color is chosen for the selected table element.

Managing object assignment preferences

In the Object Assignment tab, you can set defaults for the assignment and unassignment of the BMC Client Management objects and a the default operational rule schedule. You can manage the following object assignment preferences:

- Device Assignments and Unassignments
- Operational Rules
  - Modifying the default schedule
- User Assignments

Device Assignments and Unassignments

Actions such as assigning or unassigning require activation to make them valid. This frame defines the setting for the type of activation.

Parameter	Description
Activation Type	Enables setting the activation for assigning, for example, a device group. The options include: • Prompt: Activations will be accompanied by a message box requesting that the user confirms activation should go ahead using the default schedule.

Parameter	Description
	• Automatic: This type enables full automation. No user interaction is required. You cannot advertise packages with this type of assignment activated. • Manual: The user fully controls the activation. The default activation type is **Prompt**.

Operational Rules

The elements in this box allow the administrator to manage the schedule for operational rules.

Parameter	Description
Default Schedule	Defines the default schedule for the execution of the **Operational Rules** . If you do not define your own default schedule, the following schedule is set as the default: Immediate execution, stop after one execution.
Assignment Date	The option boxes in this panel allow you to change the default assignment from immediate to a specific time.
Warning Threshold	This parameter defines the maximum number of targets, devices or users, that can be assigned without warning. If the threshold is reached or passed a confirmation window appears on the screen and you need to confirm the assignment or you can cancel it. This value is applicable in the same way when reassigning or activating an operatinal rule or publishing it to the targets. The default threshold is set to 1000 targets. To deactivate this function enter **0** (zero). This value is also applicable to device and user groups. If the member count of all assigned groups is higher than the defined threshold, the message window also appears. This warning is used to make you aware, that you are executing a large number of assignments which might impact the performance of your systems. It allows you to cancel the assignment and possibly defer it to a less critical time.

Modifying the default schedule

1. Click **Modify** next to **Default Schedule** in the **Operational Rules** panel.
   The **Scheduler** window appears.
2. Make the desired changes to the schedule.
3. Select one of the following options for the question **When do you want this rule to be run on devices?** to define when the actual execution is to be launched:
   - **Right now** Select this option to start the execution immediately.
   - **At Startup** Select this option if the operational rule is to be executed every time the device is started.
   - **At Session Startup** Select this option if the operational rule is to be executed every time the agent is started
   - **At Session Close** Select this option if the operational rule is to be executed every time a session is closed.
   - **Run repeatedly on a schedule** Check this option if if the execution is to be scheduled repeatedly.
   - **Use Cronspec to Schedule** Select this option if the execution schedule is to be created via a cronspec.

   Depending on the choice you make in this list box, additional options become available.
4. *(Optional)* If you selected the **Run repeatedly on a schedule** option fill in the boxes that appear to create the execution schedule:

a. Select if the schedule is to run every day, week or month.

> **Notes**
>
> - Be aware, that the weekly option is not available for agents of version 11.5.0 or earlier. If in your target groups there are agents of these versions, the final status is always `Sending impossible` .
> - If you already used previous versions of CM , be aware that it is not possible any longer to define a schedule that executes *on the nth day of the month*.

b. If you select the weekly schedule you also need to select on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one weekday.
c. If you selected a monthly schedule you also need to select in which week of the month by selecting the respective number and on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one week and one weekday.
d. Select the **Once daily** radio button to only execute the object once per day. Then, in the list box next to it specify the time at which it is to be run.
e. Select the **Multiple times** radio button to execute the object more than once per day. Then, in the boxes that appear below, specify the frequency and the unit for the frequency. Check the **between** box if in addition these multiple times are to occur within a specific timeframe and define the start and end time of this interval in the list boxes that appear.

5. *(Optional)* If you selected the **Use Cronspec to Schedule** option fill in the values that appeared for the cronspec definition:
   - **Minute** Enter the minute value, it can vary from 0-59.
   - **Hour** Enter the hour value, it can vary from 0-23
   - **Day** Enter the day value, it can vary from 1-31.
   - **Month** Enter the month value, it can vary from 1-12 (1 is January)
   - **Week Day** Enter the week day value, it can vary from 0-6 (0 is Sunday).
   - **Weeks of the Month** Enter the weeks of the month value, it can vary from 1-5.

> **Note**
>
> Each set of ranges can be preceded by a % sign which changes the meaning from an absolute to a relative number. For instance if minutes equals 29 the timer gets fired each time the absolute time ends with a number of minutes equal to 29 (for example, 11:29) whereas %20 means every 20 minutes every hour, that is, at 13:00, 13:20, 13:40, 14:00, and so on.

- Ranges are comma-separated lists. A range is made of a number eventually followed by a '-' sign and another number
- The wildcard character asterisks (*) can be used to indicate any value.

6. *(Optional)* If the schedule is not to start immediately you need to select its starting time from the **Do you want to configure a window in which this rule can run?** box.
   - **Prevent this object from running on a schedule** Select this option if you want to disable a schedule.
   - **Start the schedule immediately** Select this option if you want to start the schedule immediately.
   - **Start the schedule at next startup** Select this option if you want to activate the schedule only after the next startup of the device.
   - **Start the schedule window on** Select this option if you want to start the schedule at a specific date and time.
7. *(Optional)* If you selected the **Start the schedule window on** option you now need to select the date and time at which the schedule is to start in the boxes that appear.
8. *(Optional)* Select after how many executions the schedule is to stop. To have it run without any limits select the option **Unlimited** from the list box.
9. *(Optional)* If the execution is to stop at a specific date and time check the **End on** box and select the desired values from the list boxes next to it.
10. Click **OK** to confirm the modifications.
    The default schedule is modified.

User Assignments

This section defines the default settings for assignments with users and user groups as targets.

Parameter	Description
Assign to Primary and Secondary Users (only primary if not selected)	Check this box if the assignments are applicable to the secondary users and the primary user. If not selected the assignments will only be carried out for the primary user. This option is only applicable if the **Deploy to devices linked to users** option is selected during assingment.
Operational Rule Assignment Policy	Select from this list the type of policy to use for the user assignments: • **Assign at User Login** : the assignment of the operational rules is carried out when the user logs on to a device. • **Assign at User Logout** : the assignment is carried out when the user logs off. • **Assign Immediately** : the assignment is carried out immediately after defining the assignment. • **Assign with Default Assignment Date** : the assignment is carried out according to the defined default schedule. This option is only applicable if the **Deploy to devices linked to users** option is selected during assignment.

Managing email preferences

The parameters in this tab define the basic settings of the mail server in your organization.

This information is required to be able to send e-mails via the respective **Tools** menu option. The following parameters must be defined for this:

Parameter	Description
Server Name	Defines the name of the mail server to which all mail is set for routing, the default is **localhost** .
Port	Defines the port number of the mail server, the default value is 25
Authentication	This box defines if the mail server requires authentication for its communication, possible values are **Force Authentication** , **Authenticate if possible** or **Never Authenticate** .
User Name	Enter into this box a valid login to the mail server. This can be any login, not necessarily that of the user defining his preferences via these options.
Password	The corresponding password.

Managing patch deployment preferences

The parameters of of the subtabs of the Patch Deployment tab define the basic patch group settings and behavior i.e., the default values that are used for creating patch groups on this console. The values entered here are prepopulated in the respective boxes whenever a new patch group is created, either manually or via the wizard.

Parameter	Description
Preinstallation	
Information Window	This option defines if a pop-up menu appears of the target device, informing the remote user that patches will now be installed and applied on his computer.
Message to Display	This is a free text box in which you can enter the message to be displayed on the screen of the target device. If no text is entered here a default message (The system is about to apply the security update.) will be displayed. This message is localized in all console languages. If you enter your own text here it will not be localized and will appear as entered on all operating system languages.
Allow User to Extend Countdown Timer	Check this box if the user can extend the countdown timer before the patch installation will automatically start.
Initial Countdown (sec)	This box defines in seconds the time before the information window that displays is auto-validated to allow the patch installation to proceed. To deactivate the option 0 must be set.
Timer Incrementation Value (min)	This value in minutes defines the interval by which the countdown timer is incremented each time the user decides to extend it, if he was allowed to do so by the preceding option.
Timer Maximum Extension Value (min)	This value defines the maximum interval the countdown timer can be extended. If for example the initial value is 2 minutes, the user can each time extend it by 2 minutes as well, and this value is set to 5 minutes, the user can extend the countdown once, 2 min initial 2*2 min extension makes 6 minutes which is higher than the defined 5 minutes.
Installation	
Quiet Mode	This option displays if the installation of the patch group's patches is to be executed without the remote user being aware of it. Otherwise the default dialog boxes concerned with patch installation appears. By default this value is set to *Yes* .

Parameter	Description
Stop On Error	With this option you can define if the installation of patches is to continue even if one of the patches of the group has failed to install. By default this option is set to `true` , continue the installation.
Lock mouse and keyboard on client device	Defines if the mouse and keyboard on the target device are blocked during the patch installation, that is, the user logged on to the local device may not execute any other operations during the installation.
Locking Message	Enter into this box the message to be displayed on the screen of the target device to inform the user what is happening on his device. If no text is entered here a default message appears.
Force Installation	This option allows you to force the installation of a patch group again even if it was already installed. This can be useful, if for example a problem occurred in the network or a device crashed during the installation.
Patch Group Options	In this section, you need to define the type of installation for the patch. If the patch to install is not applicable to any of the Microsoft Office products, select **No Specific Office Install Options** from the drop-down list. Otherwise, you have the following options for Microsoft Office patches: • **No Specific Office Install Options**: This option indicates that the patch to be installed does not concern any Microsoft Office product. • **Administrative Installation**: This option should be used if Microsoft Office was installed via an administrative installation. For this option to work, the path to the location of the Microsoft Office DVD or share must be entered into the **Path** box together with a valid user name and password. • **Full File Installation**: This installation option is for a complete install of Microsoft Office without any DVD being required. • **Mixed Installation:** For the mixed installation, the path to the location of the Microsoft Office DVD or share might be necessary. Enter it into the **Path** box together with a valid user name and password.

Path	Enter into this box the location of the Microsoft Office installation source. This can be:
	• a local path. For example, `C:/patchex/MS/office/office2010`
	• a network share in either of the following formats:
	  • *[IpAddress]\\[SHARE]\MSOFFICE2010*. For example, *FD43-0-0-0-8C84-4BAD-D413-DD68.ipv6-literal.net\CDSERVER\MSOFFICE2010*
	  • *\\\[IpAddress]\\[SHARE]\MSOFFICE2010*. For example, *\\192.155.1.24\CDSERVER\MSOFFICE2010*

User	If the source location is on a device/share that requires identification you must enter here a user name with which it can be accessed. Otherwise you can leave the text box empty.
Password	If identification is required enter here the password for the specified login.
Confirm Password	Re-enter the password for confirmation.
Patch Job Options	In this section you can define additional options specific to patch jobs.
Retry Attempts	The number of installation retries before the patch is shown as failed in the Console. Updating the ConfigFiles reinitializes this parameter to 0 and the installation process starts again.
Reboot	
Reboot Type	This list box appears if a reboot is previewed after the installation of the last patch package of the patch group. Possible values are `No reboot` and `Reboot after deployment` . Be aware that if you do not reboot after installation when a reboot is expected by one of the patches installed, this patch will still be seen as missing even if you force a scan after install by the following option. If no user is logged on to the target device the reboot will be automatically launched. If there is an open session that is locked the reboot mechanism will wait until the session is unlocked before displaying the respective window and launching the reboot.

Parameter	Description
Shutdown After Reboot	Check this box, if the device is to be shut down after the required reboot after the patch installation is completed.
Display Reboot Dialog	**Check this box if a pop-up window is to be displayed on the target screen informing the local user of the imminent reboot of his device.**
Customize Reboot Message	This text box contains the title of the window which will be displayed on the screen of the remote device before the device is shut down, for example, *Maintenance Shutdown* .
Shutdown Initiated by User	This parameter specifies which user initiated the device reboot; for example *Admin* or *Patch Administrator* . This information is displayed in the defined reboot pop-up menu.
Enable End-User Interaction	**The following boxes are only applicable for this option:**
Allow User to Cancel Reboot	Specifies if the user can definitely cancel the reboot of the concerned device.
Reboot Directly after Disconnecting	This option defines if the user can decide to immediately reboot the device, without awaiting the end of the specified countdown.
Force reboot if Session is Locked	This option defines if the reboot is to be executed even if the session is locked. By default this option is deactivated, that is, the reboot will wait until the session becomes unlocked.
Allow User to Extend Countdown Timer	This option defines if the user can extend the time before the device is rebooted.
Initial Countdown Timer (min)	The value in this text box indicates the waiting time in minutes between the pop-up menu first displays and the actual initialization of the reboot of the device. The default value is *2* minutes.
Countdown Timer Increment (min)	This value in minutes defines the interval by which the countdown timer is incremented each time the user decides to extend it, if he was allowed to do so by the preceding option. The default increment time is *2* minutes.
Countdown Timer Maximum (min)	This value defines the maximum interval the countdown timer can be extended. If for example the initial value is 2 minutes, the user can each time extend it by *2* minutes as well, and this value is set to *5* minutes, the user can extend the countdown once, *2* min initial *2*2* min extension makes *6* minutes which is higher than the defined 5 minutes. The default value of this option is *5* minutes.
Only Reboot if Requested by Patch	This option defines if the device is always rebooted after a patch installation or only if a patch specifically requests it. By default this option is activated. If this option is deactivated a reboot occurs if at least one patch successfully installed, independently of whether it requires a reboot. If this parameter is activated a reboot occurs only if at least one patch of a patch group or a patch job installed successfully and at least one of the successfully installed patches requires a reboot. If none of them do so, the device is not rebooted. No reboot occurs in either case if all patch installations of the group or job fail.
Reboot after Logoff	This option defines that the reboot of the device is effected only once the user has logged off the device.

Modifying the Pop-up window logos

If thus configured, a pop-up window appears on the remote device after the patch installation has finished and before the restart is launched, providing a number of options as defined in the restart parameters. You can also modify the logos of this window to those used by your organization, or any others. To do so, proceed as follows:

1. Prepare the following images, and ensure they are all there, all five of them are needed. The images must be in the .BMP format.
   - TinySized.bmp - 574 x 379 pixel
   - SmallSized.bmp - 574 x 455 pixel
   - MediumSized.bmp - 574 x 509 pixel
   - FullSized.bmp - 574 x 572 pixel
   - RebootAfterLogOut.bmp - 574 x 274 pixel
2. Copy these images to the following directory: `<InstallDir>/master/data/core/res`.
3. ALso, copy these images to directory `<InstallDir>/client/data/core/res` on all client devices.
   Once these images are saved to this location, they will be used in the safe restart pop-up windows when they are displayed on the target screens.

You have successfully modified the logos of the pop-up window that displays on the remote device after a patch installation to inform the user of the required restart.

Managing alert preferences

The **Alert Management** tab allows you to define the alert settings for BMC Client Management events.

As a prerequisite for these options, you must have an email address configured in your administrator account and the email settings in the **System Variables** must be specified otherwise these settings are not available. For more information, see Managing email settings.

Parameter	Description
Check for alerts every	Check this box to activate the alert check function. If this option is activated you need to define the frequency at which the agent checks for new alerts in the box to the right. If, for example you enter *60* minutes, the administrator receives an email every hour, if, within that hour, new alerts have arrived. This email contains the list of the alerts generated during the last hour with their basic information, such as the device on which it occurred, the severity, the category, etc. When this option is first activated, only new alerts are sent, any alerts that existed before the activation are ignored.
Send multiple alerts in one email	Defines if alerts are grouped into one single email (default). If this option is deactivated, you receive one email for each generated alert.
	Click the arrow icon next to the event category to define for which events you want to receive alerts. This will expand the respective section and display all its available events. Check the boxes of the events for which alerts are to be generated and sent. You can select as many events as you want. Below you can see the list of available events.

Parameter	Description
Send me an email when the following occurs:	

Events available for notification

The following events are available for notification:

- BCM application
- Updates
- Directory synchronizations
- Discovery and inventory
- Applications and application licensing
- Compliance
- Agent-based monitoring

BCM application

The events and alerts of this section are concerned with the general workings of the BCM agents and licensing problems.

Parameter	An event notification is generated whenever
Error detected on BCM Agent	the agent on a client or relay has a problem executing correctly or has stopped working. The alert is automatically closed once the agent is executing again properly.
Error detected on BCM Master	the agent on the master has a problem executing correctly or has stopped working. The alert is automatically closed once the agent is executing again properly.
BMC Client Management license expired	a BMC Client Management license that you have purchased passed its expiry date. The alert is automatically closed once the respective license is valid again.
BMC Client Management license exceeded	a BMC Client Management license that you have purchased exceeds its number of allowed objects created in the database. The alert is automatically closed once the respective license is valid again.

Updates

The events and alerts of this section are concerned with the update status of different functionalities.

Parameter	An event notification is generated whenever
Installation of updated Patch Knowledge Base	the patch knowledge base was successfully updated to the new version.

Directory synchronizations

The events and alerts of this section are concerned with the synchronization between groups and directory servers.

Parameter	An event notification is generated whenever
New administrator discovered in directory server	the agent discovered that the directory server OU with which one of your administrator groups is synchronized has a new administrator, you should resynchronize with it.
New device discovered in directory server	the agent discovered that the directory server OU with which one of your device groups is synchronized has a new device, you should resynchronize with it.
New user discovered in directory server	the agent discovered that the directory server OU with which one of your user groups is synchronized has a new user, you should resynchronize with it.

Discovery and inventory

The events and alerts of this section are concerned with the individual devices in the network and their agent and connection status.

Parameter	An event notification is generated whenever
New device without agent discovered	a new device on which no BCM agent is installed was discovered in your network.
New device with agent discovered	a new device on which an BCM agent is already installed was discovered in your infrastructure.
A device's software has changed	the software inventory of at least one device has changed.
A device's hardware has changed	the hardware inventory of at least one device has changed.
An agent has changed relay	a device in your infrastructure has changed its direct parent.
A device's network settings have changed	one or more parameters of a device's network settings have changed.
A computer or device lost contact	a device in your network has lost contact with its parent or is in general not reachable. The alert is automatically closed once the device is contactable again.
A device was deprecated	a device has reached the end of its useful life and was deprecated, that is, it was physically removed from your infrastructure.

Applications and application licensing

The events and alerts of this section are concerned with application license monitoring and prohibited managed applications.

Parameter	An event notification is generated whenever
Software license count maximum exceeded	an application is newly installed on a device but there are no more licenses for it available. The alert is automatically closed once the respective application license is valid again, that is, additional licenses are purchased or the application is removed from the device.
Software license expiration date exceeded	an application with a time license is found on at least one device in your network of which the final license date has expired. The alert is automatically closed once the respective application license is valid again.

Parameter	An event notification is generated whenever
Software license expiration threshold exceeded	the threshold of a licensed application was reached, at which point you are informed that almost all available licenses are now in use.
Underinstalled licensed software	an application is found for which there are still licenses available, that is it can still be installed on more devices. The alert is automatically closed once all available licenses of the application are installed.
Software license count threshold exceeded	The installed application base approaches the specified threshold at which notification is required. For example, if 100 licenses are available and the threshold is set to 80%, an alert is generated when the application is installed for the 80th time. This might be the time to consider purchasing additional licenses. The alert is automatically closed once the installed application base falls below the respective application license threshold again, that is, additional licenses are purchased or applications are uninstalled, for example, from devices on which they are no longer required.
A prohibited application was started	an application is started on a device on which its execution is prohibited.

Compliance

The events and alerts of this section are concerned with compliance.

Parameter	An event notification is generated whenever
All Defined Custom Compliance Alerts	an alert that was defined for device compliance is generated. Many of these alerts can be closed automatically once the criterion that caused the alert on the device matches its requirements. For more information about the available alerts and how to define them refer to the *BMC Compliance Manager* manual.

Agent-based monitoring

In this section you can select which operations rule steps are to send event notifications when they are generating alerts.

Parameter	An event notification is generated whenever
Check URL Availability	the step finds that the URL that it verified is not reachable. Once the step finds the URL reachable again the alert is closed automatically. If the URL in the step is changed, the first alert is closed automatically and a new alert is generated if the new URL is not reachable either.
Check Windows Events	the step finds a Windows event entry that contains either the specified string or has the specified event ID.
Check Running Process	the step either does not find the specified process or could not terminate it, if this was requested. The alert is automatically closed once the process can be found (and terminated).
Advanced Process Execution Check	the step does not find the specified process. The alert is automatically closed once the process can be found.
	a custom alert is generated by the step.

Parameter	An event notification is generated whenever
Generate Custom Alert	
File Analysis via Regular Expression	the step finds a match for the specified regular expression in the listed files.
Check Installed Software	the step does not find the specified software installed on the target. The alert is automatically closed once the specified software is found installed on the target.
Advanced Installed Software Check	the step does not find the specified software installed on the target. The alert is automatically closed once the specified software is found intalled on the target.
Service Execution Check	the step finds that a process that it has verified is not running. The alert is automatically closed once the specified service is found executing.
Low Disk Space	the step finds that the free disk space has fallen under the defined percentage limit on the target device. The alert is automatically closed once the step finds enough free disk space.
Check Disk Space	the step finds that there is less free disk space on the target device than defined in the step. The alert is automatically closed once the step finds enough free disk space.
The total size of the memory has changed	the total size of the memory on a specified device has changed.

Managing miscellaneous preferences

The **Miscellaneous** tab define specifics for miscellaneous objects and functionalities of BMC Client Management.

Inventories:

The item in this box define specifics for all different types of inventories collected in BMC Client Management - Inventory . It has the following parameter:

Parameter	Description
Inventories	
Display Fields with an Empty Value	This parameter specifies if columns which contain no value for any instance due to the value not being recovered (for example if the value is not applicable to the operating system) are to be displayed in the table anyway. By default this box is checked, indicating that yes, empty fields are displayed in all concerned tables.
Advance Search	
Case Sensitive	This parameter specifies if any search conducted in the console is to be take into account the different cases. By default this option is not activated, that is, searches are not case sensitive. If the option is activated, case sensitivity will be applied to all searches in the **Search** table, under the **Search** node, the patch knowledge base and the bulletin filters. Be aware, that this option will not work if the database you are using is not defined as case sensitive.
Trees	

Parameter	Description
Number of mouse clicks to expand a node	This box defines the number of clicks with the left mouse button are needed to open a node in the hierarchy tree on the left. Possible values are 1 and 2, by default one click is defined. Closing a node always requires a double-click no matter the value entered here.
Filters	
Filter bulletins also on patch names	This parameter defines if the search for bulletins is only executed in the bulletin name box or also in the patch name box, which is also the default. If this check box is not selected, any search of bulletins will only take the bulletin name into account.
Log Files	
Display Console Log File	This parameter defines if the console log displays in the console terminal window on the screen. By default this option is not activated.
Balloon Tips	
Display Balloon Tips	This parameter defines if the balloon tips are displayed for all pop-up windows in the console by default. It is possible to remove the balloon tips individually in a window by clicking the respective icon in the top right corner of the window.
Instant Expert	
Display Instant Expert™	This parameter defines, if the **Instant Expert** panel in the right window pane are displayed when you access a top node. If this option is not activated the panel is displayed in the form of a tab on the bottom right of the right pane.
Customer Packager	
Enable Full Path	This parameter defines if the package is to include the full path of the file or to put the file at the root of the installation.
On-line Satisfaction Survey[1]	
Enable regular prompts for participation in on-line satisfaction surveys	Check this box to activate the prompting for the on-line satisfaction survey. In this case a pop-up menu displays every 35 logins to propose the customer satisfaction survey to the administrator. Taking the survey can be postponed, then the pop-up menu redisplays 5 logins later. If the participation is declined this option becomes deactivated.
Device Topology	
Show Members Tab by Default	Defines if the Members tab is to be shown by default.

1. This parameter defines if the CM online customer satisfaction survey is activated for the current administrator. The administrator must have managing capabilities for at least one of the following objects/object types:
    - Administrator
    - Security Profile
    - Directory Server
    - License
    - System Variables

- Transfer Windows
- Rollout or Inventory Filters

If this is not the case this option is dimmed. The default setting for this variable setting is defined in the System Variables. However, once the administrator is created, this option becomes independent of the system variable and can be modified individually.

Managing the BMC Client Management agent

BMC Client Management deploys intelligent agents to all workstations that are capable of automatically interacting with their surrounding IT environment in order to determine their location and system needs. Whether the computer is a laptop, making irregular connections via dial-up, or a fixed workstation, the agents constantly report their presence and status to the nearest or most appropriate BMC Client Management server. As a result, the master server is capable of dynamically updating its topology database and of displaying this information in an easy way to understand expandable file tree format.

The CM client agent is installed on each client and operates completely independent of the master server, sending information either at regularly defined intervals or when polled by the master or any other module through its respective relay, such as reporting their connection status. Agents receive data/actions from and forward data to their upper level based on a pre-defined schedule allocation. They provide monitoring of and reporting on a very large number of parameters. The nature of these parameters depends on the operating system of the client on which the agent is installed, that is, if it is a Windows client, a Linux client or a Mac OS X client.

This topic includes:

- Using the agent web interface
- Managing agent configuration

Using the agent web interface

BMC Client Management provides access to the agents locally via a browser interface. This agent interface provides access to some of the agent's functionalities that are to be executed by the local user, such as installing specific software or running scripts locally. It also provides access to specific local settings and information, such as inventories, privacy and public reports.

The agent web interface also provides the following functionalities:

- Viewing device information
- Viewing the windows services, events, and ports
- Managing agent privacy settings

Accessing and logging on to the agent web interface

To access all pages of the local agent interface, you must log on as an administrator. To access the agent user interface, right-click the agent icon in the system tray and select the **Agent Interface** option. You can also directly enter the agent's address in the browser window in the following format:

http://<host name>:<console port number>

For example: `http://scotty:1611` or `http://localhost:1611`

> **Note**
>
> You can enter the host name either as its short or full network name such as *scotty* or *scotty.enterprise.com* , or in the form of its IP address. Be aware that when you use IPv6, you need to put square brackets around the IP address. For example, *[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611*.

The browser displays the login screen in which you must provide a valid login to the local device or the BMC Client Management agent.

Depending on the provided login, you have access to the following pages:

Page\User	Local user	Client agent
Home	✓	✓
Tools	✓	✗
Inventory	✓	✗
Privacy	✓	✗
Maintenance	✓	✗
MyApps	✓	✓
Helpdesk Ticket	✗	✓

In addition to these the interface pages, there are a number of pages which can only be accessed directly and not through the interface:

- **Welcome to the Rollout Server**: For more information, see Rolling out agents.
- **Console Download Page on**: For more information, see Downloading and installing the BMC Client Management console.
- **Report Portal**: For more informationi, see Managing reports.
- **Import multiple MSI Files**: Fore more information, see Bulk-importing MSI packages.

Viewing device information

The **Home** tab displays a summary information about the local device.

Parameter	Description
Host Name	The name of the local computer in either its long or short network format or as its IP address in dotted notation.
IP Address	Displays the IP address of the local computer in its dotted notation.
Agent Version	The version of the CM agent that is installed on the local device.
Operating System	Displays the operating system installed on the computer.
Processor Name	The name of the processor of the device.
System Memory	Displays the total RAM installed on the local host in MB.
Local Disk	For each local disk partition an entry will be displayed showing the total amount disk space allocated to the drive /partition and the still available disk space. Any floppy/CD/DVD drives will also be listed with both values at 0, if no mediums are currently in the drive.
Published Rule Count	This parameter displays the number of operational rules that are advertised and ready for usage on the **MyApps** .

Viewing the windows services, events, and ports

In the **Tools** tab, you can see all information about the Windows Services and Events of the local computer.

It is therefore divided into the following parts:

- Windows services
  - Summary
  - List
- Windows Events
  - Application Events
    - Summary
    - List
  - Security Events
  - System Events
- Open ports
  - Open TCP Ports
  - Open UDP Ports

Windows services

Windows services are programs or routines that perform a specific system function to support other programs, particularly at a low (close to hardware) level.

Examples of such services are File Replication, Routing and Remote Access Services. The services part is divided into the following sections:

- Summary
- List

Summary

The **Services Summary** presents the summary information of the **Windows Services** of the local host. It displays amongst other information a graphical representation of the services by status and by start type in the form of pie charts

List

The **List of Services** displays all **Windows Services** together with the following information:

Column	Description
Name	This column list all Windows Services currently registered.
Status	This field displays the respective status of the service which can be either **Stopped** or **Running** .
Startup Type	Shows the respective start type of the service, which can be either Manual, Started, Automatic, On Demand, On Start up or Disabled.
Binary Path	This field displays the installation path for the executable file of the service.
User	This field shows the user of the service which normally would be LocalSystem.

You can access more detailed information about each of the loaded agent modules by clicking its name. The browser window displays the following details:

Column	Description
Name	The fields list the Windows Services currently registered.
Status	This field displays the respective status of the service which can be either Stopped or Running.
Binary Path	This field shows the complete path of the service's installation directory.
Start	This field shows the respective start type of the service, which can be either Manual, Started, Automatic, On Demand, On Start up or Disabled.
User	This field shows the user of the service which normally would be LocalSystem.
Group	This field displays to which group the currently selected service belongs, if applicable.
Action	The contents of this field depend on the current status of the service. It provides you with the different running options of the service. If the service is currently running, you can either Stop or Pause it, if it is stopped you can Start it by clicking the respective link.

Windows Events

An event is any significant occurrence in the system or in application that requires users to be notified. Any event not requiring immediate attention is noted in an event log. Event logging starts automatically each time a Windows device is started.

With an event log and an event viewer you can troubleshoot various hardware and software problems, because the careful monitoring of event logs can help predict and identify the sources of system problems and monitor Windows security events. The Events tab provides event information in the following sections:

- Application Events
- Security Events
- System Events

Depending on the operating systems and the installed software, you can find further event logs here for IE 7, Microsoft Office, and so on.

Application Events

The Application Events pages display information about events logged by applications. For example, a database program might record a file error in the application log. The details of these events are displayed in the following pages:

- Summary
- List

Summary

The Summary page provides information on the logged application events in the form of a table and a pie chart displaying the distribution:

Information	Description
File Path	This entry shows the full path of the local installation of the application log.
Maximum File Size	This file displays in MB the maximum size of the log file. If the size is reached, the oldest entry will be deleted to be able to record the newest event in the log file.
Number of Events	This entry shows how many events were generated for the local client.
Repartition of the Events by their Type	The graphic below this entry shows the repartition of the generated events by their type, that is, the percentage of Errors, Warnings and Information events.

List

The Events tab displays the list of Application events of the managed device. It provides the following information:

Information		Description
Date		The date and time the event occurred in the standard format of.
Severity	Error	Significant problems, such as a loss of data or loss of functions. An Error might be logged for example, if a service was not loaded during Windows startup.
	Warning	Events that are not necessarily significant but that indicate possible future problems. A Warning event might be logged, when disk space is low.
	Information	

Information		Description
		Infrequent significant events that describe successful operations of major server service. An Information event might be logged, when a database program loads successfully or an administrator logged on.
	AuditFailure	An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
	AuditSuccess	An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.
Source		The software that logged the event, which can be either an application name or a component of the system or of a larger application, such as a driver name.

Security Events

The Security log records security events. The log can contain valid and invalid login attempts and events related to resource use, such as creating, opening or deleting files or other objects. If helps track changes to the security system and identify any possible security breaches. If, for example, you use User Manager to enable login and logoff auditing, attempts to log on to the system are recorded in the security log. For further details on the individual items and the subnodes Summary and List, refer to the Application login the previous paragraph.

System Events

The System log contains events logged by the Windows system components. Logged events would be for example the failure of a driver or other system components to load during start up. The events types logged by the system components are predetermined by Windows. For further details on the individual items and the subnodes Summary and List, refer to the Application log topic.

Open ports

This menu option provides access to the list of following types of open ports on the local client:

- Open TCP Ports
- Open UDP Ports

Open TCP Ports

This page displays the list of open TCP ports on the local device and the following information:

Information	Description
Local Address	The local address is the "inside" address of the local client on which the open port was found, possible values for this address are for example 0.0.0.0 and 127.0.0.1.
Local Port	The inside number of the open port.
Remote Address	The "outside" IP address on the local client.
Remote Port	The "outside" address of the port, that is, the port number through which the local client can be accessed from the outside.
State	The state of the port, possible values are Listening, Established, Close_Wait and Time_Wait.

Open UDP Ports

This page displays the list of open UDP ports on the local device and the following information:

Information	Description
Logical Address	The logical address is the inside address of the local client on which the open port was found, possible values for this address are for example 0.0.0.0 and 127.0.0.1.
Local Port	The inside number of the open port.

Managing agent privacy settings

The **Privacy** tab provides access to all types of privacy settings of the agent.

Privacy settings define the remote access rights to the local host, such as its registries, directories and files, etc, through **Direct Access** and any other functionality accessing or defining the local host. To avoid having privacy settings of a user overridden through a remote connection this page is only accessible locally.

This page provides the privacy configuration for the access rights to the local client. Privacy means that the user of the local client has some control over which elements the administrator can access. If an administrator tries to access the local computer through the **Direct Access** node in the console he needs to provide a valid login and password to be able to access the local computer and he can only see or modify in the elements to which he is accorded the corresponding access. Some elements, such as the Remote Control, must be confirmed by the local user before the administrator can access.

It is very important to realize that only the directories specified here are visible from the console. This does not only impact the **Direct Access** and **Remote Control** features but also features which, for example, define exports to this client or want to import from it. Be therefore very careful when making changes to the access privacy

The browser page shows the following information about the privacy elements:

Element		Description
Class	File System	The file system manages the access to the directories of the local device. The access is to a directory is divided into read and write access. Read access allows the administrator to view the directories and their contents and the following files. Read and write access allows the administrator to modify, delete, copy, rename, and so on, the respective element. The default values are Read,Write without acknowledgment for the hard disks and for all logins (*). There is only one exception by default: in the Documents and Settings/* under Windows and in /home/ under Linux, no access is permitted via the value None.
	Windows Registry	The Windows Registry entry controls the access to the keys and values of the registry for Windows systems. This class is not applicable to non-Windows systems. The access principles are similar to those of the file system (see preceding paragraph). The access permissions are applied to the registry key paths. By default there are the following values: `HKEY_CLASSES_ROOT/` **`, HKEY_CURRENT_USER/`** `, HKEY_LOCAL_MACHINE /*` with Read,Write access without acknowledgment for all logins (*); and * with Read Only access without acknowledgment for all logins (*).
	Windows Services	

Element		Description
		The Windows Services class controls the access to all services installed on the Windows operating systems. This class is not applicable to Linux and Mac OS. The access principles are similar to those of the file system (see preceding paragraph). The access rights are applied to the services. The default value is * with Read, Write access without acknowledgment for all logins (*).
	Remote Control	Remote Control manages the Remote Control access to the local device. This class is not applicable to non-Windows systems. Read access allows the administrator to view the remote client; read/write access allows him to execute certain operations on the remote client - such as backup and software maintenance operations. The default value is * with Read,Write access without acknowledgment for all logins (*).
Name		Shows the name of the element, which can be key names, service names or path names, for example, `HKEY_CLASSES_ROOT` , or `C:/Documents and Settings` , and so on If the name is followed by an asterisks, the access rights are applicable for all which are located lower down in the hierarchy, such as subdirectories or sub-keys.
Login		Displays the login of the administrator to connect to the device. The optional login ('*' indicating all valid users) can be assigned to all entries.
Access		Three different access levels are available: Read Only, permitting the administrator or user to view and examine the elements and their content through a console, Read/Write, which allows for the execution of operations such as deleting, copying, or renaming the respective elements, and None, which denies the access of any kind. Each class has its own default access rights which are explained in the preceding paragraph.
Acknowledged		The acknowledgment indicates if the local user must allow the access. This parameter is only applicable for the Remote Control module. If acknowledgment is required, a pop-up menu appears of the local device in which the concerned user can accept or refuse to hand over the control over his device.

All entries of the File System, Windows Registry and Services can contain wildcard characters such as the asterisks (*) to avoid having to list each individual directory name, registry key name, to be activated. For example, the access rights for the entry `C:/WINDOWS/SYSTEM32` apply only to this directory while the rights for entry `C:/WINDOWS/SYSTEM32/*` are applicable as well to all subdirectories.

A very important aspect of the Access Rights is the algorithm used to match entries against access requests from the console. Given a full directory path, the Access Rights are scanned for the entry which *most closely matches the supplied path* . The permission settings for that entry are then used to determine the access.

Managing agent configuration

The **Agent Configuration** node enables the administrator to view or modify configurations remotely and directly for the selected device.

When you try to access a managed device's **Agent Configuration** (**Device Groups > (Your Managed Device) > Agent Configuration**), you will be asked to provide the login and password to the remote computer to verify you have access permissions.

You can provide the login as one of the following options:

- as the simple login name of a local user of the remote computer, such as ***Administrator***

- as `\\domain\logon` for a domain login of the administrator, such as `\\LAB\TEST`. The domain part can be set to `.` to indicate the local computer.

If you are not sure that your local Administrator login has the same passwords for all targets, use the domain login. For domain logins to work correctly, the necessary domain trust relationships must already be set up between the different domain controllers.

This topic includes:

Modifying agent configurations

To modify the settings of any aspect of the agent configuration, proceed as follows:

1. Select **Device Groups> Your Managed Device> Agent Configuration** in the left window pane.
2. Select any line in the table in the right window pane of the respective subnode.
3. Select **Edit> Properties** .
   The **Properties** window appears.
4. Make the desired modifications to the individual values.

Configuration Type	Description
Security	The parameters in this node define the options for secure agent communication. This includes the way the agents communicate between each other and the certificates being used for secure communication. For Windows devices, the access to the **MyApps** can also be defined.
Communication	The parameters under this node define the basic access settings for the communication between the agents and agent and console, such as the different ports of communication, the timeouts for different types of communication and the frame and connection queue sizes.
User Interface	These parameters define the settings for the application kiosk **MyApps** . If packages are advertised to a device, they will appear in the system tray. If not, a message will be displayed on the local device.
Reboot Management	The parameters defined in this section define the default reboot settings which are used by the BMC Client Management - Patch Management .
Logging	The **Logging** node provides access to the log files of the agent via its **Parameters** tab. The parameters in this view define the basic settings for log files of the software, that is, the values specify the contents of granularity of the log files and their output location for example. This also includes the log file sizes and numbers, which types of entries are to be logged, the time format, if alerts are to be sent in case of logged errors, etc.
Module Configuration	See the Configuring modules section below.

5. Click **OK** to confirm the modifications and close the window.

Configuring modules

This node provides access to all BMC Client Management modules that are currently loaded on the selected device. Here you can modify configuration parameters and access local information about the respective module. Modules in CM are responsible for a certain functionality in the product. Their settings are defined through individual configuration files, one per module which are stored in the `config` directory. The modules themselves are stored in the`modules/agent` directory in the form of one `.dll` file for computers with a Windows operating system, for Linux systems you can see there one `.so` file per module.

From the Module Configuration section, you can perform the following actions:

Viewing agent modules

The **Configuration** tab displays the modules currently loaded on the selected device. This Console view provides an overview over all modules which are currently loaded. You cannot execute any modifications on any of the modules listed in this view, these are carried out directly in their configuration files or via the **Agent Configuration** nodes.

Column	Description
Name	The name of the loaded module.
Version	The complete version information of the respective module, that is, the version number with the build number and the date and time the version was compiled at.
Path	The full installation path of the respective module.
Action Count	The number of actions contained in this module which may be called by other modules.
Description	This box can contain a description of the module.

Configuring agent modules

1. Select **Device Groups > Your Managed Device > Agent Configuration > Module Configuration** in the left window pane.
2. Select the desired module in the left window pane.
3. Select **Edit > Properties** .
   The **Properties** window appears.
4. Make the desired changes in the boxes.
5. Click **OK** to confirm.

The configuration of the selected agent module is updated.

Loading agent modules

Depending on the usage of the individual client, further modules might have to be loaded to those which are loaded by default or defined through the rollout installation.

1. Select **Device Groups > Your Managed Device > Agent Configuration > Module Configuration** in the left window pane.

2. Select **Edit > Load Modules** .
   The **Select Agent Modules** window appears.
3. To add modules to the list of loaded modules mark them in this list box.

> The check box **Persistent** defines if the agent module now being selected is to be loaded from now on at every agent startup. By default this box is checked.
> In the following list box all modules are listed which are currently not loaded and available for the operating system of the selected device.

4. Click **OK** to confirm.

The selected modules are added to the list of loaded modules.

Unloading agent modules

Not all modules need to be loaded on all clients. You can unload modules that are not required on a specific device.

1. Select **Device Groups > Your Managed Device > Agent Configuration > Module Configuration** in the left window pane.
2. Select the module to be unloaded in the right window pane.
3. Select **Edit > Unload Modules** .
   A **Confirmation** dialog box appears on the screen.
4. Click either:
   - **Yes** , if the module is not to be loaded at every agent startup from now on
   - **No** , if the module is only to be unloaded this one time

The selected module is unloaded.

Viewing autodiscovered objects

You can view the complete list of all objects found in the network by the Autodiscovery module in the **Global Settings** > **Auto Discovered** node. It is a compilation of the lists of autodiscovered devices found by all clients in the network.

The table of the **Autodiscovered Objects** can be filtered according to the following criteria:

Parameter	Description
Autodiscovered Type	This list on top allows you to define which type of autodiscovered devices are to be displayed in the following table.
Agent Installed	This criteria allows you to filter the list of devices according to the installation status of the CM device on each, that is, if it is installed, not installed or it will show devices of both cases.

The table of the **Autodiscovered Objects** node provides the following information about all discovered devices:

Parameter	Description
Name	Displays the name of the device.
IP Address	The IP address of the autodiscovered device.
Discovery Time	This column displays the date and time at which the individual devices were discovered for the first time.
OS Name	If the discovered device is of type PC this field displays its operating system, such as Windows 2003 or Solaris.
Network Name	The full network name of the device.
Agent Version	This column displays the version number of the CM agent if it is already installed on the autodiscovered device.
Uploading Relay	This field displays the name of the relay which uploaded the respective device.
Type	Displays the type of the autodiscovered devices, which can be one of the following: • **PC** If this option is selected the list displays all devices of type PC, those that already have an CM agent installed and also those without. • **Printer** This option displays all autodiscovered devices which are printers. • **Switch** This option displays all autodiscovered devices which are switches. • **Server** This option displays all autodiscovered devices which are servers. • **Firewall** This option displays all autodiscovered devices which are firewalls. • **Other** Displays all devices that were found in the network which are another than the previously listed types.
Notes	If available, this field shows more information on the autodiscovered device.

Managing dynamically populated user and device groups

In BMC Client Management, you can dynamically populate device and user groups. The criteria used for populating members are similar for both device groups and user groups.

This section includes:

- Dynamically populating groups with queries
- Dynamically populating groups with directory server
- Dynamically populating groups with compliance rules

> **Note**
>
> Using compliance rules, only device groups can be populated.

Dynamically populating groups with queries

The **Queries** subnode (**Device Groups or User Groups > Your Group > Dynamic Population > Queries**) provides access to the query or queries associated with the currently selected device group or user group. Queries are assigned to groups for dynamic grouping. Assigning a query to a group means that the members of this group are automatically checked at regular defined intervals if they still belong to this group according to the specific criteria defined in the query or the conditions defined through the free query, and at the same time the whole system population is browsed for any object that may have changed its criteria/conditions and now belongs to this group.

However, if the group is managed by a Directory Server or a Compliance Rule, it cannot be assigned to a query at the same time. Also, if a query is assigned to a device group the device type of the group will automatically be modified to *Devices with Agent* , if this option was not yet applied.

The operations to manage groups that are dynamically populated with queries include:

- Assigning query to a group
- Unassigning query from a group
- Modifying populator of a group
- Modifying operator of a group
- Re-evaluating members of a group
- Viewing query of a user or device group

The list with the query or queries associated with a group is structured as follows:

- **Queries** : Displays the names of all queries which are associated with the currently selected group.
- **Status** : Displays the status of the query. Possible values are *active* and *inactive* . If a query is *inactive* it will not be taken into account when defining the members of this group, even if the query operator is defined as *AND* . If the query is *active* , the members of the group are dynamically managed through the query. A query becomes *inactive* if it is being modified.
- **Last Evaluation** : Displays the date and time of the last evaluation of the members of the group as determined by the query.
- **Time of Assignment** : Displays the date and time at which the assignment between the query and the group was created in the database.

Populator

The populator defines the 'owner' of the group, that is, the administrator that assigns the query to the group and according to whose access rights the contents of the group are defined. This means that even if admin logs on, he will see the same group content as the populator. When the group is created the populator is the creator of the group. When a query is assigned to the group, the populator will automatically change to the administrator creating the assignment.

The administrator *France* is the populator of the group and assigns a query called *AllUsers* to the group. The group will only contain devices or users which are located in France, because the administrator France only has access rights defined for those. If admin logs on to display the group, he will also only see the devices or users located in France, even though theoretically he has access to all devices or users in the database.

Operator

This list defines the operator through which the assigned queries are connected. The possible values are *AND* and *OR* . If the queries are connected through the *AND* operator, they all together dynamically manage the membership of that group, that is, the group members must match the criteria/conditions of all queries listed, if the operator is *OR* , only one will define the group membership, that is, the group members need not match all criteria, but only one of one of the queries.

Assigning query to a group

To assign a query to a device group or user group, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select **Edit > Assign Query** .
   The **Assign a Query** dialog box appears.
6. Select the query to be assigned to the selected group from one of the lists boxes.
7. Click **OK** to confirm the assignment.

The selected query was assigned to the selected group.

Unassigning query from a group

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select the desired query from the list in the right window pane.
6. Select **Edit > Unassign Query**
   A confirmation window appears in which you can specify if the group should be emptied of its members.
7. Click either the
   - **Yes** to remove all devices, users and subgroups from the group

- **No** to maintain the current members of the group.

The selected query was unassigned from the selected group.

Modifying populator of a group

You must be an administrator with write access to the respective group.

> **Note:**
>
> When you change the populator of a group, the contents of the group can change drastically.

To modify the populator of a device group or user group, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select from the **Populator** list above the table in the right window pane the desired populator.

The new populator will be saved and applied immediately to the group.

Modifying operator of a group

You must be an administrator with write access to the respective group. The operator of a group associates the queries between each other.

To modify the operator of a device group or user group, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select from the **Operator** list of the preceding the table in the right window pane the desired populator.

The new operator will be saved and applied immediately to the group.

Re-evaluating members of a group

After modifications were executed in the system, such as new devices or users being added to the network and the CM agent being installed on them via rollout, BMC recommends to re-evaluate the members of existing groups which are managed through queries, using this function to make sure all new devices or users were added to their respective groups.

To re-evaluate the members of a group, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select **Edit > Reevaluate Members** .

The members of the selected group will immediately be updated.

Viewing query of a user or device group

To find a query, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Queries** in the left window pane.
5. Select **Edit > Go To** .

Under the **Search** node in the left window pane, the selected query will be shown with all its tabs and subnodes.

Dynamically populating groups with directory server

The members and subgroups of a group can be managed by a directory server through directory services such as the Microsoft Active Directory. Directory services are repositories for information about network-based entities, such as applications, files, printers, and people. They are important because they provide a consistent way to name, describe, locate, access, manage, and secure information about these resources. Many vendors build specialised repositories or directory services into their applications to enable the specific functionality their customers require. As such, enterprise class directories take an important step towards the consolidation of corporate directories by offering standards-based interfaces allowing for interoperability and centralised directory management. The directory service is based on a secure directory database containing

user IDs, passwords, access rights, and organizational information. The directory database can be automatically replicated to multiple locations for backup reliability, load-balancing performance, and reduced network impact. In addition, with one logon, users can access a globe-spanning network - even when dialing in remotely or accessing the network over the Internet.

The operations to manage groups that are dynamically populated with directory servers include:

- Assigning directory server to a group
- Unassigning directory server from a group
- Synchronizing a group with directory server
- Scheduling synchronizations with directory server

The **Directory Server** subnode is located under: **Administrator Groups, Device Groups or User Groups > Your Group > Dynamic Population > Directory Server** .

> **Note**
>
> If you manage your group through a directory server you may not manually create or add objects to this group anymore. Neither can you assign a directory server to manage this group, if the group already has members, or is assigned to a query or a compliance rule.

It is possible to synchronize devices which move between different domains.

The view of the directory server is structured as follows:

- **Directory Server**: Displays the name of the directory server.
- **Entry**: Displays the Base DN and User entries of the directory server.
- **Time of Assignment**: Displays the date and time at which the device group was synchronized for the last time with the directory server.
- **Activation**: Displays the condition on which the synchronization with the assigned directory server will be started.
- **Schedule**: Displays the frequency with which the synchronization with the assigned directory server will be executed.
- **Termination**: Displays when the synchronization with the assigned directory server is scheduled to be terminated, that is, when the synchronization is to be run for the definitely last time of the current scheduling cycle.

Assigning directory server to a group

1. Select in the left window pane either:
   - **Device Groups** ,
   - **User Groups** , or
   - **Global Settings > Administrator Groups**
2. Select the desired group in the left window pane.

3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Directory Server** in the left window pane.
5. Select **Edit > Assign Server**  .
   The **Select a Directory Server** dialog box appears on the screen. The dialog box lists all available directory servers with their organizational units depending on the base object, that is, when under a device group it displays all available device groups, and when under a user or administrator group, it displays all available user groups.
6. If the directory server you want to synchronize with is not displayed in this list, that is, it has not yet been created in CM , you can directly create it from here as follows:
   a. Click the **Create and connect to a new directory server** button.
      The **Properties** dialog box appears on the screen.
   b. Enter the required information into the respective boxes (see topic Creating a Directory Server for more information).
   c. Click **OK** to confirm the new directory server.
      The window closes and the new directory server is added to the list of available servers in the **Select a Directory Server** dialog box.
7. Select an entry from the list.
   You can either select the directory server itself or one of its children. If you want to synchronize all elements of a directory server in a flat list check the **Synchronize All Devices /Administrators/Users** box above this list together with the directory server root in the following text box. To synchronize with the server root or an OU maintaining, that is, recreating the directory structure in CM do not check this box. This does not apply to administrator groups, because these cannot have subgroups and thus will always import all elements in a flat list.
8. Click **OK** to confirm.
   The **Properties** dialog box appears on the screen. Here you can specify if all devices are to be synchronized or only those with an CM agent installed.
9. Select the respective option from the list.
10. Click **OK** to confirm.
    A confirmation window appears.
11. Click either:
    - **OK** to synchronize, or
    - **Cancel** to define the directory server without synchronization.
      If you chose to synchronize, the connection with the directory server is established and all members of the selected entry are added to or removed from your current group. The **Directory Server Synchronisation** window appears as a confirmation listing all objects that were added or removed with their status which in this case will either be *New Object* or *Error* . In case of an administrator group synchronization this can also be *Administrator maintained* if administrators are not to be deleted during synchronization. If more than 3000 elements are synchronized this window will be replaced by a simple confirmation message.
12. Click **OK** to close this window.

If you did not synchronize, the **Select a Directory Server** window will be closed and the directory server will be added to the table in the **Directory Server** node but no objects will be added.

If the directory server is assigned to a device group, the device type of the group will automatically be modified to *All Devices* .

No matter if you chose to synchronize or not, the name of your group will be changed to the name of the directory server entry followed by the full name of the server in dotted notation. For example, if your group was initially called by the default name *New Device Group* and you synchronized it with an organizational unit called *Relay Servers* , the name of your group will now were changed from *New Device Group* to *Relay Servers.Full.Directory.Name* . If the selected group has subunits these will also be synchronized and added to the group as *subunit.group.server name* .

If all elements of a type were synchronized the name of the group will change and to the full name of the directory server. The elements will be added to this group in a flat list ignoring any hierarchy they might were located in on the directory server.

> **Note**
>
> If the original group or "OU" on the directory server was renamed, moved or deleted, the CM group cannot be re-synchronized with this group. An error message will be displayed instead.

Unassigning directory server from a group

To unassign a directory server from a group proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** ,
   - **User Groups** , or
   - **Global Settings > Administrator Groups**
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Directory Server** in the left window pane.
5. Select **Edit > Unassign Server** .

The directory server will be unassigned from the selected group.

Synchronizing a group with directory server

You might want to re-synchronize your group with the directory server periodically to keep your group up to date.

> **Note**

If you have Windows XP and 2003 32-bit devices in your environment ensure that you have correctly configured the server certificate verification, that is, the server certificate is included with the trusted certificates of the clients. If the server certificate cannot be verified by the client all communication between server and client will not be encrypted.

For more information about this problem on Windows devices see the Microsoft Knowledge Base article 835208. For more information about certificates and how to configure and install them see the Client Management and SSL topic of the Reference section.

To schedule a synchronziation and thus synchronize a group with a directory server, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups**,
   - **User Groups**, or
   - **Global Settings > Administrator Groups**
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Directory Server** in the left window pane.
5. Select **Edit > Synchronize**
   A **Confirmation** window appears.
6. Click **Yes** to confirm the synchronization.
   The synchronization is started directly. The connection with the directory server is established and all members of the selected entry are added to or removed from your current group. The **Directory Server Synchronization** window appears listing all objects that were added or removed with their status which in this case will either be *New Object* or *Error* .
7. Click **OK** to close the window.

The selected group has now been re-synchronized with the directory server.

Scheduling synchronizations with directory server

After a directory server is assigned to a group, regular synchronizations can be scheduled.

1. Select in the left window pane either:
   - **Device Groups** ,
   - **User Groups** , or
   - **Global Settings > Administrator Groups**
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Directory Server** in the left window pane.
5. Select the assigned directory server in the right window pane.

6. Click **Edit > Properties** .
   The **Scheduler** window appears. For more information, see Managing schedule of an assigned object.
7. Click **OK** to confirm.

Dynamically populating groups with compliance rules

The **Compliance Rule** subnode (**Device Groups > Your Group > Dynamic Population > Compliance Rule**) provides access to the compliance rule populating the currently selected device group. Compliance rules can define the group membership according to different criteria, that is, a compliance rule populates a group with all devices which are compliant with the rule, all devices which are not compliant, or those devices which could not be evaluated. This topic includes:

- **Name**: Displays the name of the compliance rule.
- **Compliance**: Displays the criteria which defines the group membership, that is, if the group members are compliant, non-compliant or those which could not be evaluated.
- **Last Evaluation**: Displays the date and time of the last compliance evaluation of the object.
- **Status**: Displays the evaluation status of the compliance rule, possible values are: `Inactive`, `Evaluated`, `Evaluation Failed`, `Not Evaluated`, `Evaluating`, and `Evaluation Scheduled`

The operations to manage groups that are dynamically populated with compliance rules include:

- Assigning compliance rule to a device group
- Unassigning compliance rule from a device group
- Reevaluating members of a device group

Assigning compliance rule to a device group

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Compliance Rule** in the left window pane.
5. Select **Edit > Assign Compliance Rule** .
   The **Assign a Compliance Rule** dialog box appears.
6. Select the desired compliance rule from the list in the dialog box.
7. Click **OK** to confirm the assignment.
   The **Desired Compliance** dialog box appears. In this dialog box you define the type of compliance for the member devices. The options are: **Compliant** , **Not Compliant** and **Evaluation Impossible** .
8. Select the desired option by clicking the respective radio button.
9. Click **OK** to confirm.

The compliance rule was assigned to the selected device group. The icon of the device group will now change to its compliance rule populated one and the members of the group will now be managed by the results of the rule.

Unassigning compliance rule from a device group

To unassign a compliance rule from a device group, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Compliance Rule** in the left window pane.
5. Select the compliance rule you want to unassign from the device group in the right window pane.
6. Select **Edit > Unassign Compliance Rule** .

The compliance rule will be unassigned from the selected device group.

Reevaluating members of a device group

You can launch a manual reevaluation of a device or of all members of a device group assigned to a compliance rule at any time.

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the subnode **Compliance Rule** in the left window pane.
5. Select the compliance rule in the right window pane.
6. Select **Edit > Evaluate** .

The members of the selected device group will immediately be updated.

Managing devices and device groups

The main objects in BMC Client Management, through which most of the system management tasks are executed, are devices and device groups. These can be viewed in different locations in the console.

- Devices groups can be viewed and managed under the **Device Groups** node.
- Devices can be viewed and managed:
  - under a specific group under the **Device Groups** node the device is a member of.
  - in the **Device Topology** node, in either one of the available structures.

This section includes:

- Managing device topology
- Managing devices
- Managing device groups

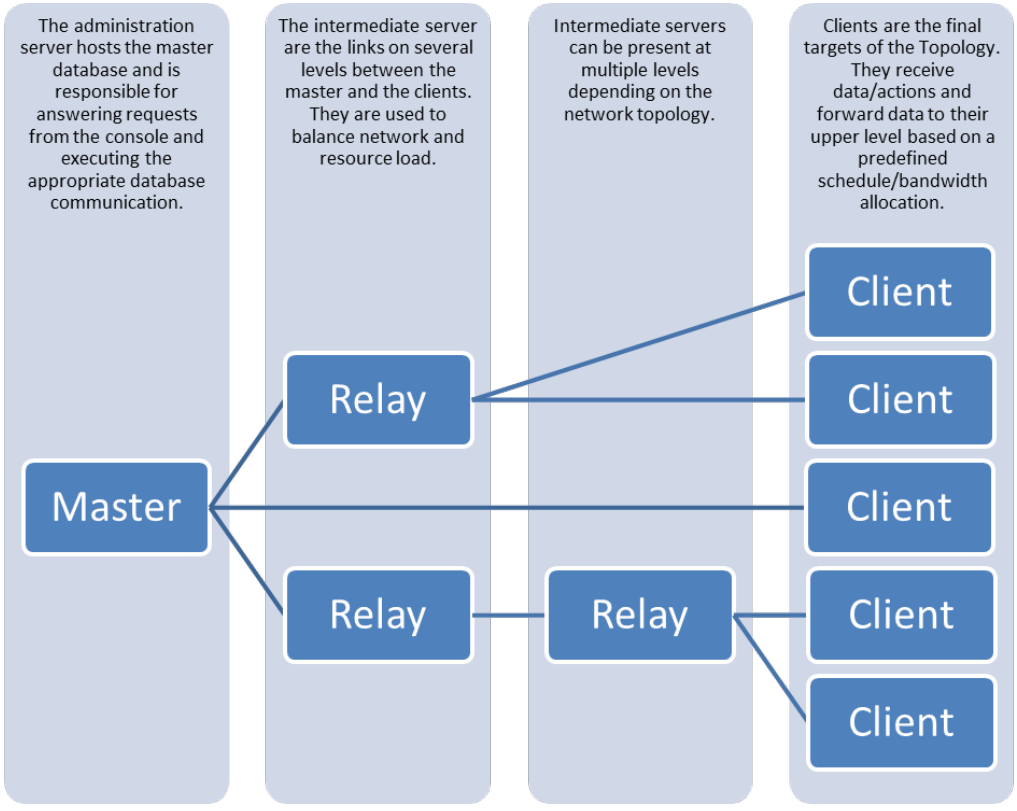
Managing device topology

The **Device Topology** node is one way of organizing all managed devices within your network and it represents it according to its logical connections. You proceed through this view from the highest (most general) level of detail to the lowest (most specific) level. These levels are displayed in the form of an explorer tree. It will represent the different types of computers of your network with their respective icons, such as the master, relays and clients.
The left window pane of the **Device Topology** view also provides all subnodes available for a device, which means that you may access any functionality available for a specific device from here and from its location under the main **Device Groups** node.

The main **Device Topology** node has the following subnodes:

- One node for each *Master Server* in the network
- One node for each *Relay* under the respective Master
- One node for each *Client* under the respective Master or Relay

The following diagram illustrates a possible network topology:



For information about device topology graph, see Managing graphs of an object topic.

For more information on member information from device topology view, see Viewing member information from device topology topic.

Viewing member information from device topology

Even though the device topology is not a group or folder it still has a **Members** tab. This tab shows all devices that are located below the currently selected device. Depending on which type of topology you selected, that is if you are looking at the topology as it is seen by CM , by the network or as the connectivity, the members of a device might not be the same. This view list all the direct children together with all the information available for each device. This information is the same as that of the **General** when you select the device.

The **Parent Device Groups** tab displays the list of groups the currently selected device is a member of. If the device does not belong to any group it is listed under the **Lost and Found** node of the **Global Settings** .

This topic includes:

- Basic device information
- Advanced device information
- Agent details
- Operating system details
- Agent roles
- Customized information

The device object is one of the main objects of CM , it can have different roles and functions in the network and thus a lot of different information is available for it. This information displays in the form of tables in the right window of the **General** tab. In the **Properties** window of a device this information it is divided into different panels to make it easier to find.

Basic device information

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
User	Click the icon next to this field and select the user to assign from one of the appearing list views.
Location	The country/region/town/building/geographical area at which the asset is located.
Last Update	The date and time at which the device information was last updated.
Type	The type of the device, that is, which purposes the device server, if it is a server, a workstation, a printer or a game console, etc. You can manually modify this value. However, in this case you also need to deactivate the automatic updates, otherwise the device type reverts to its original type at the next update. To switch to manual update click the icon next to the box, which appears when you manually change the type.
IP Address	The IP address of the device in its dotted version, such as *194.50.68.255* or *2001:db8:85a3::8a2e:370:7334* .
Topology Type	The topology type of the device, that is, if the managed device is a master, a relay or a simple client. It may also be an unconnected, a scanned, a deprecated or an unknown device.
Domain Name	The full name of the domain the currently selected device belongs to, that is, *kirk.enterprise.starfleet.com* .
	The name of the operating system installed on the currently selected device.

Parameter	Description
Operating System Name	
Host ID	If the operating system is Window it either displays the asset tag or the BIOS serial number depending on the manufacturer of the client. If the operating system is Linux this is the equivalent of the_hostid_ command. If the operating system is MacOS this value displays the system serial number that appears in the **About This Mac** window or in the **System Information** .
Parent	Displays the name or the IP address of the parent of the device. In case of the master or unconnected devices this field is empty.
Virtualized on	Defines the type of virtual machine running on the host, that is, the name of the software used. This may be either *None* if no virtual machine is installed on the device, *VM Ware Server, Microsoft VirtualPC Server, VirtualBox* or *Parallels* .

Advanced device information

Parameter	Description
Hosts a hypervisor	Displays if the agent device hosts a hypervisor, in which case this field displays the name of the virtualizing software, otherwise it is empty.
Hypervisor Version	The version number of the hypervisor.
Network Name	The network name of the machine, either as its short or complete network name, for example, *scotty* or *scotty. enterprise.com* , or as its IP address in dotted notation, for example, *194.45.245.5* or *2001:db8:85a3::8a2e:370:7334* .
NetBIOS Name	The NetBIOS name of the currently selected client. For managed devices which have Linux or MAC OS as their operating system this field is empty.
Subnet Mask	The subnet mask of the device.
MAC Address	The MAC (hardware) address of the discovered device.
Disk Serial Number	The serial number of the hard disk of the device.
Under NAT	Indicates if at least one piece of hardware of the device uses network address translation. This box is automatically checked if this is the case.
Intel VPro Available	Indicates if the device is equipped with Intel's vPro firmware.

Agent details

Parameter	Description
HTTP Port	The range of ports on which the HTTP server listens for and sends data from.
HTTP Console Port	The number of the port that the console uses for communication with the agent.
Secure Communication	Defines if the agent sends any communication in secure format.
Agent Version	The version number of the BCM agent if it is installed on the device.

Parameter	Description
Patch Knowledge Base Version	The currently installed version of the configuration files of the Patch Management functionality.

Operating system details

Parameter	Description
Operating System Version Major	The major version number of the operating system installed on the device.
Operating System Version Minor	The minor version number of the operating system installed on the device.
Operating System Revision	The revision number of the operating system installed on the currently selected device.
Operating System Build	The build number of the operating system installed on the device.

Agent roles

Parameter	Description
Packager	Indicates if the currently selected device is a *Packager* in the **Package Factory** , that is, if packages may be created on it. If this option is set to **No** , the device is not visible under the **Package Factory** node.
Patch Manager	Indicates if the currently selected device is serving as a Patch Manager, that is, if it may handle MS Secure files and all other options pertaining to patch management. If this option is set to **No** the device is not displayed under the **Patch Manager** node.
OSD Manager	Indicates if the currently selected device is a OSD Manager, that is, if it can create and manage operating system deployments as well as install them on the defined target devices. If this option is set to **No** , the device is not displayed under the OS Deployment node.
Asset Discovery Scanner	Check this box if the device is to be an Asset Discovery Scanner.
Rollout Server	Check this box if the device is to be a Rollout Server.
Web Service	Check this box if the Web services are to be active on this device.
Directory Server Proxy	Check this box if the device is to be a Directory Server Proxy.

Customized information

This panel displays the list of all device attributes that are defined as visible with their respective values. You can change the individual values in this window.

Managing devices

In BMC Client Management, a device is any type of computer in your network. It can be one of the following:

- *Master* (also called *Master Server* or *Administration Server*)
- *Relay* (also called *Intermediate Server*)
- *Client*

Peripheral devices such as printers or pointing devices are not included in this denomination.

Devices do not have their own specific top node. They are displayed with all their available information in two different locations in the console:

- **Device Topology**
- **Device Groups**

> **Note**
>
> The **Parent Device Groups** tab displays the list of groups the currently selected device is a member of. If the device does not belong to any group, it is listed under the **Lost and Found** node of the **Global Settings** .

Devices have the following subnodes. Depending on their topology type, not all of them might be available:

- **Agent Configuration**
- **Direct Access**
- **Remote Control**
- **Inventory**
- **Assigned Objects**
- **Alerts and Events**
- **Financial Asset Management**
- **vPro**

Devices have the following tabs. Depending on the location at which you look at the device, not all of them are available:

- **Members** - this tab is only available under the **Device Topology** node.
- **Parent Device Groups** - this tab is only available under the **Device Topology** node.
- **Virtual Guests**
- **Graph**
- **General**
- **Users**
- **Security** - this tab is only available under the **Devices** node.

Related topics

- Understanding device types
- Performing basic device tasks
- Performing advanced device tasks
- Managing virtual guests of a device
- Managing users of a device

Understanding device types

The devices are distinguished by their main type, which can either be:

- Base Type Devices
- Device type evolution

Base Type Devices

The icons representing the devices as a node comprise the information of three different attributes of the device:

- Topology Type
- Connection Status
- Operating System

Topology Type

The topology type makes two basic distinctions between the devices stored in the CM database:

Icon	Type	Description
	Super Master	This icon indicates that the device is of topology type super master and its operating system is Linux or Window or the last icon indicates that the operating system is not known.
	Master	This icon indicates that the device is of topology type master and its operating system is Linux / Window or the last icon indicates that the operating system is not known.
	Relay	This device is of type relay with a Linux / Windows / Mac or unknown operating system.
	Client	This device is of type client with a Linux / Windows / Mac or unknown operating system.
Icon	**Type**	**Description**
	Unmanaged	The device is an unmanaged device, that is, the device is not connected to the network but is registered as a member or it has no CM agent installed but has its inventory and other data generated and uploaded to the master via USB or another device with CM agent .
	Unknown	The device was created either manually or via an active directory synchronization but is not part of the managed objects of CM as it has no CM agent installed. This type of device is a subtype of the unmanaged device type.
	Scanned	

Icon	Type	Description
		The device is a scanned device, that is, the device does not have an CM agent installed but was scanned by a vulnerability scanner. If the scan was successfully executed the "blue" scanned device icon is used, if the scan failed the "red" scanned icon will be shown.
	Deprecated	The device is a deprecated device, that is, the device has arrived at its end of life and been (physically) removed from the IT park but its data is still archived in the database.

Connection Status

The connection status only applies to devices with an installed CM agent and indicates if the device is currently reachable or not. The color of the icon indicates the respective connection status.

Icon	Connection Status	Description
	Established	The connection with the device is established and everything is running smoothly.
	Lost	The device was lost. A device is declared as lost when the master has not received any sign of life of the device for a longer period of time than that specified in the **System Variables** under the **Device Lost Delay** entry.

Operating System

If it is known, the symbol on the client icon indicates the operating system of the respective device. This is applicable to devices with and without CM agent , however, devices of type ***Unknown*** never display their operating system; being unknown, their OS cannot be detected. Neither do the icons of scanned devices display the operating system, though this can be found.

Icon	Operating System	Description
	Windows	These icons, a running master and a lost, an unmanaged and a deprecated device all have Windows as their operating system.
	Linux	These icons display Linux as the devices‘ operating system.
	Mac OS X	These icons display Mac as the devices' operating system.
	Unknown	These icons only display their topology type and connection status, because the operating system for the respective device could not be found.

Device type evolution

When a device is first found or created in the database it is assigned a topology type. Depending on the operations executed on it, its type might change. However, not all device types can change into any other type, the direction is one-way and cannot be reversed. The following changes of type are possible, but not mandatory:

Source Type	Target Type	Operation Description
Unknown	Scanned	Add the unknown device to a target list and scan it for vulnerabilities.
	Unmanaged	Execute an asset discovery scan on the unknown device.
	Agent	Roll out the CM agent to the unknown device.
Scanned	Unmanaged	Execute an asset discovery scan on the scanned device.
	Agent	Roll out the CM agent to the scanned device.
Unmanaged	Agent	Roll out the CM agent to the unmanaged device.

Performing basic device tasks

The basic tasks for devices include:

- Creating a device
- Deleting devices
- Rolling out agent

Creating a device

Devices can either be standalone or within a device group. If the new device shall be a standalone device, skip step 2.

To create a new device,

1. Select **Device Groups** in the left window pane.
2. Select the desired device group for the new device.
3. Select **Edit > Create Device** .
   The **Properties** dialog box appears.
4. Enter the desired data in the respective boxes.
   Not all boxes can be filled in manually, such as assigning a specific functionality to the new device, for example, to make it a *Patch Manager*.
5. Click **OK** at the bottom of the window to confirm the data for the new device.

A new device with the specified properties was created.

Deleting devices

Devices can be deleted from two different locations in the console:

- From any type of graph in the **Device Topology**

- From their device group under the **Device Groups** node.

> **Note**
>
> You need write access to the immediate parent from which the device is being deleted, that is either its relay or the device group it is a member of.

To delete devices,

1. Select either the **Device Topology** or **Device Groups** node in the left window pane.
2. Find the device to delete in the hierarchy and select it in the right window pane.
3. Click **Edit> Delete** .
4. Find the device to delete in the hierarchy and select it in the right window pane.
5. In the **Confirmation** window click **Yes** .

The selected devices are deleted immediately.

Rolling out agent

The BMC Client Management agent must not already be installed on the selected device(s) in order for this function to work. With an agent rollout, the BMC Client Management agent can be installed on one or more devices at a time. However, this function cannot be used to update an already installed CM agent .

To perform an agent rollout,

1. Select **Device Groups** in the left window pane.
2. Select the device group containing the desired device(s) in the left window pane.
3. Select the desired device(s) from the list in the right window pane.
   You can select multiple objects by either pressing the CTRL-key and selecting the desired objects, or by selecting the first object, pressing and holding the Shift-key, then selecting the last object.
4. Select **Edit > Agent Rollout** .
   The **Agent Rollout Wizard** dialog box appears.
5. Follow the instructions in the wizard and provide the required information.

The CM agent rollout will be performed on the selected device(s).

Performing advanced device tasks

The advanced tasks for devices include:

- Merging a device with another
- Deprecating a device
- Auditing a device

- Viewing inventory summary
- Using direct access tools
- Reassigning operational rules

Merging a device with another

The topology type of the devices to be merged has to be *Scanned Device* .

In some cases a managed device, that is already in the database might be created a second time as a *Scanned Device* . For example, this might happen because the DNS server is not responding during a scan of an IP address range and therefore the CM agent cannot find all the required information to uniquely identify a device. In this case a new device will be created.

To merge one device with another, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select the device group containing the device to be merged in the left window pane.
3. Select the device to be merged from the list in the right window pane.
4. Select **Edit > Merge with Device** .
   The **Select a Device** dialog box appears on the screen.
5. Select the device you want to merge with the one you selected in step 3.
6. Click **OK** to confirm.

The data of the scanned device has now been merged with the data of the already existing device. Its topology type will be updated in the table.

Deprecating a device

After a device has reached the end of its lifecycle and will be physically removed from the IT environment it must also be removed from the CM representation of the network. In this case its topology type will become *Deprecated Device* and its GUID will be erased. The basic data of the device, such as its OS, MAC and IP address, etc, and hardware, software, custom and security inventory will be archived in the CM database, but the device will no longer be manageable. It can also still be viewed in specific groups. If the device is a relay and still has children, all these will be deprecated, too.

To deprecate a device, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select a device from the list in the right window pane.
   If the desired device is allocated to a device group, double-click the name of the respective group to reveal its member devices.
3. Select **Edit > Deprecate Device** .
   A confirmation window appears.
4. If the selected device has a Windows 32-bit or 64-bit operating system and you want to uninstall the CM agent , check the **Agent Uninstall** box.

5. Click **OK** to deprecate and archive the device.
   If **Agent Uninstall** was selected, the **Agent Rollout Wizard** will be displayed on the screen in which you can either select an existing uninstall rollout or create a new one. If the CM agent is not uninstalled, that is, identity information will still be uploaded from that device, a new device will be created with the same GUID and its name will be suffixed with its deprecate index number, for example, (0), (1), and so on. The icon of the device will be changed to its deprecated version. An CM agent and possibly also a Patch Management license, if applicable, will be freed up and its basic data and inventories will be archived.

Auditing a device

Audit Now allows you to directly launch an asset discovery scan of the selected device, to generate and upload the latest device information, and a summary of its hardware, software and security inventory.

To perform Audit Now , proceed as follows:

1. Navigate to the desired device.
2. Select **Edit > Audit Now** .

The device scan is launched directly and the data in the **Asset Summary** tab of the device's **Inventory** node will be updated once the scan is finished.

Viewing inventory summary

To view the inventory summary of a device, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select the device group containing the desired device in the left window pane.
3. Select the desired device from the list in the right window pane.
4. Right-click the desired device.
   A pop-up menu appears.
5. Select **Inventory Summary** .

The focus of the console will jump to the **Asset Summary** tab of the device's **Inventory** subnode, displaying its inventory summary.

Using direct access tools

A number of Direct Access Tools are available for the devices in your network, such as accessing its registry, services, or rebooting the device. The direct access tools are available from the **Device Topology** and the **Device Groups** nodes.

To use the direct access tools, proceed as follows:

1. Navigate to the desired device.
2. Right-click the device.
   A pop-up menu appears.

3. Select **Direct Access Tools** .
   A pop-up menu appears.
4. Select the desired tool from the list.

The device will open on either the subnode representing the selected tool or the main device node, where you can now execute the necessary operations. If you selected an immediate action such as checking the connection or rebooting the device the focus of the console stays at its current location.

Reassigning operational rules

If you made modifications to an operational rule which is already assigned to a device or device group the rule must be reassigned. This means that the operational rule is updated with its modifications on the assigned devices. If the reassignment is effected through a group assignment it is effective for the whole group.

To reassign operational rules, proceed as follows:

1. Select **Device Topology** in the left window pane.
2. Double-click the master server in the right window pane.
3. Select the tab **Parent Device Groups** in the right window pane.
4. Select the desired device group from the list in the right window pane.
5. Select **Edit > Reassign Operational Rule** .

The group's operational rules were activated for the selected device group and will be executed as soon as they arrive at their destination.

Managing virtual guests of a device

Virtual guests are virtual machines that were discovered on the devices of your network with or without BMC Client Management agents.

This topic includes:

The the following virtual machine software products are supported by BMC Client Management:

Platform	Vendor	Software	Version
Windows	Oracle Corporation	Oracle VM VirtualBox	5.1
	RingCube Technologies, Inc.	vDesk Client	2.x and 3.x
	Sun Microsystems, Inc.	VirtualBox	5.1

Platform	Vendor	Software	Version
	Microsoft	Hyper-V	10.0
	VMware, Inc.	VMware Player	12.5
		VMware Server	2.x
		VMware Workstation	10.0 and 12.5
		VMware Fusion	7.1
Linux	Citrix Systems, Inc.	Xen	3.x
	Sun Microsystems, Inc.	VirtualBox	5.1
MAC OS X	Parallels	Parallels Desktop	4.x
	Sun Microsystems, Inc.	VirtualBox	5.1
	VMware, Inc.	VMware Fusion	2.x

Detecting virtual guests

BMC Client Management can detect virtual guests using the agent installed on a device or by using the Asset Discovery program.

Using BCM Client Management agents to discover guests

After the BMC Client Management agent has detected a virtual guest on a device, it collects the following basic information about this guest:

- Virtual device name
- MAC address
- Guest member ID
- Descriptive or friendly name of the virtual device
- Operating system

The agent also collects different types of inventory, however, you cannot view these data in the current view. To view the collected inventory, you need to create a group collecting the required virtual machines and under these virtual machines, you can view the inventories, either as a group or individually.

- Hardware inventory
- Software inventory

You can execute the following actions on the guest members of a device:

- Remotely access the virtual machine
- Access its inventory summary
- Start, stop, pause and resume the machine
- Display its properties
- Use the Direct Access Tools

Using Asset Discovery to discover guests

The Asset discovery program in BMC Client Management uses the remote WMI to discover hypervisors and the list of virtual machines available under that hypervisor.

Checking connection to a virtual device

This option allows you to verify the connection of the remote device, that is, to see if it is contactable.

1. Select the device in the right window pane.
2. Right-click the mouse button and select the **Direct Access Tools > Check Connection** option from the **Direct Access Tools** pop-up menu.
   A ping is directly sent to the virtual machine on the remote device.

The result of the connection verification displays in an Information window.

Managing virtual devices

The aim of virtual device management is to start, stop, shut down and pause the virtual devices.

1. Click **Manage** .
   The **Identification** window displays.
2. Enter valid system credentials in the respective boxes.
3. Check the **Save Credentials** box if necessary.
4. Click **OK** .
   After having successfully connected, the **Virtual Guest Management** window appears. It displays the list of virtual devices that are installed on the hypervisor.
5. Select the device on which you want to execute an operation.
6. Click the icon for the operation you want to perform.

Managing users of a device

Devices can be assigned to primary or secondary users. In this view, you can assign or unassign these types of users to the selected device by creating a relationship between the two objects. For more information about the types of users, refer to the Understanding users and user types topic.

A **User** is any person that has a "relation" with the respective computer, that is, a user that can log on to the **Device** to execute operations on it. Every time a user-device relation is modified, the user is automatically assigned any missing operational rules that come with the new relation or be unassigned form those not conforming to his new relation.

Creating a relationship between user and device

1. Select **Add Relationship** .
   The **User Relationship** window appears.
2. Click **Select an existing user** next to the **User** box.
   The **Assign to User** window opens on the screen.

> **Note**
>
> It will show you all users that can be assigned to the device.

3. Select the desired user from one of the available list views.
4. Click **OK** .
5. In the **Relation Type** box select the type of the user, that is, if he is to be a primary or secondary user of the device.
   You can only add one primary but as many secondary users as you want to a device.
6. Clear the **Disable automatic relationship update from agent running on the device** box, if you want the agent to automatically update the primary user for the device when he changed.
7. Click **OK** to confirm the device user.

You have now added a user to the device. The user will now be always updated on all operational rules that are assigned/unassigned from its device.

Managing device groups

In BMC Client Management, **Device Groups** are another way of organizing all managed devices within your network. The structure defined through the groups is individual and freely configurable by the administrator. These groups can contain any type of device, that is, clients, relays or even the master server. Devices can also be present in more than one group. For example, a Windows 7 client may be in a group called *Windows 7 Servers* and at the same time in another group called *Accounting Clients*. Device groups can thus be used to create extensive and comprehensive inventories, facilitate the installation of new software within the network, or to simply modify a configuration setting.

The main **Device Groups** node has the following subnodes:

- One node for each created device group
- One node for every member device

This section includes:

- Understanding device group types and their criteria
- Performing basic device group tasks
- Performing advanced device group tasks
- Manually populating device groups

For information on dynamically populated device groups, see Managing dynamically populated user and device groups.

Understanding device group types and their criteria

There are two general types of device groups:

- Static device groups
- Dynamic device groups

Static device groups are those which are populated manually, that is, all devices are individually added by the administrator.

Dynamic device groups are populated and maintained through either:

- a query,
- a directory server which was assigned to this group, or
- a compliance rule, which collects the group's members according to their compliance, non-compliance or inability to be evaluated.

The different types of group are distinguished by their icon:

Icon	Description
	static device group
	dynamic device group, managed via assigned queries
	dynamic device group, managed via a directory server
	dynamic device group, managed via a compliance rule. It contains all members which are compliant with the rule criteria
	dynamic device group, managed via a compliance rule. It contains all members which are not compliant with the rule criteria
	dynamic device group, managed via a compliance rule. It contains all members which could not be evaluated

Device group criteria

Device groups can be created according to the following criteria:

- Geographical location of the devices: In this case the groups would be divided in the continents, countries, cities, buildings, etc.
- Corporate structure of the managed devices: The organization through groups could contain in this case the administration and functional divisions of the company, such as Engineering, Support, Sales, Accounting, Directors, and so on.
- Characteristics of the devices: This could either be a group organized according to:
  - the physical components of the clients such as the size of RAM or hard disk, the type of processor, etc.,
  - their operating systems, installed software, and so on, or
  - the function they have within the network, such as relay, first level relay, second level relay, client, and so on.

Performing basic device group tasks

The basic tasks for device groups include:

- Creating a device group

- Deleting device groups

Creating a device group

1. Select **Device Groups** in the left window pane.
   If you want to create a new device group within an existing device group, select the respective device group before continuing with step 2.
2. Select **Edit > Create Device Group** .
   The **Properties** dialog box appears on the screen.
3. Set the properties for the new device group:
   a. Enter a name.
   b. Select from the **Display Nodes** drop down box which subnodes the new group node should display.
   c. Select from the **Device Type** drop down box which types of devices are to be displayed, if in the preceding paragraph you have decided to do so.
   This drop down box is only accessible if the device group is populated dynamically.
4. Click **OK** at the bottom of the window to confirm the data for the new device group.
   A new device group with the specified properties was created.

Deleting device groups

1. Select **Device Groups** in the left window pane.
2. Select the desired device or device group from the table in the right window pane.
3. Select **Edit > Delete** .
4. In the appearing **Confirmation** window click **Yes**.
   The selected device group is deleted immediately.

> **Note**
>
> You need write access to the immediate parent from which the device or device group is being deleted.

Performing advanced device group tasks

The advanced tasks for device groups include:

- Creating device group from a query
- Creating patch group
- Activating a group's operational rules
- Modifying status of a dynamic device group
- Viewing report results
  - Assigning report to a device group
  - Viewing report result of a device group
  - Unassigning report from a device group

Creating device group from a query

To create a device group, to which a query is assigned, the type of the query has to be *Device*.

1. Select **Queries** in the left window pane.
2. Select the query for which you want to create a device group in the right window pane.
3. Select **Edit > Create Device Group** .

The new device group will be created with the same name as that of the query, directly under **Device Groups** in the left window pane. The query assigned to it has the status: *active* .

Creating patch group

To create a new patch group from an existing device group, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select the device group you want to create a patch group from in the left window pane.
   The new patch group has the same members as the selected device group.
3. Select **Edit > Create Patch Group** .
   The **Create Patch Group** dialog box appears.
4. Set the properties for the new patch group:
   a. Enter a name.
   b. In the **Folder** field, enter the name of the desired parent folder or click Browse **...** to find and select one.
5. Click **OK** at the bottom of the window to confirm the data for the new patch group.

A new patch group with the specified properties was created.

Activating a group's operational rules

To be activated, the group's operational rules must at least consist of one step. With this option, you can immediately activate all operational rules assigned to the currently selected group.

> **Note**
>
> Be aware that using this option, the schedule defined for the individual rules is ignored.

The group's operational rules will be activated immediately and executed as soon as they arrive at their destination.

To activate the group's operational rules,

1. Select **Device Groups** in the left window pane.
2. Select the desired device group from the list in the right window pane.
3. Select **Edit > Immediately Activate Group's Operational Rules** .

The group's operational rules were activated for the selected device group and will be executed as soon as they arrive at their destination.

Modifying status of a dynamic device group

In BMC Client Management, you can change the status of dynamic groups of any type. The status of a group can either be *active* or *inactive* .

To modify the status of a group,

1. Select one of the following nodes in the left window pane:
   - **Device Groups**
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select the desired status from the **Group Status** drop-down list of the preceding table in the right window pane.
   The new status was saved and applied to the selected group.

Viewing report results

You can view the report results of a selected group from the **Device Groups > Your Device Group > Report Results** page. Each time a report is generated, a new entry is created. The list with the generated reports in the right window pane is structured as follows:

- **Name** : Displays the name of the generated report. It consists of the local generation date and time of the computer on which the report was generated.
- **XML Status** : Displays the status of the XML version of the respective report.
- **HTML Status** : Displays the status of the HTML version of the respective report.
- **PDF Status** : Displays the status of the PDF version of the respective report.
- **Report Name** : Displays the name of the generated report as defined under the **Reports** node.
- **Public Report** : Defines if the respective report is to be generally accessible via the Report Portal. By default this option is set to *No*.

This section includes:

Assigning report to a device group

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Report Results** in the left window pane.
4. Select **Edit > Assign Report** .
   The **Assign a Report** dialog box appears.
5. Select the desired report from the list in the dialog box.

6. Click **OK** to confirm the assignment.
   A confirmation window appears.
7. Click either the
   - **Yes** to immediately generate the newly assigned report.
   - **No** to only add it to the list of assigned reports.

The selected report was assigned to the selected device group.

Viewing report result of a device group

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Report Results** in the left window pane.
4. Select the desired report result in the right window pane.
5. Select **Edit > View** .

A browser window appears displaying the contents of the selected report result.

Unassigning report from a device group

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Assigned Objects** in the left window pane.
4. Select the subnode **Reports** in the left window pane.
5. Select the desired report from the list in the right window pane.
6. Select **Edit > Unassign Report** .

The selected report was unassigned from the selected device group.

Manually populating device groups

Static groups are populated manually. The following tasks help you manage manually populated device groups:

- Adding device to a device group
- Adding one device group to another device group
- Importing devices from a CSV file
- Removing devices or device subgroups from a device group

Adding device to a device group

1. Select **Device Groups** in the left window pane.
2. Select the parent device group from the right window pane.
3. Select **Edit> Add Device** .
   The **Select a Device** dialog box appears.
4. Select the device to be added to the parent device group.
5. Click **OK** to confirm.
   The parent device group now contains the device selected in step 4.

Adding one device group to another device group

In BMC Client Management, one device group can comprise other device groups.

1. Select **Device Groups** in the left window pane.
2. Select the parent device group from the right window pane.
3. Select **Edit> Add Device Group** .
   The **Select a Device Group** dialog box appears.
4. Select the device group to be added to the parent device group.
5. Click **OK** to confirm.
   The parent device group now contains the device group selected in step 4.

Importing devices from a CSV file

The .CSV file must have the following format:

```
DeviceName,NetworkName,NetworkMask,UserName,DeviceType,OperatingSystemName,NetbiosName,DomainName,
IPAddress,MACAddress,AssetTag,Notes MyDevice1,MyDevice1.com,255.255.255.0,"James Kirk",... MyDevice2,
MyDevice2.com,255.255.255.0,"First Spy",...
```

The following rules apply for format of the file content:

- The first line (Header) must list all attributes for the devices that are listed in the file. It is not necessary that all attributes are present.
- The first value must be the DeviceName, the remaining columns can be placed in a different order.
- The number of attributes listed in the Header line must match the number of values in the following lines per device. If the numbers do not match, the import will stop at the first error.
- Double-quotes are accepted and recommended for each cell.
- Only the comma is accepted as separator character, do not add spaces.
- If the `DeviceType` is to be localized in the CM console it must be one of the following values:
  VoIP adapter, VoIP phone, WAP, firewall, broadband router, storage-misc, bridge, print server, specialized, PBX, webcam, power-device, media device, phone, remote management, telecom-misc, proxy server, security-misc, terminal, load balancer, printer, PDA, game console, general purpose, router, switch, server.

Device lists in the form of .csv files can be directly imported into the CM database with all their provided information. This way you can create new devices in the database and update existing devices with new values.

To import the devices listed in a .csv file,

1. Select **Device Groups** from the left window pane.
2. Select the group in the left window pane to which devices are to be added.
3. Select **Edit > Import Devices from CSV File** .
   The **Open** dialog box appears on the screen.
4. Browse to the desired .csv file and select it.

5. Click **Open** to open the list.
   The **Select Devices from the List** dialog box appears on the screen.
6. Select the device from the list to be added to the group.
   You can select all devices in the list by clicking **Select All**.
7. Check the **Create not Existing Devices** box if the list contains devices which are not yet in the CM database and which are to be created.
8. Click **OK** to confirm.
   Not existing devices are added to the CM database.

If changes on existing devices were made, the **Import a CSV File** dialog box appears on the screen with options to save the import results as a .xml file via the respective icon .

If operational rules are assigned to the device group you are adding the imported devices to and the respective system variable is activated, a confirmation window appears.

Removing devices or device subgroups from a device group

Members can only be manually removed from a device group if the group is not assigned to a directory server or a query, or if the query is inactive.

1. Select **Device Groups** in the left window pane.
2. Select the object(s) to be removed.
   You can select multiple objects by either pressing the CTRL-key and selecting the desired objects, or by selecting the first object, pressing and holding the Shift-key, then selecting the last object.
3. Select **Edit > Remove** .
   A **Confirmation** dialog box appears.
4. Click **OK** to confirm the removal.
   The selected objects were removed.

Managing users and user groups

User groups are a way of organizing all defined users within your network. User groups are created as organizational containers for different types of users. They can contain any number of user groups and users for managing the client system. The structure defined through the user groups is individual and freely configurable by the administrator. A single user can be a part of multiple user groups. The main **User Groups** node has the following subnodes:

- One node for each **User Group**
- One node for each **User**

This section includes:

- Performing advanced tasks
- Manually populating user groups

Understanding users and user types

In BMC Client Management, users can be any member of the organization with a system login to at least one client in the network. They are used to execute specific tasks on the system to which they have access via the Agent Interface . The users will execute these tasks via operational rules to which they are assigned by the administrator via the console. Contrary to administrators the users usually do not have access, that is, a login and password, to the console.

Users are furthermore created to provide specific people of the company with specific access limitations to the Agent Interface . Because operational rules are assigned to users and not to devices, the users will always see the same view of assigned operational rules, no matter which client they are using.

User types

In BMC Client Management, based on the relationship of the user with the device, the user can either be:

- **Primary user**: The primary user of the device is the user most often and longest logged on to the device, as calculated by the agent. If the automatic primary user update feature is deactivated, this user can be defined manually and will remain thus until either manually modified or the automatic update is reactivated.

  > **Note**
  >
  > A device can only have one primary user.

- **Secondary user**: The secondary user is any other user that can log on to the device. A device can have more than one secondary user.

Understanding user groups and user group types

There are two general types of user groups:

- Static user groups: Static user groups are those which are populated manually, that is, all users are individually added by the administrator.
- Dynamic user groups: Dynamic user groups are populated and maintained through either a query or a directory server. For more information on dynamically populated user groups, see Managing dynamically populated user and device groups.

The different types of group are distinguished by their icon:

Icon	Description
	Static user group
	Dynamic user group, managed via assigned queries
	Dynamic user group, managed via a directory server

Managing device-user relationship

A **User** is any person that has a "relation" with the respective computer, that is, a user that can log on to the **Device** to execute operations on it. Devices can be assigned to either primary user or secondary users. You can assign or unassign these types of users to the selected device by creating a relationship between the two objects. Every time a user-device relation is modified the user will be automatically assigned any missing operational rules that come with the new relation or be unassigned form those not conforming to his new relation.

Creating a relationship between a device and a user

1. Select **Add Relationship** .
   The **User Relationship** window appears.
2. Click **Select a device** next to the **Device Name** field.
   The **Assign a Device** window opens on the screen. It will show you all devices that may be assigned to the user.
3. Select the desired device from one of the available list views.
4. Click **OK** .
5. In the **Relation Type** field select the type of the user, that is, if he is to be a primary or secondary user of the selected device.
   A user can be the primary user and secondary users of as many secondary devices as necessary.
6. Clear the **Disable automatic relationship update from agent running on the device** box, if you do want the agent to automatically update the primary user of this device.
7. Click **OK** to confirm the device user.

You have now defined a device of which the selected user is a user. The user will now be always update on all operational rules that are assigned to/unassigned from this device.

Performing basic tasks

The basic tasks for user and user groups include:

- Creating a user
- Creating a user group
- Deleting users or user groups

Creating a user

Users can either be a standalone user or member of a user group. If the new user shall be a standalone user, skip step 2.

To create a new user, proceed as follows:

1. Select **User Groups** in the left window pane.
2. Select the desired user group for the new user.
3. Select **Edit > Create User** .
   The **Properties** dialog box appears.
4. Enter the desired data in the respective boxes.
5. Click **OK** at the bottom of the window to confirm the data for the new user.

A new user with the specified properties was created.

Creating a user group

1. Select **User Groups** in the left window pane.
   If you want to create a new user group within an existing user group, select the respective user group before continuing with step 2.
2. Select **Edit > Create User Group** .
   The **Properties** dialog box appears.
3. Enter a name for the new user group.
4. Click **OK** at the bottom of the window to confirm the data for the new user group.

A new user group with the specified name was created.

Deleting users or user groups

You need write access to all parents, from which the user or user group is being deleted.

1. Select **User Groups** in the left window pane.
2. Select the desired user or user group from the table in the right window pane.
3. Select **Edit > Delete** .

The selected user or user group will be deleted immediately.

Performing advanced tasks

The advanced tasks for user and user groups include:

- Creating user group from a query
- Modifying status of a dynamic user group

Creating user group from a query

To create a new user group, to which a query is assigned, the type of the query has to be *User* .

1. Select **Queries** in the left window pane.
2. Select the query for which you want to create a user group in the right window pane.
3. Select **Edit > Create User Group** .

The new user group was created with the same name as that of the query. It displays directly under **User Groups** in the left window pane and the query assigned to it has the status: ***active***.

Modifying status of a dynamic user group

In BMC Client Management, you can change the status of dynamic groups of any type. The status of a group can either be *active* or *inactive* .

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select from the **Group Status** drop-down list of the preceding table in the right window pane the desired status.

The new status was saved and applied to the selected group.

Manually populating user groups

You can manually populate static user groups. The following tasks help you manage manually populated user groups:

- Adding user to a user group
- Adding a user group to another user group
- Removing users or user groups

Adding user to a user group

1. Select **User Groups** in the left window pane.
2. Select the parent user group from the right window pane.
3. Select **Edit > Add User** .
   The **Select a User** dialog box appears.
4. Select the user to be added to the parent user group.
5. Click **OK** to confirm.

The parent user group now contains the user selected in step 4.

Adding a user group to another user group

1. Select **User Groups** in the left window pane.
2. Select the parent user group from the right window pane.

3. Select **Edit > Add User Group** .
   The **Select a User Group** dialog box appears.
4. Select the user group to be added to the parent user group.
5. Click **OK** to confirm.

The parent user group now contains the user group selected in step 4.

Removing users or user groups

Users can only be manually removed from a user group if the group is not assigned to a directory server or a query, or if the query is inactive.

1. Select **User Groups** in the left window pane.
2. Select the object(s) to be removed in the right window pane.
   You can select multiple objects by either pressing the CTRL-key and selecting the desired objects, or by selecting the first object, pressing and holding the Shift-key, then selecting the last object.
3. Select **Edit > Remove** .
   A confirmation window appears.
4. Click **OK** to confirm the removal.
   The selected objects were removed.

Discovering assets

Devices that are connected to the network but on which no BMC Client Management (BCM) agent is installed can be remotely inventoried by any CM agent, which collects the software and hardware inventory of these devices.

Unmanaged devices in BCM are devices of your infrastructure that:

- Are never connected to the network or
- Do not have a BCM agent installed

Nevertheless, BCM provides possibilities to inventory (hardware and software) these devices and include the generated inventories in the BCM database. The custom inventory for unmanaged devices can only be created directly in the BCM console.

The **Asset Discovery** functionality of BCM allows you to scan your network or parts of your network for all existing assets. It finds all types of assets, PCs, printers, routers, and so on, with and without CM agent installed. The discovery also scans the devices for their basic information such as operating system and inventories and displays these in the console window.

Components

Asset Discovery in BCM is done via a number of different components and objects listed in the following, and on which you can see detailed information in the following sections and topics:

- Asset discovery scanner
  The **Asset Discovery Scanner** is any device in your network, defined as the scanner. It is responsible for the whole scanning process. By default the master is predefined as the scanner, but any other device with a reasonably strong configuration fitting the previously mentioned requirements can take over this role.
- Discovered device inventory
  The discovered device inventory for a device or a group is an extraction of the inventories available and generated by the BCM agent, that is, it generates the discovered hardware, software and parts of the security inventory for all discovered assets as well as the connectivity inventory, that is, the actual physical connections between the devices.
- Asset discovery wizards
  BCM also has a wizard that guides you through the different options of scanning your network devices and launching the scans.

Prerequisites

The following prerequisites must be fulfilled for asset discovery to be operable:

- The operating system of the scanner device must be Windows XP, Windows 2003, Workstation and Server for all versions, Windows Vista Business and Ultimate, 64-bit Windows, Windows 2008, Windows 2008 R2 64 bit, Windows 8, Windows 8.1, Windows 2012 R2 64-bit or Linux AS/ES 3 and 4, CentOS and SUSE.
- The master/scanner should have a permanent Internet connection, preferably via Ethernet, it *mustnot* use a wireless connection.
- IPv6 addresses are supported by the asset discovery, however, be aware that specifying complete IPv6 subnets can take a very long time. It is recommended not to do so.

For information on configuring asset discovery, see Configuring asset discovery.

Managing asset discovery scans

A scan presents information about its configuration, that is, its targets, ports, schedule, and so on, and details on its last execution. Each **Asset Discovery Scan** node has the following tabs:

- Scan Configuration
- Target Lists
- Assigned Schedule
- Sessions

The following topics are provided:

- Assigning a configuration to a scan
- Assigning a schedule to a scan
- Reassigning scan
- Activating scan
- Reassigning scan

- Canceling scan
- Assigning a target list to a scan
- Viewing scan sessions
- Viewing scan log

Assigning a configuration to a scan

If you manually created the scan, you might still need to assign a configuration to it. If the scan was created by the wizard, the configuration might already be defined. You can change an assigned scan configuration by first removing the currently assigned configuration as explained and then adding the newly required one. To do so, proceed as follows:

1. Click **Edit > Assign Scan Configuration** .
   The **Assign a Scan Configuration to the Scan** dialog box opens on the screen. It displays the list of available scan configurations in its **Available Objects** box.
2. Select the desired configuration
3. Click **OK** to add it and close the window.

Assigning a schedule to a scan

When a scan is created it is automatically assigned a scheduler. The **Assigned Schedule** tab of the scan's node provides the possibility to modify the timer for the currently selected scan and to define when and at which frequency it is to run. The default settings of the scheduler's timer are to execute the scan once a immediately with immediate activation as well, however, the assignment is still paused. If you created the scan via the wizard you will also defined the schedule, and these settings will be displayed here.

Parameter	Description
Status	The fields of this column display the status of the scan.
Last Status Update Time	This time value indicates at which date and time the status previously displayed was updated by the target's agent for the last time.
Activation	This field shows the condition on which the scan will start executing on the targets.
Schedule	The fields of this column display the frequency with which the scan will be executed on the assigned device.
Termination	This field displays when the scan execution is scheduled to be terminated, that is, when the scan is to be run for the definitely last time of the current scheduling cycle.
Time of Assignment	This field displays the date and time at which the assignment between the objects was created in the database.

Reassigning scan

If you made modifications to a scan which is already assigned for execution it must be reassigned. To reassign, proceed as follows:

1. Select the scan which is to be reassigned in the table in the right window pane.
2. Click **Edit > Reassign Scan** .

The reassignment process of the scan will be launched.

Activating scan

Depending on the choice of activation the scan might be deactivated. To activate, proceed as follows:

1. Select the entry to activate in the table in the right window pane.
2. Click **Edit > Activate Scan** .

The scan will be automatically activated.

Reassigning scan

If you made modifications to a scan which is already assigned for execution it must be reassigned. To reassign, proceed as follows:

1. Select the scan which is to be reassigned in the table in the right window pane.
2. Click **Edit > Reassign Scan** .

The reassignment process of the scan will be launched.

Canceling scan

To cancel a currently executing scan proceed as follows:

1. Select the scan to stop in the table in the right window pane.
2. Click **Edit > Cancel Scan** .

The scan will be stopped.

Assigning a target list to a scan

The Targets Lists tab of a scan displays the target lists and targets the scan is to check. These lists can contain individual devices with or without a CM agent installed and all the members of already existing device groups.

If you manually created the scan, you need to assign target lists to it. If the scan was created by the wizard, these might already be defined. You can also add additional targets or target lists later on, which is done via this tab. To do so, proceed as follows:

1. Select the **Target Lists** tab of the scan to which you want to add a new target list.
2. Click **Edit> Assign Target List** .
   The **Assign a Target List** dialog box opens on the screen. It displays the list of available target lists in its **Available Objects** box.
3. Select the desired target list(s)
4. Click **OK** to add it and then close the window.

Viewing scan sessions

Scans are executed in sessions. A session is the complete scanning of one device of the target list. Generally an executing scan consists of as many sessions as it has targets, which can, however, not all be executed at the same time. The number of simultaneously running sessions can be defined in the settings of the Asset Discovery module of the respective scanner.

The **Sessions** tab displays the following information about the different sessions of the currently executing scan on the scanner:

Parameter	Description
Status	These fields display the current scan status of the respective target. If the target cannot be scanned, that is, it is not contactable, the status displays `Unreachable`.
Device Name	The fields of this column display the names of the scan targets.
IP Address	The IP address of the device in its dotted version, such as 194.50.68.255.
Operating System Name	Name The name of the operating system installed on the discovered device.
NMAPOS	The field indicates the status of operating system detection via Network Mapper (NMAP). (See the legend at the bottom of the table for status information.)
SSH	The field indicates the status of Secure Shell (SSH) credential validation. (See the legend at the bottom of the table for status information.) If the SSH credentials are valid, SSH is used to detect operating system, software, and hardware. If the credential validation fails, the SSHOS, SSHSW, and SSHHW tests are not run and the corresponding columns remain empty.
SMB	SMB The field indicates the status of Server Message Block (SMB) credential validation. (See the legend at the bottom of the table for status information.) If the SMB credentials are valid, SMB is used to detect operating system and software. If the credential validation fails, the SMBOS and SMBSW tests are not run and the corresponding columns remain empty.
WMI	WMI The field indicates the status of Windows Management Instrumentation (WMI) credential validation. (See the legend at the bottom of the table for status information.) If the credentials are valid, WMI is used to detect operating system, software, and hardware. If the credential validation fails, the WMIOS, WMISW, and WMIHW tests are not run and the corresponding columns remain empty.
SNMP	SNMP The field indicates the status of Simple Network Management Protocol (SNMP) credential validation. (See the legend at the bottom of the table for status information.) If the SNMP credentials are valid, SNMP is used to detect operating system, hardware, and network connectivity. If the credential validation fails, the SNMPOS, SNMPHW, and SNMPCON tests are not run and the corresponding columns remain empty.
SSHOS	SSHOS The field indicates the status of operating system detection via SSH. (See the legend at the bottom of the table for status information.)

Parameter	Description
SMBOS	SMBOS The field indicates the status of operating system detection via SMB. (See the legend at the bottom of the table for status information.)
WMIOS	WMIOS The field indicates the status of operating system detection via WMI. (See the legend at the bottom of the table for status information.)
SNMPOS	SNMPOS The field indicates the status of oeprating system detection via SNMP. (See the legend at the bottom of the table for status information.)
SSHSW	SSHSW The field indicates the status of software detection via SSH. (See the legend at the bottom of the table for status information.)
SMBSW	SMBSW The field indicates the status of software detection via SMB. (See the legend at the bottom of the table for status information.)
WMISW	WMISW The field indicates the status of software detection via WMI. (See the legend at the bottom of the table for status information.)
SSHHW	SSHHW The field indicates the status of hardware detection via SSH. (See the legend at the bottom of the table for status information.)
WMIHW	WMIHW The field indicates the status of hardware detection via WMI. (See the legend at the bottom of the table for status information.)
SNMPHW	SNMPHW The field indicates the status of hardware detection via SNMP. (See the legend at the bottom of the table for status information.)
SNMPCON	SNMPCON The field indicates the status of network connectivity detection via SNMP. (See the legend at the bottom of the table for status information.)
Detail	This field displays the latest status of the scan.
Discovery Time	This column displays the date and time at which the individual devices were discovered for the first time.
Start Time	The date and time at which the scanning session was started on the target client.
End Time	The date and time at which the session finished.
Duration (Sec)	The the total time the session needed to execute in the regular time format hh:mm:ss.
MAC Address	The MAC, that is, the hardware address of the currently discovered device.

Legends:

- Yellow ( ): Operation in progress
- Red ( ): Operation failed
- Green ( ): Operation successful
- (Empty cell): Operation not performed as the protocol credentials are either not supplied or are invalid.

Viewing scan log

You can view the log of each item in the inventory scan. To view the log:

- Right click the row for which you want to view the log and select **Display Log** .

Viewing result of the last scan

You can view the result of the last asset discovery scan to check the status of individual protocols. You can also check the log for each device.

This topic includes:

Viewing the scan result

1. Navigate to **Asset Discovery** > **Scanners** > **(Your scanner)** > **Module Configuration**.
2. Select the **Device List** tab.
   The following information is displayed about the last scan:

Parameter	Description
Status	These fields display the current scan status of the respective target. If the target cannot be scanned, that is, it is not contactable, the status displays `Unreachable`.
Device Name	The fields of this column display the names of the scan targets.
IP Address	The IP address of the device in its dotted version, such as 194.50.68.255.
Operating System Name	Name The name of the operating system installed on the discovered device.
NMAPOS	The field indicates the status of operating system detection via Network Mapper (NMAP). (See the legend at the bottom of the table for status information.)
SSH	The field indicates the status of Secure Shell (SSH) credential validation. (See the legend at the bottom of the table for status information.) If the SSH credentials are valid, SSH is used to detect operating system, software, and hardware. If the credential validation fails, the SSHOS, SSHSW, and SSHHW tests are not run and the corresponding columns remain empty.
SMB	SMB The field indicates the status of Server Message Block (SMB) credential validation. (See the legend at the bottom of the table for status information.) If the SMB credentials are valid, SMB is used to detect operating system and software. If the credential validation fails, the SMBOS and SMBSW tests are not run and the corresponding columns remain empty.
WMI	WMI The field indicates the status of Windows Management Instrumentation (WMI) credential validation. (See the legend at the bottom of the table for status information.) If the credentials are valid, WMI is used to detect operating system, software, and hardware. If the credential validation fails, the WMIOS, WMISW, and WMIHW tests are not run and the corresponding columns remain empty.
SNMP	SNMP The field indicates the status of Simple Network Management Protocol (SNMP) credential validation. (See the legend at the bottom of the table for status information.) If the SNMP credentials are valid, SNMP is used to detect operating system, hardware, and network connectivity.

Parameter	Description
	If the credential validation fails, the SNMPOS, SNMPHW, and SNMPCON tests are not run and the corresponding columns remain empty.
SSHOS	SSHOS The field indicates the status of operating system detection via SSH. (See the legend at the bottom of the table for status information.)
SMBOS	SMBOS The field indicates the status of operating system detection via SMB. (See the legend at the bottom of the table for status information.)
WMIOS	WMIOS The field indicates the status of operating system detection via WMI. (See the legend at the bottom of the table for status information.)
SNMPOS	SNMPOS The field indicates the status of oeprating system detection via SNMP. (See the legend at the bottom of the table for status information.)
SSHSW	SSHSW The field indicates the status of software detection via SSH. (See the legend at the bottom of the table for status information.)
SMBSW	SMBSW The field indicates the status of software detection via SMB. (See the legend at the bottom of the table for status information.)
WMISW	WMISW The field indicates the status of software detection via WMI. (See the legend at the bottom of the table for status information.)
SSHHW	SSHHW The field indicates the status of hardware detection via SSH. (See the legend at the bottom of the table for status information.)
WMIHW	WMIHW The field indicates the status of hardware detection via WMI. (See the legend at the bottom of the table for status information.)
SNMPHW	SNMPHW The field indicates the status of hardware detection via SNMP. (See the legend at the bottom of the table for status information.)
SNMPCON	SNMPCON The field indicates the status of network connectivity detection via SNMP. (See the legend at the bottom of the table for status information.)
Detail	This field displays the latest status of the scan.
Discovery Time	This column displays the date and time at which the individual devices were discovered for the first time.
Start Time	The date and time at which the scanning session was started on the target client.
End Time	The date and time at which the session finished.
Duration (Sec)	The the total time the session needed to execute in the regular time format hh:mm:ss.
MAC Address	The MAC, that is, the hardware address of the currently discovered device.

Legends:

- Yellow ( ): Operation in progress
- Red ( ): Operation failed
- Green ( ): Operation successful
- (Empty cell): Operation not performed as the protocol credentials are either not supplied or are invalid.

Viewing scan log

- Right click the row for which you want to view the log and select **Display Log**  .
  The logged entries for the selected row is displayed.

Managing discovered devices

After successful scan, the **Discovered Devices** node provides the list of all devices without BMC Client Management agent.

You can perform the following operations on the discovered devices:

- Rolling out agent to a discovered device
- Viewing inventory of a discovered device
- Viewing inventory status
- Purging inventory

This list shows all discovered devices independent of their function, such as servers, workstations, printers or game consoles.

Parameter	Description
Name	The name of the scanned device. If no name is available the IP address will be displayed instead. The icon of the device will indicate the operating system of the device, that is, if it is a Windows, a Linux or a Mac device for discovered PCs and the type of device for any other type of hardware, etc, if it is a switch, a router, and so on.
IP Address	The IP address of the scanned device.
Topology Type	The topology type of the device, which in this case will either be **Unmanaged Device** or **Scanned Device** , if the device was already scanned.
Type	This field displays the purpose type of the discovered device, that is, if it is a server, a workstation, a switch, a game console, and so on.
Operating System	The operating system running on the scanned device.
Virtual Guest Count	The number of virtual machines that are located on the discovered device.
Discovered By	The name of the scanner that discovered the device.
Discovery Date	The date and time at which it was discovered.

A discovered device is an unmanaged device scanned by the Asset Discovery Scanner for its assets. It displays the information found as usual in the form of tabs and subnodes.

The following information can be collected for unmanaged devices:

- General information displayed on the device's **General** tab.
- Inventory information which can be found under the respective nodes:
  - Connectivity inventory displayed in the device's **Connectivity** node.
  - Custom inventory displayed in the device's **Custom** node.
  - Hardware inventory displayed in the device's **Hardware Inventory** node.
  - Software inventory displayed in the device's **Software Inventory** node.

Rolling out agent to a discovered device

You can select in this list of scanned devices a number of them that do not yet have the BMC Client Management agent installed and create a new agent rollout to directly install the agent on them. Be aware, that this shortcut only works for devices on which no agent is yet installed, you cannot upgrade the agent this way.

1. Select the target device(s) in the table in the right window pane.
2. Click **Edit> Agent Rollout**  .
   The **Agent Rollout Wizard** appears.
3. Follow the instructions in the wizard and provide the required information. For more details on the wizard and its parameters refer to the Automatically Rolling out the CM agent via the Wizard section.
4. Click **Finish** to confirm all choices in the wizard and launch the rollout as scheduled.

Viewing inventory of a discovered device

The inventory for a device is accessed through the device's **Inventory** subnode. It provides access to all different types of inventory that can be collected for a device.

Its information displays via its tabs:

- Asset Summary: For more information, see Viewing inventory details.
- Hardware Inventory: For more information, see Hardware Inventory of a discovered device.
- Software Inventory: For more information, see Software Inventory of a discovered device.
- Inventory Status: For more information, see Inventory Status for a device.

The specific inventory information can be accessed via the respective subnodes:

- Connectivity Inventory: The Connectivity for a discovered asset is only available if the asset is a hardware that can be contacted via SNMP and is able to connect other hardware devices, for example, if it is a router, a switch, and so on. This inventory then displays the hardware connections of this asset. For more information about the hardware inventory of a device, see Connectivity asset summary of a discovered device.
- Custom Inventory: The **Custom Inventory** for an unconnected or a discovered device provides the same data and information as for any other device in the network. Contrary to other inventory types, however, it is not collected remotely by an agent, it must be directly created in the device's console view. For more information about how to create the custom inventory of a device and its possibilities refer to the Custom Inventory topic.

- Hardware Inventory: The **Hardware Inventory** for an unconnected or discovered device provides the same data and information as for any other device in the network. For more information about the hardware inventory of a device refer to the Hardware Inventory topic.
- Software Inventory: The **Software Inventory** for an unconnected or discovered device provides the same data and information as for any other device in the network. For more information about the software inventory of a device refer to the Software Inventory topic.

Viewing inventory status

The **Inventory** node displays the following information about the different types of inventory available for the currently selected device. This tab is not available if no inventories can be generated due to license restrictions.

Parameter	Description
Name	The fields of this column list the available types of inventory.
Last Update	The date and time the respective inventory type was last updated.
Status	This field displays the license status for the inventory type, that is, if it is exceeded or expired. If the field is empty the license is valid. This field is applicable if no inventory has yet been generated. If the license is not valid this type of inventory cannot be generated for the respective device.

Purging inventory

All other inventory types can be purged. All inventory data will be deleted in this case. This operation is also taken into account by the Inventory license which will then be incremented again. If the device for which the inventory is purged does not have a CM agent installed, that is, it is of topology type **Scanned Device** , not only the inventory will be purged but the device itself will be deleted from the CM database. To purge a device and all its connected data from the database, proceed as follows:

1. Select the inventory to purge from the list in the left window pane.
2. Select the **Edit > Purge** .
   A confirmation window appears.
3. Click **Yes** to confirm and delete all hardware inventory data.

Discovering the assets via the wizard

Asset Discovery scans can also be configured and executed via the provided wizard.

The wizard can either use existing objects to execute or it can create new ones. Be aware, that to create new objects you need the manage capability for the top node of the respective object or at least one of its folders. By default objects created with the wizard will be located directly under the object‘s top node. If you do not have access to this node the new object will be created in the first

folder for which you do have access rights. Otherwise, that is, if you do not have access to any of the objects of the type the object created via the wizard will be stored under the **Lost and Found** node. However, you now also have the possibility to specify the target directory for the newly created objects.

The **Asset Discovery** wizard is available under the main **Asset Discovery** node and on the main **Wizards** menu which is always present, thus can be called at any moment.

- From anywhere in the console select the **Wizards > Asset Discovery** menu item.
- The wizard appears with its first window, which lets you perform the following:
  - Discovery Type
  - Executing an Automatic Scan
  - Defining a Configurable Discovery
  - Defining the Scanner
  - Selecting the Scan Configuration
  - Defining a New Scan Configuration
  - Defining the Scan
  - Protocols
  - Defining the Target List
  - Configuring a new target list
  - Scheduling the Scan

Discovery Type

The first wizard window allows you to decide if you want to execute an asset discovery scan with the predefined default values or if you would like to create a new customized scan.

> **Note:**
>
> If you want to scan your network for virtual devices and physical ones you need to use the customized scan.

1. Select the radio button for the scan type you want to execute.
   a. If you have left selected the **Automatic** radio button to execute a default scan the following list now explains the values that will be used for the default scan.

      > Be aware that the master will not be scanned using this option.

   b. Enter the login to access the remote devices into the **Windows Login (DomainLogin)** and **Windows Password** boxes.

      >

The login name must have the following format:

- <domain name>/<user logon> if you are on a domain,
- <user logon> if you are not on a domain.

Executing an Automatic Scan

This window provides a recaptitulation of the options defined for an automatic scan of your assets.

1. Check all defined options.
2. To modify any values click **< Back** to return to the previous window and select the **Configurable** option.
3. If all options are defined as desired click **Scan Now** to launch the scan.

Defining a Configurable Discovery

In the second window you can define which parts of the scan are to be specifically defined, and for which the default values are to be used.

1. Select the respective radio buttons in the different boxes.
   Depending on your choices the corresponding steps in the hierarchy on the left will be highlighted and become available.
2. Click **Next** to continue.

Defining the Scanner

The **Scanner** window only appears if you selected to *not* use the Master as your scanner. In this case another device to be used as the scanner must be selected.

1. Select the scanner device which is to execute the scan that is being defined via the wizard.

   If none of the defined scanners fits your requirements, you can also add another device as a Scanner:

   a. Click **Add Scanner** on top of the list box.
      The **Add a Scanner** pop-up window appears displaying the list of all devices that can be a scanner because of their operating system.
   b. Select the device to be added from one of the list boxes.
   c. Click **OK** to confirm and close the window.
      The device will be added to the table of Scanners and its configuration parameter will be updated.
   d. Select the newly defined scanner in the list.
2. Click **Next** to continue.

Selecting the Scan Configuration

This window appears if you selected to use an existing scan configuration instead of creating a new one. It displays all scan configurations that are available.

1. Select the desired scan configuration from the displayed list of existing configurations.
2. Click **Next** to continue.

Defining a New Scan Configuration

This window will only be displayed if the option to create a new configuration was selected.

1. Enter the required information in the respective boxes.
2. Click **Next** to continue.

Defining the Scan

In this wizard window, a unique descriptive name must be defined for the scan. This is the name of the scan which will be created with the data you define in the next windows and which will be added to the list of assigned scans under the selected scanner's node.

1. Enter a name for the new scan into the **Name** field.
2. Select a folder if the new scan is to be located in a specific folder.
3. Click **Next** to continue.

Protocols

The **Protocols** window only displays on the screen, if you are defining a new scan configuration. In this window you can define which protocols are to be used for scanning.

1. By default all protocols are activated, to deactivate a protocol clear the box next to it.

   > If you are not scanning for virtual devices you can clear the **VMware vSphere** and **Hyper-V** protocols.

2. To add credentials to a protocol select its entry in the table and then click **Add Credential** to the right.
   The **Credentials** box becomes available.
3. To add a new user identification click **Add** at the bottom.
   The **Properties** dialog box appears.
4. Enter the login name and corresponding password in the respective text boxes and reenter the password for confirmation. The login name must have the following format:
   - `<domain name>/<user logon>` if you are on a domain,
   - `<user logon>` if you are not on a domain.

5. If you are adding credentials for the SNMP protocol you must enter into these text boxes the name of the community and confirm it by re-entering into the respective field.
6. To view the passwords/communities you can also clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
7. To confirm the new user account click **OK** at the bottom of the window.
8. The account will be added to the list in the right part of the dialog.
9. Repeat the preceding steps to add more authentications if necessary.
10. To delete an existing user login from the selected protocol select it in the table and click **Delete** below the box.
11. Click **Next** to continue.

Defining the Target List

This window only displays if you selected to use an existing target list instead of creating a new one:

1. Select the target list to be used from the list of existing target lists.
2. Click **Next** to continue.

Configuring a new target list

This step is only required if you decided to create a new target list for the devices to scan.

1. Enter a name for the new target list into the **Name** field and define a specific folder if necessary.
2. Add the devices to the scan. For this you have a number of different methods available.

See:

- Adding targets from lists
- Adding existing devices as targets
- Adding existing device groups as targets
- Adding targets via an address range

3. Click **Next** to continue.

Scheduling the Scan

This step will only be displayed if you decided to define a specific schedule for the scan. You can define the intervals and frequencies at which the scan is to be run.

1. Select in the **Validity** tab first the date of the actual execution by selecting the respective radio button.
2. Select in the **Termination** box when the scan is to be run for the last time.
3. Select the **Frequency** tab.

4. Here you can define the interval at which the scan is to be executed.
   Depending on the choice made at the radio buttons the different additional options of this tab become available.
5. When you made your selections click Finish to confirm all scan configuration choices and launch the process.

A confirmation window appears now on the screen. Here you can define the focus of the console, that is, which node will be displayed once the wizard closes and the scan in launched.

- To go directly to the newly created scan check the **Go to Scan** box.
- To immediately activate the new scan click **Yes** .
- To create the scan without activating it, click **No** . To launch this scan it must then be activated specifically via its **Assigned Schedule** tab.

Rolling out agents

The following topics are provided for rolling out agent:

- Agent rollout overview
- Getting started with agent rollout
- Rolling out your first agent
- Downloading and installing a rollout from a server
- Scheduling a rollout
- Alternative rollout methods
- Uninstalling the client agent via rollout
- Managing targets of a rollout
- Automatically rolling out agent using a wizard

Agent rollout overview

BMC Client Management provides you with a rollout mechanism through which you do not have to physically visit each device on your network to manually carry out the install procedure of the CM agent . Client Management contains a node directly accessible via the CM console , which distributes the agents to any number of networked devices. This rollout also enables reinstalling and uninstalling, if and when required.

The rollout functionality includes two separate modes in order to fulfill the maintenance operations. The active mode (Push) prepares and installs CM agents on remote devices while the passive mode (Pull) bundles the Client Management software so it can be downloaded and installed manually by end users via a specific page on the agent interface.

Rollout folders are created as organizational containers for different types of rollouts. They can contain any number of predefined or custom-made rollouts for the management of the client system.

The Client Management Rollout makes the installation, reinstallation, or uninstall of the CM agent on your client population a quite simple and quickly executed task. All different installation possibilities are executed through the same operation.

A rollout is configured via the parameters provided by the rollout's subnodes:

- Agent Configuration
- Post-Install
- Servers

Getting started with agent rollout

The following sections guide you through the startup of all parts of the software and through your first login to the BMC Client Management console.

The following information is provided:

- Importing the licenses and license types
- Logging on to console
- Preparing console for agent rollout

The BMC Client Management agent installed on the master should start up automatically. To verify this, you must proceed as follows, depending on your operating system. If your agent should not be running for any reason you can also find out how to start it. This process is also valid for the startup of the client agents, therefore you can also find a paragraph for MAC, which is not available as a master agent.

After these agents are running they are filling in their data into the Client Management database on the master.

Depending on the operating system, there are different ways to start the client agent:

- Starting the client agent on Windows
- Starting the client agent on Linux
- Starting the client agent on Mac

Starting the client agent on Windows

The CM agent icon should be displayed in the systray of your master server or client when the agent is running. It can be one of the following colors indicating a specific status:

- The icon is gray during the agent's initialization.
- The icon is blue when the agent is running.
- The icon is green or flashing green when an operation is in progress.
- The icon is red when the agent tries to carry out an unauthorized action or access.
- The icon turns yellow when the local device is taken over through remote control.

- The blue icon  shows a package when packages and operational rules are advertised to the client and are available for download and installation.

If you want to start a stopped agent, you need to do so via the Services window of the Control Panel. If you double-click it, a graphic agent interface opens giving the administrator(s) access to various modules and settings related to this agent. The administrator can modify settings and actions via this interface. For more information about this interface, refer to the Agent Configuration topic.

Command line options

The agent can also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.
-i	--install	Installs the service. This option must be used in connection with the -sn "Service Name" option.
-r	--remove	Removes the service. This option must be used in connection with the -sn "Service Name" option.
-sa	--standalone	Starts the agent as standalone.
-cw	--consolewindow	Starts with pop-up menu (for output text).
-sn	--servicename	Used to install/remove using non-default service name.
-dn	--displayname	Used to install/remove using non-default service display name.

Starting the client agent on Linux

The CM agent installed on the master should start up automatically. This can be checked by typing `ps -ax | grep mtxagent` and pressing the Enter key. The console or terminal window should return: **/usr/local/bmc-software/client-management/master/bin/mtxagent** as one of the running processes in the process list that is now displayed.

To start or stop the agent type the following command into a terminal window:

```
service BMCClientManagementAgent start
```

```
service BMCClientManagementAgent stop
```

Command line options

The agent can also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.
-sa	--standalone	Starts the agent as standalone.

Starting the client agent on Mac

The CM agent installed on a Mac device should start automatically after a device reboot. This can be checked by typing `ps -eaf |grep mtxagent` and pressing the Enter key. The console or terminal window should return: **/usr/local/bmc-software/client-management/client /bin/** as one of the running processes in the process list that is now be displayed.

If the agent does not start, type the following into a terminal window:

```
SystemStarter start BMCClientManagementClient
```

then press your **Enter** key. The agent starts now.

The agent can also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.
-sa	--standalone	Starts the agent as standalone.

Importing the licenses and license types

Before you can execute any operation in Client Management, you need to import your license. You should have received a license in the form of a text or xml file from the Support Team.

For more information about licenses, see the following topics:

- Available licenses for BMC Client Management
- License considerations for a super master architecture

> **Attention**
>
> You must install the master on the device for which you provided that data to the Support Team, because this information is used to generate the license; it is not valid for any other device.

1. Click the **Global Settings** node and select from its children the **Licenses** node in the left window pane.
2. Select **Edit > Import License** .
   A dialog box opens displaying the directory structure in a Windows Explorer-like format.
3. Select the file containing your license.
4. With the file selected, click **Open** at the bottom of the window. The information is then read from the file and displayed in the table in the right window pane as follows:

Parameter	Description
Name	The fields in this column display the names of the licenses.
Count	This number indicates how many agents the license contains (that is, on how many devices you can install clients). If you have a temporary license for testing purposes, this number is 20. For all other licenses, this field displays 1 if the license is activated (that is, purchased) or 0 if you do not have this license.
Available	This column indicates the number of remaining licenses. It is applicable to all functionalities with agent counts, such as the agents themselves, patch management, inventory, compliance management, software distribution and so on. It displays how many licenses are still free to be used. For all other purchased licenses this field always displays 1.
Expiry Date	This field is empty, if you have an unlimited license for use in your system. If the license is temporary and thus limited, this field displays the expiry date of the license, in the default format defined in the user preferences. A temporary license is valid 30 days.
Status	This field shows the current status of the license, which should be Valid. If you are using the test license it displays Expiring.

Now that you have installed your license and thus validated your database and console, you are ready to start working with BMC Client Management. You can proceed to installing a relay and rolling out the agent throughout your network, as detailed in the next topics.

Available licenses for BMC Client Management

The following table lists all available licenses and describes their functionalities:

License	Description	Commercial License Module
Application Management	Activates all the different options of application management, that is, the monitoring and prohibiting of applications and self-healing functionalities as well as the software license management for Windows devices, application monitoring, prohibiting and software license management for Linux devices.	BMC Client Management - Inventory
BCM Agents	The basic license of the product; it provides you with the maximum number of agents installed on clients which the database accepts. For the initial and evaluation license this number is fixed at 20. Note that unconnected devices for which the inventory is integrated do not decrease this value (that is, these devices are not counted for licensing purposes).	All licenses
Compliance Management	Activates the device compliance management of BMC Client Management. If you want to include software compliance you require the Software Catalog-specific license as well.	BMC Client Management - Compliance Management
Direct Access	Provides the direct access features to the remote clients of your installation.	Remote Manager
Inventory	Activates all base inventories: software, hardware, custom, connectivity, security, and the inventory of unmanaged devices. All other inventory types are part of their respective functionality.	BMC Client Management - Inventory
Multicast	Activates the multicast transfer option for transferring packages and other information between the CM agents.	All licenses

License	Description	Commercial License Module
Operating System Deployment	Activates the operating system deployment module which allows you to create OS images and deploy them to any device within your network. This feature is only available for Windows devices.	BMC Client Management - Deploy
Patch Knowledge Base Update	Required to maintain the patch knowledge base up to date on which the patch management functionality is based.	BMC Client Management - Patch Management
Patch Management	Defines how many devices can be patched at the same time. For the initial and evaluation license this number is fixed at 20. This license is not available for Linux or Mac OS devices.	BMC Client Management - Patch Management
Power Management	Activates the Green IT / Power Management feature.	BMC Client Management - Compliance Management
Remote Control	Activates the remote control feature. This feature is not available for Linux devices.	Remote Manager
Security Configuration Updates	Required to maintain the Security Products catalog up to date, which is required for the Security Products inventory.	BMC Client Management - Compliance Management
Software Catalog Updates	This license is required to maintain the Software Catalog up to date.	BMC Client Management - Compliance Management
Software Catalog	Activates the Software Catalog option. It is used for software inventory, software compliance, software license management and application management.	BMC Client Management - Compliance Management
Software Distribution	This license activates all software distribution features of the product such as package generation and scheduling the distribution.	BMC Client Management - Deploy
Super Master	This license is required for a super master architecture with a super master and a number of site masters.	BMC Client Management - Compliance Management
Topology Graph	Activates the graphical display of your network topology.	All licenses
Windows Device Management	This license activates the peripheral device monitoring and controlling functionalities for Windows devices.	

License	Description	Commercial License Module
		BMC Client Management - Compliance Management

Logging on to console

The following sections guide you through your first startup and login of the console according to your operating system and the first preparatory actions to take before you can execute any operations.

The following topics are provided:

- Starting the console
- Logging on to the console for the first time
  - Logging on to the console from a device other than the master
  - Logging on to the console from outside the company network

Starting the console

The console is a Java application and can thus be launched using the generally available startup options provided by Java, such as `-Xmxn` to extend the maximum size of the memory allocation (n must be a multiple of 1024, for example: `Xmx80m` or `Xmx81920k`). By default, the anti-aliasing option is used for the console. To switch it off, open the console shortcut's Properties window and modify the `-Dswing.aatext` option from true to false. To launch the console with its standard options follow the steps indicated in the following table, depending on the operating system on which your console is installed:

System	Launching the console
Windows	Click your **Start** menu, select **Programs > BMC Software > Console** or double-click the console desktop icon.
Linux	You need to type `BMCClientManagementConsole`, then press your **Enter**.
Mac OS	Double-click the icon for the console **Web Start** on the desktop.

For information about how to start the console via the command line or Java Web Start and possible parameters see the topics Launching the BCM console via the Command Line and Launching the BCM console via Java Web Start.

Logging on to the console for the first time

When you launch the console for the first time, you must use the predefined default administrator logon `admin` as login name. Because this login has no predefined password, a pop-up menu appears, in the language version of the operating system, or in English, if it is of a language not supported by Client Management, requesting you to define it. After you entered the new password in the respective text box and confirmed it, the console opens on the screen.

Attention

Be aware, that if you installed master and relay agents with the SSL=0 option, you also must use the non secure connection option here to connect the console with the master. If the master and agents are installed with any other SSL option the console only accepts SSL connections.

Note

If you installed master and relay agents with the SSL=3 option, do not forget to supply the client certificate to the console.

Logging on to the console

1. Enter the user name `admin` and no password into the respective boxes.
2. The line **Server:Port** displays the name of the database server and its port number to which the console connects.

   If the console is installed on the master server, this text box is filled in with the default value localhost:1610. If you are connecting via Java Web Start, this text box is filled in with the master information (that is, either the master's name or IP address)

3. Click **Login** at the bottom of the window.

Logging on to the console from a device other than the master

If your console is on a device other than the master, no information is prepopulated.

1. Enter the user name `admin` and no password.

2. Replace the prepopulated localhost entry with the name of the master server you want to connect to and its port number separated by a colon (:) in the **Server:Port** box.

   > You can enter the host name either as its short or full network name such as **scotty** or **scotty.enterprise.com**, or in the form of its IP address. Be aware that when you use IPv6 you need to put square brackets around the IP address, for example, **[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611**.

3. Click **Login** at the bottom of the window.

Logging on to the console from outside the company network

If you need to connect to Client Management via the Internet and you have installed your console separately from your master, you must provide the public IP address of the master to be able to connect.

1. Enter the user name **admin** and no password.
2. Replace the prepopulated localhost entry with the public IP address of the master server you want to connect to and its port number separated by a colon (:) in the **Server:Port** box.

   > You can enter the host name either as its short or full network name such as **scotty** or **scotty.enterprise.com**, or in the form of its IP address. Be aware that when you use IPv6, you need to put square brackets around the IP address, for example, **[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611**.

3. Click **Login** at the bottom of the window.

Preparing console for agent rollout

Before you can execute any operations in the console such as rolling out the agents across your network, you must provide the license for your system. You can download this license from the BMC website. If you are unable to download the license, contact BMC to provide you with one. However, a basic temporary license will automatically be installed with the software to enable you to launch it. This license is limited to 20 managed devices and 15 days. It is erased and replaced as soon as you import your full license.

The license file contains all the necessary information about the purchased product options. After it is installed, you can access all of these. Licenses are imported via their files and cannot be added manually. If you have a license that excludes some features of the product, you can acquire an additional license for these features at any time. If your license is expired, only the **Licenses** node will be shown in the console so you can import a new one.

- License considerations for a super master architecture

License considerations for a super master architecture

As with the regular architecture, you must first import the licenses delivered with your software into all your masters, including the super master. Be careful to use the correct license for each master device, because the contents reflected in the license key are different for each license:

Super Master

- The global maximum number of all devices (for example, a site has one 50-device-license a second one for 30 devices, then the super master has a license for 81 agents)
- The global maximum number of all scans (for example, a site has one 50-scan-license a second one for 30 scans, then the super master has a license for 80 inventory scans)
- The global maximum number of all patched devices (for example, a site has one 50-device-license a second one for 30 devices, then the super master has a license for 80 patch inventories)
- The Super Master license.

Site Masters

- The total number of devices the respective site manages (for example, for 50 agents)
- The licenses for all purchased functionalities, such as software distribution, patch management, power management, and so on

Changing the console display language

The console is available in seven different languages: American English, British English, Brazilian Portuguese, French, German, Japanese and Spanish. The language chosen by default is the language of your operating system. If that language is not supported, the display language defaults to American English. If you prefer to work in some other language you can change it as follows:

1. Select **Tools > User Preferences** or click the **Your Preferences** link in the **Welcome** part. The **Preferences** window appears on the screen.
2. In the **General** tab select the language from the **Language** list.
3. Click **OK** to confirm and to close the window.

The console refreshes and displays in the selected language.

Rolling out your first agent

Most management features in Client Management (patch management, remote control, software distribution, and so on) require that agents are installed on the target computers.

The agent rollout wizard facilitates installation of the CM agent within your environment. The two main components of this process are:

- The **Rollout Server**, a device that generates self-extracting agent installation packages and can push them on the target devices.
- **Rollouts** which include agent installation files, target devices and rollout options.

A typical Client Management architecture has a smaller number of relays directly under the master and a larger number of clients under each relay. This first section therefore teaches you how to perform the two main types of rollout:

1. Rolling out relay agents (with the master server as their direct parent) and
2. Rolling out final clients (with one of the previously installed relays as their parent).

The following topics are provided:

Before you begin

Before starting a rollout ensure that the following prerequisites are fulfilled:

- Remote shares are accessible from the rollout server (for example, *//ClientComputer1/C$*).
- The RPC service is started.
- No NAT-configurations are used.
- The remote services are accessible.
- For Linux installations ensure that the SSH service is installed and running on the targets.
- For Linux installations the root account must be enabled on the targets raiz.
- For Mac OS installations ensure that SSH and the root account are enabled on the targets.

Creating a rollout server

A Rollout Server is an CM agent used to deploy other agents. To define a device as Rollout Server, proceed as follows:

Remember

- To remotely deploy agents to Windows targets the Rollout Server *must* also have a Windows operating system.
- Any Rollout Server can remotely deploy CM agents to other operating systems (such as Linux/MacOS).

Note

If you have a very heterogeneous or distributed environment you might want to define specific Rollout Servers for subnets or the different operating system platforms.

To define other Rollout Servers, proceed as follows:

1. Click **Add Rollout Server** .
2. Select the new device which is to be *Your Rollout Server* from the list.
3. Click **OK** to add it and close the window.

Rolling out the relay agents

Before you begin

This rollout uses device groups. If you have not yet created a device group, do so now. It is also possible to find your rollout targets via other lists, such as the Microsoft Network option or autodiscovered devices.

1. To create a relay agent rollout with the master as its direct parent (only applicable if the master was installed with the default values), launch the rollout creation wizard by selecting **Wizards > Agent Rollout** .
   The **Core Setup Configuration** window appears.
2. Check the box for **Enable agent as a relay for the other agents**.

   If you want to schedule the rollout at a specific date and time check the box for second-to-last question.

3. Click **Next**.
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, *Linux Relay Agents*) into the **Name** box.
5. Enter the name for the rollout package executable in the **Auto-extractable Name** box (for example, *linuxrelayagent12.sh* or *linuxrelayagent10* for a Linux rollout, or *win7relayagent12.exe* for a Windows 7 installation).
6. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** box, for example, *Linux.*
7. Click **Next**.
   The **Targets & Accounts** window appears.
8. Click **Select a device** .
9. Select the desired group that contains the relay rollout targets of the defined operating system type in the **Available Objects** box.
10. To select individual devices instead of a group, click **All** on the left bar and select your devices from the list that appears.
11. Click **OK** to add the group and close the window.

12. Click **Add Administrator** .
13. Enter the required data for the account login into the respective boxes.
14. To add a new account, click **Add Administrator** .
    The Properties dialog box appears on the screen.
15. Enter the following data for a new account login into the respective boxes:
    a. Enter the name of the domain to which the rollout is going into the **Administrator Domain** box. If the rollout is going to all domains, you can use an asterisk (*).
    b. Enter the login name of the admin (for when the agent deployment tries to log on to the remote target to install the agent) into the **Administrator Login** box.

    > - For Windows XP Professional rollouts, you must enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) and targets.
    > - If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already be set up between the different domain controllers

    c. Enter the password of the previously entered admin in the **Password** box.

    > For security reasons the passwords is only displayed in the form of asterisks (*).

    d. Confirm the previously entered password into this text box.
    e. Click **OK** to confirm the new account and add it.
    The new account is now shown in the preceding list.
16. Click **Verify Rollout** at the bottom of the dialog box to ensure that the credentials are correct.
17. Click **Finish**.
18. In the Confirmation dialog box, select the **Go to Rollout** to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
19. If you did not check the **Go to Rollout** box at the end of the wizard, select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

> In the Assigned Schedule tab, you can follow the general progress of the relay rollout assignment.

20. After this value reads `Executing`, select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial`, and final status should be `Installed`).

To continue installing your architecture with clients below the relays continue with the next task.

> **Important**
>
> When you are rolling out agents on MAC OS X devices and you want to remotely control these devices, you must reboot them after the installation.

Rolling out the client agents

Before you continue with the following procedure, ensure that you have at least one relay installed.

1. Select **Wizards > Agent Rollout** .
   The **Core Setup Configuration** window appears.
2. If you want to select a specific relay for the rollout targets, select the **Configure the relay selection or use master otherwise** check box.
3. If you want to schedule the rollout at a specific date and time, select the **Configure a custom schedule for this rollout (default is one immediate execution)** check box.
4. Click **Next**.
   The **General Parameters** dialog box appears on the screen.
5. Enter the name of the new rollout, for example, *Windows 32 Bit Clients* into the **Name** box.
6. Enter the name for the rollout package executable in the **Auto-extractable Name** box, for example, *win32clientagent12.exe* for a Windows 32-bit client rollout.
7. From the list of the **Operating System** list, select the operating system group to which the agent is to be rolled out, for example, *Windows XP/2003 ... (32 bit).*
8. Click **Next.**
   If you checked the option **Configure the relay selection or use master otherwise** in the first window, the **Communication** window appears. If not, continue with step 13.
9. To find the relay, click **Select a device** next to the **Parent Name** box.
10. Click **All** .
11. Select the desired parent device from the list that appears and click **OK.**
12. Click **Next**.
    The **Targets & Accounts** window appears.
13. Click **Select a device** .
14. From the **Available Objects** box, select the desired group that contains the client rollout targets of the defined operating system type.
15. *(Optional)* To select individual devices instead of a group, click **All** on the left bar and select your devices from the list that appears.
16. Click **OK** to add the group and close the window.

17. Click **Add Administrator** .
18. Enter the required data for the account login into the respective boxes.
19. To add a new account, click **Add Administrator** .
    The Properties dialog box appears on the screen.
20. Enter the following data for a new account login into the respective boxes:
    a. Enter the name of the domain to which the rollout is going into the **Administrator Domain** box. If the rollout is going to all domains, you can use an asterisk (*).
    b. Enter the login name of the administrator whose account the rollout uses to log on to the remote target to install the agent into the **Login** box.

    > - For Windows XP Professional rollouts, you must enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) and targets.
    > - If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already be set up between the different domain controllers.

    c. Enter the password of the previously entered admin into the **Password** box. For security reasons the passwords are only displayed in the form of asterisks (*).
    d. Confirm the previously entered the password in the next text box.
    e. Click **OK** to confirm the new account and add it.
    It is now shown in the preceding list.
21. Click **Verify Rollout** to ensure that the entered account data is correct.
22. Click **OK** and then **Finish**.
    The Confirmation dialog box appears.
23. Select the **Go to Rollout** to change the focus of the console window to the new rollout.
24. Click **Yes** to confirm the immediate activation.
25. If you did not check the **Go to Rollout** box at the end of the wizard, select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

    > In the Assigned Schedule tab you can follow the general progress of the client rollout assignment.

26. After this value displays `Executing`, select the Targets tab to follow the progress of each individual target through the Status column (initial status is `Initial` and final stage should be `Installed`).

Your first client rollout is now completed and your installed base is large enough to execute any other operation. To install all remaining clients in your network, repeat this procedure for all other target device groups.

Important

When you are rolling out agents on MAC OS X devices and you want to remotely control these devices you must reboot them after the installation.

Downloading and installing a rollout from a server

This page makes all rollout packages on the server available for download by clients that cannot be accessed directly by the rollout. To download and install, proceed as follows:

1. To download a package, right-click its name and save it on the local client, or launch it directly for installation by double-clicking.
2. Before the actual download or installation process starts, provide the password for the download a second time.

Scheduling a rollout

The **Assigned Schedule** tab displays the execution schedule defined for the selected rollout. It allows you to modify this schedule an/or to reassign the rollout to its targets.

Generating the rollout package

If the rollout is to be available on the Rollout Server page of the HTML agent interface for 'pulling' the rollout to the device and then installing it (formerly *Pull Rollout*), a specific self-extracting installation package must be generated.

1. Select **Edit > Generate Rollout Package** .
   The package is immediately generated and made available on the Rollout Server and its browser page.

Starting a rollout after all configurations

After all the configuration of a rollout is defined and it is assigned to its targets and its schedule specified, it can be launched:

1. Select **Edit > Start Rollout** .

The rollout is launched immediately ignoring any schedule that can be defined for it.

Scheduling the rollout at a given time and date

In the **Core Setup Configuration** window, ensure that the **Configure a custom schedule for this rollout (default is one immediate execution)** box is selected. Then, after the **Targets & Accounts** window, the **Schedule** window appears.

1. Select the **Validity** tab.
2. Define in the **Execution Date** box at what moment the rollout is to be launched for the first time (for example, at the next device startup).
3. Define in the **Termination** box when the rollout is to be run for the last time (for example, stop after 5 executions).
4. Select the **Frequency** tab.

> Here you can define the exact day, time or frequency at which the rollout is to be launched on the target. To run the rollout more than once makes sense only if you expect that some rollout executions might not succeed at the first try.

5. Click **Finish** .

The rollout is now defined and scheduled to be executed at the specified time.

Alternative rollout methods

This section describes alternative ways to roll out the Client Management agent to the target population, such as via the Microsoft Network Neighborhood or to a specific IP address range.

- Rolling out client agents via the network neighborhood
- Rolling out client agents to specific IP address ranges
  - Running an autodiscovery on an IP address range
  - Rolling out client agents to specific IP address ranges

Rolling out client agents via the network neighborhood

This procedure rolls out client agents to Windows 7 devices using the Windows network neighborhood.

1. Select **Wizards > Agent Rollout**
   The **Core Setup Configuration** window appears.
2. Check the **Configure the relay selection or use master otherwise** box.

> If you want to schedule the rollout at a specific date and time check the box for second last question.

3. Click **Next**.
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** box.
5. Enter the name for the rollout package executable in the **Auto-extractable Name** box (for example, *win7clientagent12.exe*).
6. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** box (for example, *Windows XP/2003... (64 bit*).
7. Click **Next**.
   The **Communication** window appears.
8. To find the relay click **Import Devices from CSV File** next to the **Parent Name** box.
9. Click **All** .
10. Select the desired parent device from the list and click **OK**.
11. Click **Next**.
    The **Targets & Accounts** window appears.
12. Click **Add Device from List** .
    The **Select Devices from the List** window appears. It provides you with the different methods to select the rollout targets.
13. Select the **Network** tab in the left window bar.
    The box **Available Devices** displays now the Microsoft Windows Network Neighborhood structure on the screen.
14. Open the tree structure under which the target devices are located.
15. Select the devices to be added to the list by highlighting and moving them to the **Selected Devices** list to the right via **Add** .

    - You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you have already installed the master and probably at least one relay.
    - You cannot add the master as a target device.

16. Click **OK** to add the selected devices and close the window.
17. Click **Add Administrator**
18. Enter the required data for the account login into the respective boxes.
19. Click **Verify Rollout** to ensure that the entered account data is correct.
20. Click **OK** and then **Finish**.
21. In the Confirmation dialog box, select the **Go to Rollout** to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
22. If you did not check the **Go to Rollout** box at the end of the wizard, select the newly created rollout in the left tree hierarchy and then its **Servers** subnode. In the **Assigned Schedule** tab, you can follow the general progress of the client rollout assignment.

23. After this value reads `Executing`, select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now rolled out the CM agent to specific devices of your infrastructure that were provided by the Microsoft Network Neighborhood.

Rolling out client agents to specific IP address ranges

To roll the agent out to specific IP address ranges instead of selecting the devices from the network neighborhood, an autodiscovery must be executed before starting the actual rollout procedure.

Running an autodiscovery on an IP address range

1. In the left window pane of the console select the device which is to execute the autodiscovery of the network; this should be the relay under which the clients are to be located.
2. Select the **Agent Configuration > Module Configuration > AutoDiscovery** node.
3. Select **Edit > Properties** .
   The Properties dialog box appears on the screen, displaying the module's parameters.
4. Enter the indicated values for the following parameters and leave all others as they are:

Option	Description
TImeout (sec)	2
Address Range	The IP address range to scan
Address Verification Interval (sec)	2
Use Network Neighborhood	Yes

5. Click **OK** to confirm the new parameters and to close the window.
   The autodiscovery is launched immediately. You can follow its progress by going to the **Device List** tab.
6. To see the list populated with devices found by the relay, click **Refresh** from time to time.

Rolling out client agents to specific IP address ranges

1. Select **Wizards > Agent Rollout** menu item.
   The **Core Setup Configuration** window appears.
2. Check the **Configure the relay selection or use master otherwise** box.

> If you want to schedule the rollout at a specific date and time check the **Configure a custom schedule for this rollout (default is one immediate execution)** box.

3. Click **Next**.
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** box.
5. Enter the name for the rollout package executable in the **Auto-extractable** Name box (for example, *win7clientagent12.exe*).
6. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** box (for example, *Windows XP/2003... (64 bit)*.
7. Click **Next.**
   The **Communication** window appears.
8. To find the relay click **Add Device from List** next to the **Parent Name** box.
9. Click **All** .
10. Select the desired parent device from the list that appears and click **OK**.
11. Click **Next**.
    The **Targets & Accounts** window appears.
12. When selecting the rollout targets from the autodiscovery you have two possibilities to do so:
    a. You can select the targets from a general list displaying all autodiscovered devices.

> The tab is the preselected tab when the window is opened. It displays the list of all devices found by all devices executing autodiscoveries in the network.

    i. Select the device/devices to be added to the list by highlighting the different devices and moving them to the **Selected Devices** list to the right via **Add** .

> **Remember**
>
> You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.

> **Attention**
>
> You cannot add the master as a target device.

    ii. Click **OK** to add the selected devices and close the window.
    b. You can select the targets from the autodiscovered list of a specific device.

i. Select the **AutoDisc Device** tab in the left window bar.
The **Select a Device** window appears.
ii. Click **All** and then select the device that carried out the autodiscovery, (that is, the parent relay in this example).
The **Available Devices** box now displays the list of all devices found.
iii. Select the device/devices to be added to the list by highlighting the different devices and moving them to the **Selected Devices** list to the right via **Add** .

> **Remember**
>
> You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.

> **Attention**
>
> You cannot add the master as a target device.

iv. Click **OK** to add the selected devices and close the window.

13. Click **Add Administrator** .
14. Enter the required data for the account login into the respective boxes.
15. Click **Verify Rollout** to ensure that the entered account data is correct.
16. Click **OK** and then **Finish**.
17. In the Confirmation dialog box, select the **Go to Rollout** to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
18. If you did not check the **Go to Rollout** box at the end of the wizard, select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.
In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.
19. After this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now rolled out the CM agent to a specific subnet of your infrastructure.

Uninstalling the client agent via rollout

Agents that were installed via a rollout can also be uninstalled by rollout. The procedure is similar to the installation. The wizard created for this uninstallation uses the Master as the Rollout Server and the default schedule.

Creating the uninstall rollout

1. Select **Wizards > Agent Rollout** .
   The **Core Setup Configuration** window appears.
2. Select the **Uninstall** option from the **Select the action to perform for this rollout** list.
3. Click **Next** .
   The **General Parameters** are displayed on the screen.
4. Define the following parameters for your new rollout all others leave with their predefined values:
   - Enter the name for the rollout configuration, for example, *Vista 32-bit Uninstall* in the **Name** box.
   - *(Optinal)* If the uninstallation is to be also available for download on the Rollout Server agent interface, enter the name for the auto-extractable file in the **Auto-extractable Name** box, for example, **FPAC_Vista32BitUninstall.exe** .
   - *(Optinal)* If the installation is to be executed silently, that is, without any user input on the target, on Windows devices check the **Silent mode Installation** box.
   - In the **Operating System** text box select the appropriate operating system group.
   - *(Optinal)* If the agent was *not* installed in the default directory enter its installation directory in the **Installation Directory** box.
   - *(Optinal)* If the agent was *not* installed with its default service name enter its name in the **Agent Service Name** box.
5. Click **Next** .
   The **Communication** window appears. In this window the devices on which the agent is to be uninstalled must be selected and the administrator accounts to access them. To select the target devices there are several methods available. Since all targets have an agent installed the easiest method is to select them from the device list.
6. For this select **Select a device** above the **Parent Name** text box.
   The **Select a Device** window opens on the screen.
7. Select the devices to be uninstalled from one of the tabs of the **Select a Device** dialog box.
8. Click **OK** to confirm and close the window.
   The devices are now added to the list window.
9. Click **Add Administrator** .
10. Enter the required data for the account login into the respective boxes.
11. To add a new account, click **Add Administrator** .
    The **Properties** dialog box appears on the screen.
12. Enter the following data for a new account login into the respective boxes:

a. Enter the name of the domain to which the rollout is going into the **Administrator Domain** text box. If the rollout is going to all domains, you can use an asterisk (*).
b. Enter the login name of the admin as which the agent deployment tries to log on to the remote target to install the agent into the **Login** text box.

> ⚠ If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already were set up between the different domain controllers.

c. Enter the password of the previously entered admin into the **Password** text box. For security reasons the passwords is only displayed in the form of asterisks (*).
d. Confirm the previously entered the password into this text box.
e. Click **OK** to confirm the new account and add it.
It is now shown in the preceding list.

13. Click **Verify Rollout** to ensure that the entered account data is correct.
14. Click **OK** and then **Finish** .
15. In the **Confirmation** dialog box, select the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
16. If you did not check the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.
In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.
17. After this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now uninstalled the CM agent from all the defined target computers.

> ⚠ **Note:**
>
> Devices that cannot be accessed directly by the rollout because they are in another domain or behind a firewall or for any number of other reasons must download the uninstall package from the Rollout Server page of the server's agent browser interface and execute it. To access the server enter http://<rollout server name> :<rollout server port> /rollout into the browser.

Managing targets of a rollout

The **Targets** tab provides access to all devices which are defined as rollout targets. This list can be filtered according to the device rollout status.

The following topics are provided:

- Filtering rollout targets
- Defining login accounts

Filtering rollout targets

To display only a reduced number of target devices assigned to this rollout, you can filter these via their different status values. To do so, proceed as follows:

1. Click the **View** list above the table.

   This list provides you with the following status values according to which you can sort the assigned devices:

Status	Description
All Status	to display the assigned devices of all different types of status
Initial	the rollout was not yet launched
Successful	the rollout was successfully terminated on the device
Failed	the rollout failed to execute successfully on the device
Processing	the rollout is still being executed

2. Select the desired status value.

The table updates its contents and displays only those devices, which status value corresponds to the one you selected.

Adding a device from the list of autodiscovered devices

Devices can be added to the list of rollout targets through a number of different ways. One is through different types of lists.

Note:

Be aware that you cannot add the master as a target device.

One of these lists is the list of autodiscovered devices:

The AutoDiscovery module provides a list of all devices of any type found in the network, such as printers or devices with and without the agent installed. This list is also available for the rollout functionality to facilitate the selection of the rollout targets. However, the list displayed in this case only shows all clients of type device and only those with a status of `Verified` or `Learned` , which means that all devices in this list were verified for existence either by the local client or a neighbor client and exist on the network. To add a device from the list of all autodiscovered devices known to the database, proceed as follows:

1. Select **Edit > Import Devices from CSV File** .
   The **Select Devices from the List** window opens which provides you with its different methods, with the **AutoDisc Object** tab preselected in the left window bar. On the top of the **Available Devices** box there are two drop-down lists which provide you the possibility to filter the autodiscovered objects thus reducing the list to your needs. The following filters are available:

- You can filter for the type of the autodiscovered object, that is, if all found devices are to be shown, or only PCs, printers, switches, and so on, and you can limit the list to either devices with or without the CM agent already installed.
- The box **Available Devices** displays the list of all available devices.
- Below, the **Use IP Address** option allows you to select the device by IP address. By default this option is not activated, meaning that the device is selected by its name.

1. Select the device/devices to be added as targets from the list
2. Click **Add** to move the selected devices to the list of **Selected Devices** .
3. Click **OK** to confirm the selections and close the window.

The selected devices are now added to the list of targets with the initial status `Initial` .

Adding a device from the list of devices discovered by another device

Devices can be added to the list of rollout targets through a number of different ways. One is through different types of lists.

> **Note:**
>
> Be aware that you cannot add the master as a target device.

One of these lists is the list devices discovered by another device:

The tab **AutoDisc Device** allows you to select your target devices from a list of autodiscovered devices by one specific network device.

1. Select the **Edit > Import Devices from CSV File** icon.

2. Select the **AutoDisc Device** tab in the left window bar.
   The **Select a Device** window opens on the screen.
3. Select the device of which the autodiscovered list is to be used from one of the tabs of the **Select a Device** dialog box.

The list of groups and devices provided in this window includes groups and members of synchronized directory servers.

1. Click **OK** to confirm the selections and close the window.
   The box **Available Devices** displays now the list of all devices which were discovered by the selected network device.
2. Select the device/devices to be added as targets from this list
3. Click **Add** to move the selected devices to the list of **Selected Devices** .
4. Click **OK** to confirm the selections and close the window.

The selected devices are now added to the list of targets with the initial status `Initial` .

Adding a device from the Microsoft network neighborhood

Devices can be added to the list of rollout targets through a number of different ways. One is through different types of lists.

> **Note:**
>
> You cannot add the master as a target device.

One of these lists is the Microsoft Network Neighborhood:

1. Select **Edit > Import Devices from CSV File** .
2. Select the **Network** tab in the left window bar.
   The box **Available Devices** displays now the **Microsoft Windows Network Neighborhood** structure on the screen
3. Select the device/devices to be added to the list from one of its groups.
4. Click **OK** to confirm the selections and close the window.

The selected devices arel now added to the list of targets with the initial status *Initial* .

Adding a device from a CSV list

Devices can be added to the list of rollout targets through a number of different ways. One is through different types of lists.

> **Note:**
>
> Be aware that you cannot add the master as a target device.

One of these lists is a CSV list that contains the respective devices.

1. Select **Edit > Import Devices from CSV File** .
2. Select the **CSV List** tab in the left window bar.
   A window opens, in which you can select the file containing the device list.
3. Click **Open** at the bottom of the window to open the list.
   The box **Available Devices** displays now the list of all devices contained in the selected CSV list.
4. Check the **Header** box, if your CSV file has a title line which is to be removed.
5. Select the device to be added to the rollout from the list in the window.

You can also select all devices in the list by using **Select All** .

1. Click **OK** to confirm the selections and close the window.

The selected devices arel now added to the list of targets with the initial status Initial.

Manually adding targets

You can also add a device by directly entering its name. To do so, proceed as follows:

> **Note:**
>
> Be aware that you cannot add the master as a target device.

1. Select **Edit > Add Device** .
   The **Select a Device** window opens on the screen.
2. Select the device to be added from one of the tabs of the **Select a Device** dialog box.

   > The list of groups and devices provided in this window includes groups and members of synchronized directory servers.

3. Click **OK** to confirm the addition and close the window.

Adding an existing device

You can also add one or more devices by typing their name or address. To do so, proceed as follows:

> **Note:**
>
> You cannot add the master as a target device.

1. Select **Edit** *> *  .
   The **Add a Device** dialog box appears.
2. Enter the name of the device to be added to the list in the respective text box. The name can be entered:
   - Either as its short or long network name, for example, `scotty` or `scotty.enterprise.com` or as its IP address, for example, `159.124.5.10` ,
   - Or as a comma separated list of names or ranges, for example, `scotty; 192.168.4.45-192.168.4.47` which includes computers `scotty.enterprise.com` , `192.168.4.45, 192.168.4.46` and `192.168.4.47` .
   - A range can also be entered as CIDR notation in the form of `192.9.205.22/18` .
3. Click **OK** to add the device and close the window.

Verifiying the rollout

The **Verify Rollout** action verifies the validity of `domain/username/password` on the rollout server and on the target devices before launching a rollout. If no targets were defined yet, the server account is only verified. If one or more devices are specifically selected in the table only those are verified. To verify the rollout, proceed as follows:

1. If specific devices are to be verified, select these in the table in the right window pane, or do not make any selection to verify all targets.
2. Select **Edit > Verify Rollout**  .

A message box appears with the result of the verification for each device.

Displaying the rollout log file

Logging of rollout is not included in the general logging in the mtxagent.log file, it is written in its own specific log file, the mtxsetup.log, which is located in the Installation Directory/master/data /rollout directory. It is possible to directly access the log file of a specific client assigned to the currently selected rollout. Be aware, that this option is only available for devices with an established connection, it is never available for unconnected, retired or unknown devices. To do so, proceed as follows:

1. Select the target device in the right window pane.
2. Select **Edit > Display Log**  .
   A new window appears, displaying the contents of the log file of the rollout on the selected client. The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as ERR for error or T for trace, and so on and the description itself.
3. Click **Close** to close the window.

Reassigning a rollout

If targets failed to install during a rollout, they can be reassigned and thus re-executed.

1. Select the devices to which the rollout is to be reassigned. If the rollout is to be reassigned to all targets shown in the table to the right, do not select any device.
2. Select **Edit > Reassign Rollout** .
   A confirmation window appears.
3. Click **Yes** to confirm the reassignment and launch it according to its schedule.

Generating the rollout package for a target

If the rollout is to be available on the Rollout Server for "pulling" the rollout to the device and then installing it (formerly Pull Rollout), a specific package must be generated

1. Select **Edit Generate Rollout Package** .

The package is immediately generated and made available on the Rollout Server.

Defining login accounts

Specific login accounts can be defined to be used for the rollouts. These logons then try to log on to the device to execute the rollout in the order in which they are defined. The logons are tried in the order they are defined in the table, and once a login is successful all further accounts are ignored

Adding an account to the rollout deployment

To add an account to the rollout deployment, proceed as follows:

1. In the **User Accounts** tab select **Edit > Add Account** .
   The **Properties** dialog appears.
2. Enter the required data for the new account login.
3. Click **OK** to confirm the new account and to close the window.

Automatically rolling out agent using a wizard

The definition and execution of the different rollouts to be executed in the network can be done manually by creating the rollout and then defining all options, or they can be created via the **Agent Rollout** wizard. This wizard creates a new rollout from scratch with all the required settings and sends it to the list of targets. The pre-entered values are those defined during the installation of the master.

The wizard is available directly on the main **Wizards** menu from anywhere in the console, or it can be called from specific locations in the console.

1. Select the **Wizards> Agent Rollout** menu item from the menu bar.
2. The first wizard window appears.

The following topics are provided:

- The Agent Rollout wizard 1 - Specifying core setup configuration

The Agent Rollout wizard 1 - Specifying core setup configuration

The first step allows you to specify which aspects of an agent rollout require specific configuration and for which the default values can be used.

1. For the first question select the type of rollout to be executed from the list. Depending on your choice a number of the following questions might be dimmed.
2. Answer the following questions by checking or leaving the check box unselected. Checking the box adds the respective step to the wizard in which you need to provide information.
3. If you selected to create a task for this operation, the **Create Task** box displays and, if tasks of type **Agent Rollout** exist, you can also select to add this rollout to one of the existing tasks by checking the **Use Existing Task** box and selecting it from the list.
4. After you have answered all questions click **Next** to start the rollout configuration.

The Agent Rollout wizard 2 - Defining general parameters before rolling out the agent

This window is one of the two mandatory wizard steps that are always part of the rollout configuration, because it defines is basic parameters. The following parameters must be defined for a rollout to work:

1. Enter a name into the respective text box.
2. If the rollout is to be made available on the browser interface page of the **Rollout Server** , enter a name for the auto-extractable file.

This can be necessary if the rollout is assigned to devices that cannot be accessed directly by the rollout. This can be the case, if they are in another domain or behind a firewall or for any number of other reasons. For these cases the install package must be downloaded from the Rollout Server page of the server's agent browser interface and executed locally.

1. Select the operating system for which the rollout is to be created.
2. *(Optional)* If another than the default directory is to be used, define the installation directory.

3. *(Optional)* If another than the default name is to be used, define the agent service name and define its startup type.
4. Click **Next** to go to the following wizard page.

The Agent Rollout wizard 3 - Communication settings

This window defines the communication settings between the agent to be installed and its parent, such as the parent name and port, the port for interagent communication, connection timeout values. and tunnel definitions. The predefined values in this window are the parameter values defined for the master; therefore, if the agents to be rolled out have the master as their parent, no changes are required here.

For any other cases, you have the following options to define the relay:

- The Agent Rollout wizard (3)- Defining a static relay
- The Agent Rollout wizard (3)- Defining an automatic relay selection
- The Agent Rollout wizard (3)- Defining communication specific parameters

The Agent Rollout wizard (3)- Defining a static relay

To define a static relay for the agent targets:

1. Enter the range of ports on which the HTTP server will listen for and send data from into the **Port** box.
2. Enter the number of the port the console uses for its communication into the **Console Port** box.
3. Enter the name of the direct parent directly into the **Parent Name** box or select it from the list of available devices. The displayed list is pre-filtered to show only those devices for which the *Relay* option is activated. If no value is entered, the master is used by default.
4. Enter the number of the port on which the new agent connects to its parent into the **Parent Port** box.
5. Click **Next** to continue.

The Agent Rollout wizard (3)- Defining an automatic relay selection

Automatic relay selection allows the clients to try to find their relay using one ore more specifically selected methods in the order that they are defined. If one method cannot find a relay it returns and the next method in the list is tried.

1. Select the **Auto-Select Relay** radio button.
2. In the **Available Relay Selection Methods** box select the first method to be used to find the relay.
3. Click **Add** .
4. Enter the required parameter values in the **Properties** window.
5. The method moves to the **Selected Methods** box to the right.
6. Repeat these steps for all methods that are to be used for finding a relay.

7. If you want to make changes to the order, select the method to move in the **Selected Methods** box and click **Move Up** or **Move Down** above the box until the method is at the desired place.
8. Click **Next** .

The Agent Rollout wizard (3)- Defining communication specific parameters

If you require specific settings for the agent communication with the relays, you can define these:

1. Select the **Advanced** tab.
2. Make the required changes in the available parameters.
3. Click **Next** .

The Agent Rollout wizard 4 - Defining security parameters before rolling out the agent

The parameters in this window define the settings on how the communication between the agents is secured. The prepopulated default values are those defined for the master. To use those no modifications are required. Otherwise make the necessary changes to the boxes of the window.

> **Note:**
>
> If you are using secured communication with mutual authentication, don't forget to define the certificates and authorities, otherwise the agents cannot communicate.

Click **Next** to continue.

The Agent Rollout wizard 5 - Defining user interface and reboot management

The parameters defined in this window concern the user interface, that is, the information, if any, displayed in the systray and the way rebooting the device is managed by the CM agent . The default settings are:

- **User interface**
  The CM agent icon displays in the systray dynamically with all its different possible status and colour changes.
- **Reboot Management**
  A message box appears on target device for a reboot request and the reboot waits for a maximum of 5 minutes before executing.

Make any changes as required and then click **Next** to continue.

The Agent Rollout wizard 6 - Defining logging parameters before rolling out the agent

The logging parameters define the basic settings for the main agent log file (that is, the values specify the granularity of the contents of the main agent log file, and their output location, the amount of information to keep, and the displayed types, for example.)

Make any changes as required and then click **Next** to continue.

The Agent Rollout wizard 7 - Available modules for target devices

This window provides the list of all available modules that might be installed on the target device and loaded at startup for the selected operating systems according to your licenses. The default modules are pre-checked. Modules which are required for the basic functioning of the agent are listed with the mandatory icon ( ) and cannot be unloaded.

1. To load or unload a module for the target device select it in the table.
2. Then either select the **Edit> Load Modules** or **Edit> Unload Modules** / icon.The icon of the selected modules is automatically changed to indicate its modified loading status via the **Yes**/**No** icon (/).

The Agent Rollout wizard 7 - Configuring modules for target devices

It is also possible to directly configure a number of the modules from here. Be aware that not all modules may be preconfigured by the rollout; modules such as OsDeployment may only be configured directly on the device. If a module is specifically configured, the **Customized** icon displays in the respective column. The relay module is always shown as configured, because it was automatically adapted with the parent information.To configure a module proceed as follows:

1. Select the respective module in the table.
2. Then either select the **Edit > Properties** icon.
   The **Properties** window appears. It displays all module parameters which are configurable.
3. Make the necessary modifications
4. Click **OK** at the bottom of the window to confirm the modifications or click **Cancel** to abandon without modifications and to close the window
5. Click **Next** to continue.

The Agent Rollout wizard 8 - Defining the rollout server for the rollout

This window defines the Rollout Server to use for this rollout. By default the Master is defined as Rollout Server. You can either use another already existing server by selecting it in the table or add another one in this step.

1. Click the **Add Device** icon on top of the table.
   The **Add a new rollout server** pop-up window displays displaying the list of all devices, that can be a server due to their operating system.
2. Select the device to be added from one of the list boxes.

3. Click **OK** to confirm and close the window.
4. The device is added to the table of available servers and selected.
5. Click **Next** to continue.

The Agent Rollout wizard 9 - Rollout targets and rollout accounts

This window is the second obligatory step of the rollout wizard, because it defines the target devices and the credentials to access them.

The following topics are provided:

- Defining rollout targets
- Defining rollout accounts

Defining rollout targets

In the first part of the window the rollout targets are defined. You cannot add the master as a target device. Devices can be added to the list of rollout targets through a number of different ways:

After all devices are added click **Next** to continue.

Defining rollout accounts

Specific login accounts can be defined to be used for the rollouts. These logons then try to log on to the device to execute the rollout in the order in which they are defined. The logons are tried in the order they are defined in the table, and once a login is successful all further accounts are ignored.

1. Click **Add Administrator** .
2. Enter the required data for the account login into the respective boxes.
   The access to the devices must be defined in the same way as for the installation before you can schedule the rollout.
3. To add a new account, click **Add Administrator** .
   The **Properties** dialog box appears on the screen.
4. Enter the following data for a new account login into the respective boxes:
   a. Enter the name of the domain to which the rollout is going into the **Administrator Domain** box. If the rollout is going to all domains, you can use an asterisk (*) .
   b. Enter the login name of the admin as which the agent deployment tries to log on to the remote target to install the agent into the **Administrator Login** box.

> as the "simple" login name of a local user of the remote computer, such as `Administrator`
> as `.\logon` for a local logon, or
> as `domain\logon` for a domain login of the administrator, such as `LAB\TEST` . The domain part can be set to a dot (.) to indicate the local computer.

If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already were set up between the different domain controllers.

c. Enter the password of the previously entered admin into the **Password** box. For security reasons the passwords is only displayed in the form of asterisks (*).
d. Confirm the previously entered the password in this text box.
e. Click **OK** to confirm the new account and add it.
It is now shown in the preceding list.

5. Click **Verify Rollout** at the bottom to ensure that the credentials are correct.
6. Click **Finish** .
7. Click **Next** to continue with the wizard.

The Agent Rollout wizard 10 - Post-installation scripts and files

This window allows you to create a script in the BMC Software proprietary Chilli language after the installation of the agent has finished or to add files to the rollout package.

The following topics are provided:

- Creating post-installation scripts
- Adding post-installation files

Creating post-installation scripts

In this box you add and edit a script to be executed after the rollout of the agent has terminated, and add files to be installed on the remote client. This can be to fine-tune agent settings for a specific computer or to simply add some individual configuration files.

Note

The script must be in the BMC Software proprietary Chilli language and follow all its rules. You can find Information about the Chilli programming language in the Chilli manual which is delivered with the Client Management software.

1. To create a post-installation script enter it into the following box.
2. After you finish the script and click the **Next** button, the agent tries to compile the script to verify it is correct. If it is not correct, an error message appears.

Adding post-installation files

The **Files** box allows you to add files to the rollout package which are installed or added on the local client after the actual rollout procedure. The way they are to be treated is defined through the script previously defined.You may define one file to be copied to several different locations on the device by repeating the following procedure for the file and each target location:

1. Click the **Add Postinstall File** icon above the list box.
   The **Add a Postinstall File** window appears.
2. Select the required file from the file hierarchy displayed in the list window.
3. Click **OK** .
4. Enter its target path in the **Define the destination path on the client for the selected files:** pop-up menu.
5. Click **OK** to confirm the addition and to close all windows.
6. Click **Next** to continue.

The Agent Rollout wizard 11 - Scheduling the rollout

Now that the rollout and the members were defined, it must be scheduled to execute at a specific time. By default it is scheduled to execute once and immediately. If this is your choice you do not need to make any modifications in this window. To schedule the rollout for a specific moment proceed as follows:

1. Check the **Available on Rollout Server** box, if the rollout is to be made available on the Rollout server (that is, if you have target devices that cannot be reached directly by the rollout).
2. Check the **Allow 32 bit Agent Installations on 64 bit Architecture** box if
3. If the rollout targets are Windows devices select the connection mode that is to be used from the **Windows Connection Mode** list.
4. In the **Assignment Date** box select at what moment the assignment to the target devices is to be launched. The assignment in this case means that the link between the rollout and the target is established and the rollout package will be sent.
5. Select the **Validity** tab.
6. Define in the **Execution Date** box at what moment the rollout is to be launched for the first time.
7. Define in the **Termination** box defines when the rollout is to be run for the last time.
8. Select the **Frequency** tab. Here you can define the exact day, time or frequency at which the rollout is to be launched on the target. To run the rollout more than once only makes sense, if you expect that some rollout execution tentatives might not succeed at the first try due to specific reasons.
9. If you have specified to create a task , click **Next** to continue or click **Finish** to confirm all settings, create the rollout as defined and launch its execution.

The Agent Rollout wizard 12 - Creating a task for the rollout

This step of the wizard allows you to create a task for the rollout defined via this wizard or to assign it to an existing task. This option is only available, if you checked the corresponding box in the first window of the wizard.

1. Define all parameters for the task that is to follow this rollout.
2. When you made your selections click **Finish** to confirm all choices and launch the process.

The Agent Rollout wizard 13 - Confirming all definitions

A confirmation window appears on the screen. To directly move the focus of the console to the newly created rollout check **Go to Rollout** . If you have also created a task for this operation, this check box will also be available and you can select to move the focus of the console to the task by checking this box.

Click **OK** to confirm all definitions and create and start the rollout.

Managing operational rules

Managing operational rules include the following topics:

- Operational rules overview
- Getting started with operational rules
- Adding packages to operational rules
- Adding dependencies to operational rules
- Advertising an Operational Rule
- Assigning Targets to Operational Rules
- Leveraging operational rule steps
- Operational Rules Wizards
- Examples of Operational Rules

Operational rules overview

BCM introduces rules-driven administration capable of dynamically managing client systems and adapting to business change. By applying logical rules to systems management, the administrator creates dynamic scenarios that define how groups of client systems are to be managed today, and how they should automatically adapt to any changes in the future. By applying these rules to groups of end-users, BCM ensures that the users' computers are automatically provisioned with the right tools at the right time. If an end-user changes responsibilities and is assigned to a different group, the applications necessary for the new role will be provided automatically without any manual administration.

The use of intelligent agents also means that rules created within BCM persist even when a notebook is disconnected from the network, because the agent lives on the device. Moreover, centralized business rules sometimes are not optimal to all systems. The intelligent agents can automatically adapt their behavior and rules to the local system context (network conditions, CPU conditions, etc.).

Operational Rules define which and how an BCM function is to be performed. These rules are made up of a series of commands called "steps" executed by the agent. A step is a Chilli script. The behavior of BCM client agents is fully flexible and configurable. For this the administrator uses a GUI to define tasks to be performed by the client (inventory, file handling, configuration, etc.), provides parameters to these tasks, and distributes the rules.

Getting started with operational rules

This section guides you through all the steps to work efficiently with **Operational Rules**. First there is an overview of the different stages of working with **Operational Rules** to establish an understanding of the whole process. After making sure that your network is ready for **Operational Rules** , you start by creating your first **Operational Rule** . An example of **Operational Rule** is provided which displays a message box and launches the calculator.

Subsequently you learn how to make **Operational Rules** more efficient: such as adding packages or dependencies, advertising them, or configuring **Operational Rules** to adapt to your special requirements.

If you require customized actions in addition to the predefined ones, the Adding custom operational rule steps topic describes how to add your own steps to Client Management.

The Step Reference provides an explanation of all available steps listed by category.

The following topics are provided:

- What is an operational rule?
- What can I do with operational rules?
- What is the process of working with operational rules?
- Are there different types of operational rules?

What is an operational rule?

An **Operational Rule** executes one or multiple CM functions on specific devices or device groups in the defined order.

An **Operational Rule** contains:

- Steps: a series of commands executed by the CM agent
- a schedule: defining the execution of the **Operational Rule**
- assigned objects: devices on which the **Operational Rule** is to be executed

- packages (optional): software to be installed via a step
- dependencies (optional): execution of the **Operational Rule** depends on other **Operational Rules**

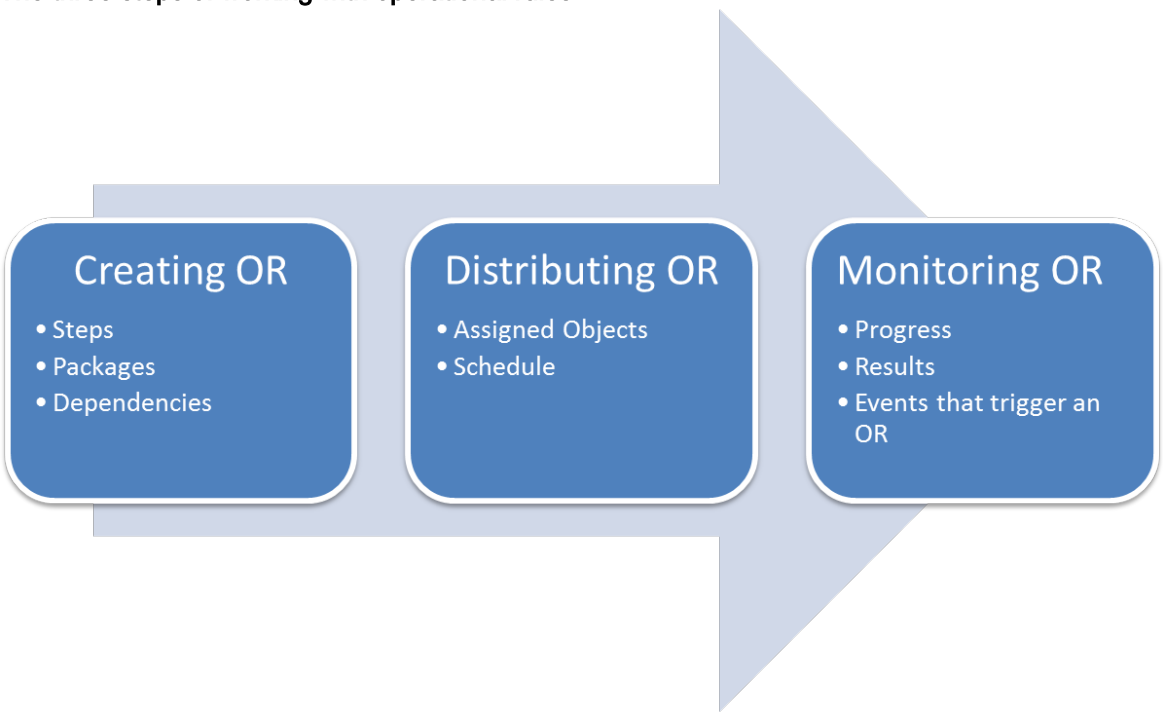
What can I do with operational rules?

With operational rules you create dynamic scenarios that define how groups of client systems are to be managed today, and how they should automatically adapt to any changes in the future.

By applying these rules to groups of end-users, CM ensures that the users' devices are automatically provisioned with the right tools at the right time.

What is the process of working with operational rules?

The three steps of working with operational rules



Working with operational rules consists of three steps:

- **Creating operational rule** : adding steps, packages, dependencies
- **Distributing operational rule** : selecting assigned objects, defining the assignment and execution schedule
- **Monitoring operational rule** : following the execution progress and results, getting noticed by events that are triggered by the **Operational Rule**

Are there different types of operational rules?

Several different types of operational rules are differentiated in the Console by an icon:

		Any operational rule performing any type of action without installing a package

	General Operational Rules	
	Software Distribution Rules	Operational rules installing any type of package with the exception of patch packages
	Patch Distribution Rules	Operational rules installing a patch package
	Quick Link Rules	This type of operational rule can only be published on **MyApps** and only contains a clickable link.

The following topics direct you through the three steps of creating your first **Operational Rule** . An example is provided on launching the calculator to s how you the process of working with **Operational Rules** . After completing the three tasks, you will be able to design even more complex **Operational Rules**.

- Creating an Operational Rule
- Distributing an Operational Rule
- Monitoring an Operational Rule

Creating an Operational Rule

In this task you create your first operational rule: First it should display a message box asking the user if he wants to launch the calculator. If he clicks **Yes** in the message box, the calculator is launched; if he clicks **No** , the operational rule is terminated.

For this operational rule you need to add two steps: one for the message box and one for launching the calculator. To create the operational rule proceed as follows:

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog box appears.
2. In the **Name** text box enter Launch Calculator and click **Next** .
3. In the **Steps** view click **Add Step** .
   The **Select a Step** dialog box appears.
4. In the **Available Steps** group box select **User Message Box > Advanced Message Box** and click **Add** .
   The **Properties** dialog box appears.
5. Fill in the following text boxes:
   - **Message Title** : Launch Calculator
   - **Message Text** : Do you want to launch the calculator?
   - **Validation Button Label** : Yes
   - **Cancel Button Label** : No
6. From the **Stop Condition** list select **The rule fails** .

> With this selection the operational rule is stopped if you click **No** and the next step, launching the calculator, is blocked.

7. Click **OK** to confirm the step.
   The dialog closes and the step is listed in the right group box.
8. In the **Available Steps** group box select **Process Management > Execute Program** and click **Add** .
   The **Properties** dialog box appears.
9. In the **Executable Path** text box enter the path to the calculator on your device .If you have a Windows operating system, the path is by default C:/Windows/System32/calc.exe.
10. Click **OK** to confirm the step.
    The dialog closes and the step is listed in the right group box under the first step.
11. Click **OK** to add the two steps to the operational rule.
12. Click **Finish** to create the new operational rule.
    The **Confirmation** dialog box appears.
13. Click **Yes** to distribute the operational rule and continue with the distribution wizard.

You just successfully created your first operational rule which includes two steps. In the next step you will distribute it to a device .

Distributing an Operational Rule

After creating the operational rule you distribute it to devices in your network. In this example you select one device , preferably the one you are currently working on, and assign and execute the operational rule immediately.

1. In the **Operational Rule Distribution Wizard** dialog select **Devices** from the **Target Type** list and click **Next** .
2. Click **Assign Device** .
   The **Assign to Device** dialog appears.
3. Click **All** , select the device to which you want to assign the operational rule and click **OK** .
   The dialog closes and the device is listed.
4. Click **Finish** to distribute the operational rule.
   The dialog closes and the **Confirmation** dialog box appears.
5. Select the **Go to Operational Rule** radio button and click **OK** .
   The dialog closes and the focus of the console is moved to the device assigned to the new operational rule.

You distributed an operational rule to a device in your network. In the next step you monitor its execution.

Monitoring an Operational Rule

After distributing the **Operational Rule** to a device , you can follow the progress of its execution. To do so, proceed as follows:

1. Make sure that **Operational Rules > Launch Calculator > Assigned Objects > Devices** is selected and follow the progress of the execution in the right window pane under the **Status** column.

> Its current status should either be `Assignment Waiting` or `Assigned` .

2. Wait until the message box appears on the target device .
   - If you want to launch the calculator, click **Yes** .
   - If you don't want to launch the calculator, click **No** .
     Depending on your choice the calculator is launched on the target screen.
3. Check the **Status** column.

If you clicked **Yes** , `Executed` appears.

If you clicked **No** , `Execution Failed` appears.

You monitored your **Operational Rule** in the Console and successfully opened a message box that launched the calculator on a device via an **Operational Rule** .

Adding packages to operational rules

In the first example you created an operational rule with two steps. Beyond that BCM offers many possibilities to create more complex and efficient **Operational Rules**.

In addition to steps, you can also add packages to an **Operational Rule**. This allows you to install software on devices. By combining the package with different steps, you can create sophisticated solutions to any problem in your network. In this case, *a simple* operational rule will become a " *Software Distribution Rule* ".

The following topics describe how to add packages to the operational rules:

- Adding Packages to a New Operational Rule
- Adding Packages to an existing Operational Rule

Adding Packages to a New Operational Rule

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog displays.
2. In the **Name** text box enter a name for the **Operational Rule** , for example, Package Installation.
3. Select the **Add Packages** check box and click **Next**.
4. If you need additional steps, add the steps via .

> When you add a package to the **Operational Rule** , the corresponding step installing the package (**Install Package**) is automatically created. Therefore you don't need to add the step manually.

5. Click **Next** .
6. Click **Add Packages**  .
7. In the **Select a Package** dialog select your **Package** and click **OK** .
   The dialog closes and the package is listed in the wizard.
8. Click **Finish** to create the new **Operational Rule** .
   The dialog closes and the **Confirmation** dialog box appears.
9. If you want to distribute the **Operational Rule** immediately, click **Yes** .
10. If you want to modify the **Install Package** step, go to **Operational Rules > Package Installation** , click the **Steps** tab and double-click **Install Package**. For example you can define conditions, add a message displayed before the installation or define a reboot after the installation.

You created an **Operational Rule** with a **Package** . Based on this **Operational Rule** you can further adapt it to your needs by adding steps, stop conditions, verification conditions, dependencies or changing the order of its elements.

Adding Packages to an existing Operational Rule

Before executing the following task, make sure that you already created a package in the console.

1. Go to **Operational Rules > Your Operational Rule** and click the **Package** tab.
2. Click **Add Package**  .
3. In the **Select a Package** dialog select your **Package** and click **OK** .
   The dialog closes and the **Package** is listed in the right window pane. The **Steps** tab displays the **Install Package** step that was also added which is responsible for installing the selected package.

You added a **Package** to an existing **Operational Rule** .

Adding dependencies to operational rules

A dependency provides one means to link different **Operational Rules** . If you add an **Operational Rule** B as dependency to an **Operational Rule** A, **Operational Rule** A will only be launched if **Operational Rule** B was successfully executed. If **Operational Rule** B failed, **Operational Rule** A cannot be launched.

A typical situation in which to use a dependency is for Microsoft Office installations: Before a patch or an upgrade for the Office software is installed the **Operational Rule** makes sure that the Office software itself was successfully installed.

There are two ways of adding dependencies: either in the **Operational Rule Creation Wizard** while creating an **Operational Rule** or adding a dependency to an existing **Operational Rule** .

The following examples also shows a common scenario. We will use the previously created operational rule installing the software package. To this we will add a verification that the target device must be of a specific operating system and if not the software will not be installed. For this we first need to create the OS verification rule.

The following topics are provided:

- Creating an operational rule for dependency
- Adding Dependencies to a new Operational Rule
- Adding Dependencies to an existing Operational Rule

Creating an operational rule for dependency

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog box appears.
2. In the **Name** text box enter *Check for Windows OS* and click **Next** .
3. In the **Steps** view click **Add Step** .
   The **Select a Step** dialog box appears.
4. In the **Available Steps** group box of the **Select a Step** dialog select **Tools > Check Operating System** and click **Add** .
   The **Properties** dialog box appears.
5. In the **Properties** dialog check all boxes that mention a Windows operating system.
6. From the **Stop Condition** list select **The rule fails** .

   With this selection the **Operational Rule** is stopped if the operating system is not any version of Windows.

7. Click **OK** to confirm the step.
8. Click **OK** to add the step to the **Operational Rule** .
9. Click **Finish** to create the new **Operational Rule** .
10. Click **No** in the **Confirmation** dialog box.

Adding Dependencies to a new Operational Rule

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog box appears.
2. In the **Name** text box enter a name for the **Operational Rule** , for example, *Software Distribution* .
3. Select the **Add Packages** and **Add Dependencies** check boxes and click **Next** .
4. Click **Add Packages** .
5. In the **Select a Package** dialog select your **Package** and click **OK** .
6. Select the **Add Dependencies** check box and click **Next** .
7. Click **Add Dependency** .

8. In the **Select an Operational Rule** dialog select the rule *Check for Windows OS* and click **OK** .
   The dialog closes and the **Operational Rule** is listed in the wizard.
9. Click **Finish** to create the new **Operational Rule** .
   The dialog closes and the **Confirmation** dialog box appears.
10. If you want to distribute the **Operational Rule** immediately, click **Yes** otherwise click **No** .

You created a new **Operational Rule** with one dependency.

Adding Dependencies to an existing Operational Rule

1. Go to **Operational Rules** > *Software Distribution* and click the **Dependencies** tab.
2. Click **Add Dependency** .
3. In the **Select an Operational Rule** dialog select the rule *Check for Windows OS* and click **OK** .
   The dialog closes and the **Operational Rule** is listed in the right window pane.

You added a dependency to an existing **Operational Rule** .

Advertising an Operational Rule

After creating an **Operational Rule** , you have two possibilities of distributing it in your network: either selecting devices and assigning it to them according to your schedule, or advertising it to devices .

By advertising an **Operational Rule** you do not force its execution; instead the **Operational Rule** is added to MyApps in the Agent Interface . The user of the device is informed that a new **Operational Rule** is available and it's the user's choice if and when to execute it.

1. Click the **Wizards > Operational Rule Distribution** menu item.
   The **Operational Rule Distribution Wizard** dialog box appears.
2. Click **Start Search** next to the **Name** text box.
3. In the **Select an Operational Rule** dialog select your **Operational Rule** , for example, **Launch Calculator,** and click **OK** .
   The dialog closes and the name of the **Operational Rule** is entered in the text box.
4. From the **Assignment Type** list, select **Publish the operational rule to MyApps for on demand execution** .
5. From the **Target Type** list, select your desired target type and click **Next** .
6. Click **Assign** .
7. Click **All** , select the target to which you want to advertise the **Operational Rule** and click **OK** .
   The dialog closes and the target is listed.
8. Click **Finish** to advertise the **Operational Rule** .
   The dialog closes and the **Confirmation** dialog box appears.

9. Select the **Go to Operational Rule** radio button and click **OK** .
   The dialog closes and the **Operational Rule** displays under the **Operational Rule** node.
10. Go to **Operational Rules > Your Operational Rule (Launch Calculator) > Assigned Objects > Your Target** and wait until the status is `Published` .On the screen of the target, the icon of the CM agent in the notification area of the task bar changes to indicating that a new **Operational Rule** is available and a tooltip will appear informing you of this fact on Windows and Mac OS devices.

You advertised an **Operational Rule** to your target and thus made it available to the local users on MyApps.

Related topics

- Creating a Quick Link Rule
- Modifying the MyApps Icon of an Advertised Rule
- Using Rules in the MyApps

Creating a Quick Link Rule

Contrary to all other types of operational rules a quick link rule has no steps and no packages, but it can have dependencies. It has only one parameter called URL, defining a web destination or an intranet share. Also, this rule type can only be advertised on MyApps and not be assigned to users and devices. When this type of rule displays in MyApps its name is clickable and links to the provided URL.

Note:

If you are using Internet Explorer the target URL must were added to the list of trusted sites.

Note:

If you are using Google Chrome or Firefox you need to have the LocalLink add-on installed on the local devices to open a browser on a file share. In this case you need to right-click the link and then select the **Open Link in Local Context** menu open with the respective submenu item where you want to open it, that is in this tab, a new tab or a new window.

Note:

Safari does not support links to file shares.

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog box appears.
2. In the **Name** text box enter a name for the **Operational Rule** , for example, *Google Home* .
3. To modify the icon that represents this rule in MyApps click the **...** button to the left.
   The **Select Operational Rule Icon** window appears displaying all available icons.
4. Select the desired icon and click **OK** .
   a. If none of the proposed icons fit your requirements, you can add other icons to this list by clicking **...** .
   b. In the **Add a MyApps Icon** window browse to the new icon's location and select it.

      > The icon symbol must have a size between 72 and 256 pixels and have an `.png` or `.ico` extension. The selected icon will be present in the **Select Operational Rule Icon** window when it is next opened.

   c. Click **Open** , this will then add the selected icon to those already available.
   d. Now select the new icon and click **OK**
      The icon to the left has now changed from the default to the selected one.
5. In the **Type** box select the **Quick Link** option.
   A new box **Url** appears.
6. Enter into this text box the URL that you want the to provide the quick link for, for example _ http://www.google.com_ .

   > If you are pointing to an intranet share the URL must have the following format: *//myshare.myserver.com/share1/share01* .

7. Click **Finish** to create the new **Operational Rule** .
   The dialog closes and the **Confirmation** dialog box appears.
8. To advertise the **Quick Link Rules** click **Yes** .
   The **Operational Rule Distribution Wizard** appears.
9. In the **Operational Rule Distribution Wizard** dialog select **Devices** from the **Target Type** list and click **Next** .
10. Click **Assign Device** .
    The **Assign to Device** dialog appears.
11. Click **All** , select the device to which you want to advertise the quick link rule and click **OK** .
    The dialog closes and the device is listed.
12. Click **Finish** to advertise the rule.
    The dialog closes and the **Confirmation** dialog box appears.

13. Select the **Go to Operational Rule** radio button and click **OK** .
    The dialog closes and the focus of the console is moved to the device assigned to the new quick link rule.

Once the **Status** `Published` you advertised the quick link rule to your target and thus made it available to the local users on MyApps . A tooltip will be displayed for **MyApps** systray icon informing you of that fact on Windows and Mac OS devices.

Modifying the MyApps Icon of an Advertised Rule

Operational rules of all types that are advertised in MyApps can be assigned a specific icon to be displayed with.

> **Note:**
>
> This icon is only applicable to MyApps and the **Properties** window of the rule. In the console in its hierarchy it will still be represented by the default icon, that is either for the default rules or for distribution rules.

To change the default icon of an advertised rule to a custom icon proceed as follows:

1. Select the rule for which to modify the icon in the right window pane.
2. Click **Properties** .
   The **Properties** dialog box appears.
3. To modify the icon that represents this rule in MyApps click the **...** button to the left of the **Name** field.
   The **Select Operational Rule Icon** window appears displaying all available icons.
4. Select the desired icon and click **OK** .
   a. If none of the proposed icons fit your requirements, you can add other icons to this list by clicking **...** .
   b. In the **Add a MyApps Icon** window browse to the new icon's location and select it.

      > The icon symbol must have a size between 72 and 256 pixels and have an `.png` or `.ico` extension. The selected icon will be present in the **Select Operational Rule Icon** window when it is next opened.

   c. Click **Open** , this will then add the selected icon to those already available.
   d. Now select the new icon and click **OK**
      The icon to the left has now changed from the default to the selected one.
5. Click **OK** .

Using Rules in the MyApps

The MyApps page provides the list of all advertised software packages and operational rules which are available for download and installation on the local client.

1. Enter the following address into your browser to access the MyApps page:

```
http://<client name>:<console port number>/kiosk
```

for example,

```
http://scotty:1611/kiosk
```

The MyApps page displays in your browser window.

2. To execute an available rule mark the box of the **Select** column at the right border of the desired operational rule, for example, Launch Calculator.
3. Click **Activate** at the bottom left of the page.
4. A confirmation window appears. Click **OK** to proceed.
   The status of the rule will change to **OK** / Updated once the rule was reassigned and then it is executed. You will see this once the confirmation message box to launch the calculator displays again on the screen.

- If you click **Yes** , and the calculator displays the status will become Executed again
- if you click **No,** the status will be Execution failed, because the rule could not be successfully completed

You have now executed an advertised **Operational Rule** on your target.

Assigning Targets to Operational Rules

Operational Rules can be assigned to different types of targets:

- devices
- device groups
- users
- user groups

The following topics are provided:

- Assigning an operational rule to a device
- Assigning an operational rule to a device group
- Assigning an operational rule to a user
- Assigning an operational rule to a user group
- Modifying the schedule of an operational rule

Assigning an operational rule to a device

To assign a device to an operational rule, proceed as follows:

1. Select **Edit > Assign Device** .
   A pop-up menu appears where you can define if the operational rule will be automatically activated with the default schedule.
2. Click **Yes** .

> If you select **No** , the operational rule must be specifically activated afterwards.

The **Assign to Device** pop-up window appears.

3. Select the device from one of the list boxes.
   If the operational rule is of type *Software Distribution* and the package is of type *MSI* and the administrative installation option is activated the **Select Installation Type** window will appear on the screen.
4. Select the desired type with which the package is to be installed:
   - **Administrative** Select this option if the package is to be installed in the classic MSI administrative installation mode.
   - **Network** Select this radio button if you want to extract the MSI package created with CM into a specific network path from which the target devices will download.
   - **Normal** Select this radio button if the package is to be simply downloaded by the target devices and installed.

   > Be aware that the administrative or network installation will work only with packages which were created with version 5.3.1 or later.

5. Click **OK** to confirm the assignment and close the window.

The device will be added to the table of assigned device groups with the default timer, which schedules execution once per hour.

Activating an Operational Rule for an Assigned Device

If the device assignment was not directly activated at the time of assignment it must be activated manually before the assignment becomes valid, that is, before the rule is transferred to the device and executed.

For an operational rule to be activated it must at least consist of one step and it must be currently deactivated. If the device assignment was effected through a group assignment the activation of the operational rule for this device will activate it for the whole group. To activate, proceed as follows:

1. Select the entry to activate in the table in the right window pane.
2. Click **Edit > Activate Operational Rule** .

The operational rule will be automatically activated.

Assigning an operational rule to a device group

To assign a device group to an operational rule, proceed as follows:

1. Select **Edit > Assign Device** .
   A pop-up menu appears where you can define if the operational rule will be automatically activated with the default schedule.

2. Click **Yes** .

   > If you select **No** , the operational rule must be specifically activated later.

   The **Assign to Device** pop-up window appears.
3. Select the device from one of the list boxes.
   If the operational rule is of type *Software Distribution* and the package is of type *MSI* and the administrative installation option is activated the **Select Installation Type** window will appear on the screen.
4. Select the desired type with which the package is to be installed:
   - **Administrative** Select this option if the package is to be installed in the classic MSI administrative installation mode.
   - **Network** Select this radio button if you want to extract the MSI package created with CM into a specific network path from which the target devices will download.
   - **Normal** Select this radio button if the package is to be simply downloaded by the target devices and installed.

     > Be aware that the administrative or network installation will work only with packages which were created with version 5.3.1 or later.

5. Click **OK** to confirm the assignment and close the window.

The device group will be added to the table of assigned device groups with the default timer, which schedules execution once per hour.

Activating an Operational Rule for an Assigned Device Group

If the group assignment was not directly activated at the time of assignment it must be activated manually before the assignment becomes valid, that is, before the rule is transferred to all members of the group and executed.

For an operational rule to be activated it must at least consist of one step and it must be currently deactivated. The reassignment will always be executed on all members of a device group if it is selected. To activate, proceed as follows:

1. Select the entry to activate in the table in the right window pane.
2. Select **Edit > Activate Operational Rule** .

The operational rule will be automatically activated.

Assigning an operational rule to a user

An operational rule can be assigned to users and to devices and device groups. In this case it can only be executed on a device if the assigned user logged on to it. To do so, proceed as follows:

1. Click **Assign User** .
   The **Assign to User** dialog displays.
2. Select the desired user from on of the available lists.
3. To allow the user to execute the rule on all devices to which he can log on, that is, of which he is either primary or secondary user check the option **Assign to Primary and Secondary Users (only primary if not selected)** .

   In addition you have the following options:

Parameter	Description
Install the selected rule as user (not as system)	Check this option if the rule is to be installed/executed as the logged on user instead of with the system account.
Deploy to devices linked to users	Select this radio button if the operational rule is to be assigned to the user and the device of which he is a user. You can define via the following options if the rule is to be assigned only to the device of which the user is the primary user or all devices of which he is a secondary user as well.
On Demand MyApps	Select this radio button if the operational rule is to be assigned to the user via MyApps. In this case the relation with the respective device(s) will be created when the user downloads and executes the rule on the device on which he is logged on. The following options are not applicable to this type of assignment.
Assign to Primary and Secondary Users (only primary if not selected)	Check this box if the assignments are applicable to the secondary users and the primary user. If not selected the assignments will only be carried out for the primary user. This option is only available if the preceding Deploy to devices linked to users option is selected.
Operational Rule Assignment Policy	Select from this list the type of policy to use for the user assignments:Assign at User Login: the assignment of the operational rules is carried out when the user logs on to a device. Assign at User Logout: the assignment is carried out when the user logs off. Assign Immediately: the assignment is carried out immediately after defining the assignment. Assign with Default Schedule: the assignment is carried out according to the defined default schedule. This option is only available if the preceding Deploy to devices linked to users option is selected.

4. Click **OK** .
   The window closes and the user to which the rule was assigned is listed in the table.

You assigned an operational rule to a user and all the devices on which he is registered in CM as a user.

Assigning an operational rule to a user group

An operational rule can be assigned to users and user groups and to devices and device groups. In this case it can only be executed on a device if a member of the assigned user group is logged on to it. To do so, proceed as follows:

1. Click **Assign User Group** .
   The **Assign to User Group** dialog box appears.
2. Select the desired user group from on of the available lists.
3. To allow the members of the user group to execute the rule on all devices to which they can log on, that is, of which they are either primary or secondary users, check the option **Assign to Primary and Secondary Users (only primary if not selected)** .

> You have the following additional options:

Parameter	Description
Install the selected rule as user (not as system)	Check this option if the rule is to be installed/executed as the logged user instead of with the system account.
Deploy to devices linked to users	Select this radio button if the operational rule is to be assigned to the user and the device of which he is a user. You can define via the following options if the rule is to be assigned only to the device of which the user is the primary user or all devices of which he is a secondary user as well.
On Demand MyApps	Select this radio button if the operational rule is to be assigned to the user via MyApps. In this case the relation with the respective device(s) will be created when the user downloads and executes the rule on devices he is logged on. The following options are not applicable to this type of assignment.
Assign to Primary and Secondary Users (only primary if not selected)	Check this box if the assignments are applicable to the secondary users and the primary user. If not selected the assignments will only be carried out for the primary user. This option is only available if the preceding Deploy to devices linked to users option is selected.
Operational Rule Assignment Policy	Select from this list the type of policy to use for the user assignments: Assign at User Login: the assignment of the operational rules is carried out when the user logs on to a device. Assign at User Logout: the assignment is carried out when the user logs off. Assign Immediately: the assignment is carried out immediately after defining the assignment. Assign with Default Assignment Date: the assignment is carried out according to the defined default schedule. This option is only available if the preceding Deploy to devices linked to users option is selected.

4. Click **OK** .
   The window closes and the user group to which the rule was assigned is listed in the table.

You assigned an operational rule to a user group and all the devices on which its members are registered in CM as users.

Modifying the schedule of an operational rule

When you assign a device to an operational rule you might want to modify the execution schedule for this device. Be aware that this only works if the device was directly assigned to the operational rule. If you modify the schedule of a device that was assigned via a device group assignment, the schedule for all members of this group is modified. To modify a schedule, proceed as follows:

1. Select the entry in the table for which the schedule is to be modified.
2. Click **Edit > Properties** .
   The **Scheduler** window appears. It shows a summary of the rule schedule right on top.
3. Make the necessary modifications by changing the provided options.

> To unassign the schedule select the **Prevent this object from running on a schedule** option in the **Do you want to configure a window in which this rule can run?** box.

4. Click **OK** to confirm the modifications and close the window.

Leveraging operational rule steps

BMC Client Management includes a large number of predefined steps for **Operational Rules**. However, you can also add (import) customized operational rule steps.

Refer to the Adding custom operational rule steps topic to learn how to create your own customized operational rule steps.

1. Make sure that both your XML and CHL files are valid and in the *[BMC Installation Directory]* /data/Vision64Database/opsteps folder.
2. In the Console , click the **Tools > Import New Steps** menu item.
3. In the **Schedule Import of New Steps** dialog, click **OK** .
   The dialog closes and the folder opstepsis checked for new steps. The XML and CHL files are verified and if successful, a new step is created.
4. To check your new step, add a step to an **Operational Rule** and in the **Select a Step** dialog select your step from the category you defined in the XML file.

You imported a step in the Console and made it available to **Operational Rules**.

Operational Rules Wizards

Operational rules can be created and executed in different ways. The CM wizards are one of the easiest ways to make your infrastructure configuration homogeneous. CM provides several wizards for the these tasks. The following wizards are available and can be launched from different locations in the console:

- Operational Rule Creation Wizard
- Operational Rule Distribution Wizard

Operational Rule Creation Wizard

The **Operational Rule Creation Wizard** guides you through the individual steps required to create a new operational rule. The wizard can be launched from anywhere in the console via the **Wizards > Operational Rule Creation** menu item or directly from the dashboard.

Related topics

- Definition - OR Wizard
- Steps - OR Wizard
- Packages - OR Wizard
- Dependencies - OR Wizard
- Confirmation - OR Wizard

Definition - OR Wizard

The first window, **Definition** , displays on the screen. In this first step the operational rule to be created must be defined:

1. Enter the name of the new operational rule into the **Name** box.
2. In the **Options** panel you can select which of the options need to be specifically defined for the new operational rule. Only the selected options will be displayed in the following windows of the wizard.
3. Click **Next** to continue.

Steps - OR Wizard

This window will only be displayed if you checked the respective box in the first wizard window. operational rules are made up of steps which tell the agent on the target devices which actions to execute. In this window you will select the steps to execute.

To add a step to an operational rule, proceed as follows:

1. Click **Add Step**  .The **Select a Step** pop-up windows appears. It displays all available steps in its Available Steps list box. In this window you can select your step in three different ways:

- In the **Hierarchy** tab you can look for the step through its class organization, by selecting the respective folder and then the desired step.
- The **All** tab displays the list of available steps in form of a table with its class and description.

- The **Search** tab allows you to search for a specific step of which you do not exactly know the name. Enter the words which you are sure it contains in the **Value** box and select the appropriate operator from the preceding **Operator** box and then click **Find** . The search will query all three values of the step: Step name, type and description. The following table displays all steps which match your condition. When you select a step a description will appear in the text box at the bottom of the window.

1. Select the desired step and click **Add** to add it to the operational rule.
   If parameters must be defined for the selected step, the **Properties** pop-up menu appears. It displays the list of parameters to define.
2. To define the parameters, enter the desired values into the respective boxes.
3. Click **OK** to add the step and close the window.
   The step is now added to the list of Selected Objects to the right.
4. To add more steps to the rule repeat the preceding steps until all required options are defined and then click **OK** to add them all to the operational rule and close the window.
5. Click **Next** to continue.

Packages - OR Wizard

In the second wizard window, **Packages** , you may add one or more packages to the rule if it is to be of type **Software Distribution** . Adding a package will automatically also create the steps required for the package installation. This window will only be displayed if you checked the respective box in the first wizard window.

1. Click **Add Package** .
   The **Select a Package** dialog box opens on the screen. It displays the list of available packages in its display window.
2. Select the desired package and click **OK** to add it to the operational rule and close the window.
3. Click **Next** to continue.

Dependencies - OR Wizard

This window will only be displayed if you checked the respective box in the first wizard window. The execution of an operational rule might depend on the successful execution of another operational rule, before it can be launched. If an operational rule on which another depends is executed but failed, all those depending on this operational rule will not be launched.

1. Click **Add Dependency** .
   The **Select an Operational Rule** dialog box opens on the screen. It displays the list of available operational rules in its display window.
2. Select the desired operational rule.
3. Click **OK** to add it and close the window.
4. Click **Next** to continue.

Confirmation - OR Wizard

After the operational rule is created a pop-up menu displays in which you can continue directly with the distribution of the newly created rule via the respective wizard. Click **Yes** to continue directly with the distribution of the new rule or **No** to just create it.

Operational Rule Distribution Wizard

This wizard allows to distribute operational rules of any type to all possible targets within your system, that is, you can distribute simple operational rules and packages, to either device groups as well as to users and user groups. It is also possible to advertise operational rules to the targets. The wizard can be launched from anywhere in the console via the **Wizards > Operational Rule Distribution** menu item.

Related topics

- Operational Rule - OR Distribution Wizard
- Assigned Targets - OR Distribution Wizard
- Scheduling the operational rule distribution
- Task - OR Distribution Wizard
- Confirmation - OR Distribution Wizard

Operational Rule - OR Distribution Wizard

In the first window of the wizard you define which rule to distribute and some distribution options:

1. Enter the name of the operational rule to distribute.
    a. If you are not sure of the name of the rule, click **Find** next to the field.
    The **Select an Operational Rule** pop-up windows appears.
    b. Select the operational rule to assign from one of the list boxes.
    c. Click **OK** to confirm the assignment and close the window.
2. Select the type of the target to which the operational rule is to be sent to and its assignment type.
3. Via the **Options** panel you can select which of the options need to be specifically defined for the operational rule distribution. Only the selected options will be displayed in the following windows of the wizard.
4. Click **Next** to continue.

Assigned Targets - OR Distribution Wizard

Assigned Targets In this next window you need to define the targets of the rule distribution. Depending on the target type you either add device groups here or users/user groups.

The following topics are provided:

- Assigning to Devices or Device Groups - OR Distribution Wizard
- Assigning to Users or User Groups - OR Distribution Wizard

Assigning to Devices or Device Groups - OR Distribution Wizard

1. Click **Assign Device** .
   The **Assign to Device** pop-up menu appears.
2. Select the device or device group from one of the list boxes.
3. If the operational rule is of type Software Distribution and the package is of type MSI and the administrative installation option is activated in the System Variables the Select Installation Type window appears. Be aware that the administrative or network installation will work only with packages which were created with version 5.3.1 or later and if the respective system variable is activated.
4. Click **OK** to confirm the assignment and close the window.
5. Click **Next** to continue.

Assigning to Users or User Groups - OR Distribution Wizard

1. Click **Assign User** .
   The **Select a User** pop-up menu appears.
2. Select the user or user group from one of the list boxes.
3. Check the **Install the selected rule as user (not as system)** box if the rule is to be executed on the device as the user and not as LocalSystem.
4. Click **OK** to confirm the assignment and close the window.
5. Click **Next** to continue.

Scheduling the operational rule distribution

The schedule of operational rule distribution is defined in the **Schedule** window by selecting options to answer the questions. Depending on the answer more options might become available.

When the schedule page is first opened it displays in the top part the default schedule that is defined for execution. As you go along with your schedule specifications this line changes to show the execution schedule you define in verbal form.

1. First the assignment needs to be defined, make the necessary selections for the following parameters:
   - **Assignment Date** Define when a job or a rule is to be assigned. Possible options are:

- **Assign Immediately** : the assignment is carried out immediately after defining the assignment.
- **Specific Date** : the assignment of the job or rule will be carried out at a specific date and time.
  - *Optional:* **Wake-up Devices** Check this box if the agent is to wake up any devices which are currently switched off, to immediately execute the assignment instead of waiting for the next startup to do so.

- *Optional:* **Run as Current User** Check this box if the distribution is to be executed and installed on the local device as the logged user and not as LocalSystem. If you are using environment variables in any of the step parameters you must check this box to make sure the variables of the local user are used and not the default values.
- *Optional:* **Advanced** Click this link if you require more assignment options:
- *Optional:* **Bypass Transfer Window** Check this box, if the distribution assignment is to be sent directly, ignoring any transfer window specifications which exist for the targets.
- *Optional:* **Upload Intermediary Status Values** Define if only the final status values, that is, *Executed* or *Failed* are to be uploaded (unchecked), or if each and every status that the operational rule execution is passing through is uploaded (checked). This option is only available if the corresponding system variable is activated.
- *Optional:* **Run while the execution fails** Defines if the operational rule/package is to be executed until its execution finally succeeds, that is, the final status *Executed* is uploaded.
- *Optional:* **Upload status after every execution** Defines that the status value is uploaded after every execution of the rule, even if it has not changed.
- *Optional:* **Assignment Activation** Defines the overall status of the software distribution rule for the respective device group. You can deactivate a group by unchecking the **Assignment Activation** box of the scheduler. By default this box is checked and the status is either *Activated* or *Paused* , if the default schedule was not selected during the assignment.
- *Optional:* **Back to Previous** Click this link to return to the main assignment options and continue with the execution schedule definition.

1. Select one of the following options for question **When do you want this rule to be run on devices?** to define when the actual execution is to be launched:

   > Depending on the choice you make in this list box, additional options become available.

   - **Right now** Select this option to start the execution immediately.
   - **At Startup** Select this option if the operational rule is to be executed every time the device is started.
   - **At Session Startup** Select this option if the operational rule is to be executed every time the agent is started
   - **At Session Close** Select this option if the operational rule is to be executed every time a session is closed.
   - **Run repeatedly on a schedule** Check this option if if the execution is to be scheduled repeatedly.
   - **Use Cronspec to Schedule** Select this option if the execution schedule is to be created via a cronspec.

2. *(Optional)* If you selected the **Run repeatedly on a schedule** option fill in the newly appeared boxes to create the execution schedule:
    a. Select if the schedule is to run every day, week or month.

> Be aware, that the weekly option is not available for agents of version 11.5.0 or earlier. If in your target groups there are agents of these versions, the final status is always `Sending impossible` .

> If you already used previous versions of CM , be aware that it is not possible any longer to define a schedule that executes *on the nth day of the month* .

    b. If you select the weekly schedule you also need to select on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one weekday.
    c. If you selected a monthly schedule you also need to select in which week of the month by selecting the respective number and on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one week and one weekday.
    d. Select the **Once daily** radio button to only execute the object once per day. Then, in the list box next to it specify the time at which it is to be run.
    e. Select the **Multiple times** radio button to execute the object more than once per day. Then, in the boxes appearing below, specify the frequency and the unit for the frequency. Check the **between** box if in addition these multiple times are to occur within a specific timeframe and define the start and end time of this interval in the newly list that appears boxes.
3. *(Optional)* If you selected the **Use Cronspec to Schedule** option fill in the values that appeared for the cronspec definition:

> Each set of ranges can be preceded by a % sign which will change the meaning from absolute to relative number. For instance if minutes equals 29 the timer will get fired each time the absolute time ends with a number of minutes equal to 29 (for example, 11:29) whereas %20 means every 20 minutes every hour, that is, at 13:00, 13:20, 13:40, 14:00, and so on.
>
> - Ranges are comma-separated lists. A range is made of a number eventually followed by a '-' sign and another number
> - The wildcard character asterisks (*) can be used to indicate any value.

- **Minute** Enter the minute value, it can vary from 0-59.

- **Hour** Enter the hour value, it can vary from 0-23
- **Day** Enter the day value, it can vary from 1-31.
- **Month** Enter the month value, it can vary from 1-12 (1 is January)
- **Week Day** Enter the week day value, it can vary from 0-6 (0 is Sunday).
- **Weeks of the Month** Enter the weeks of the month value, it can vary from 1-5.

4. *(Optional)* If the schedule is not to start immediately you need to select its starting moment from the **Do you want to configure a window in which this rule can run?** box.
   - **Prevent this object from running on a schedule** Select this option if you want to disable a schedule.
   - **Start the schedule immediately** Select this option if you want to start the schedule immediately.
   - **Start the schedule at next startup** Select this option if you want to activate the schedule only after the next startup of the device.
   - **Start the schedule window on** Select this option if you want to start the schedule at a specific date and time.
5. *(Optional)* If you selected the **Start the schedule window on** option you now need to select the date and time at which the schedule is to start in the boxes that appear.
6. *(Optional)* Select after how many executions the schedule is to stop. To have it run without any limits select the option **Unlimited** from the list box.
7. *(Optional)* If the execution is to stop at a specific date and time check the **End on** box and select the desired values from the list boxes next to it.
8. Click **Next** to continue if you selected to create a new task for this distribution or click **Finish** to confirm all choices and to activate the distribution.

Task - OR Distribution Wizard

This step of the wizard allows you to directly create a task for the rule distribution defined via this wizard or to assign it to an existing task. This option is only available if you checked the corresponding box in the first window of the wizard.

1. Provide the required information in the respective boxes.
2. Click **Finish** to confirm all choices and to activate the distribution.

Confirmation - OR Distribution Wizard

The last option provided by the wizard is to directly activate the operational rule distribution and to go to one of the objects, that is, the operational rule or the task, if one was created. Check the respective box to change the focus of the console window to the respective object. Then either click **Yes** , to go to the object, otherwise click **No** to keep the focus of the console on the currently selected view. Click **Cancel** to abandon and return to the wizard.

Examples of Operational Rules

Creating **Operational Rules** consists of putting together steps. Following you can see examples of **Operational Rules** with their respective steps to help understand how to combine steps.

ConfigFiles.cst

This predefined **Operational Rule** updates the Patch Knowledge Base of a device if its operating system is any version of Windows. It consists of the following two steps:

Step 1: **Check Operating System**

This step checks the Operating System of the device . After the check it proceeds in two different ways depending on the **Stop Condition** :

- if an operating system such as Windows XP (value = Yes) is detected, the **Operational Rule** proceeds with Step 2.
- if an operating system such as Linux (value = No) is detected, the step failed and the **Operational Rule** stops.

Parameter	Value
Stop Condition	**The rule fails**
Windows XP, Windows 2003, ... Windows 8 (64 bit)	**Yes**
Linux, Mac OS X, ...	**No**

Step 2: **Install Package**

In this step, **Install Package** the included package ConfigFiles.cstis checked for the correct checksum and installed on the device .

Parameter	Value
Package Name	ConfigFiles.cst
Package Checksum	0af1231f5c247cbad3df26c3abfc5946

Package 1: ConfigFiles.cst

Managing inventories

An inventory management system is concerned with the collection of static data from all managed devices in its network. Inventory management provides an easy-to-use functionality for data configuration of each managed device and makes this information available to an inventory system as required. The inventory software is then responsible for the cataloging and sorting of the information received from the different sources. The collected information is related to the individual properties of the object and contains extensive information, such as the installed processor and its type, speed, RAM, BIOS name and date, the software installed on the managed devices and any other custom defined attributes, such as the geographical location, for example, continent, country, town, building and room or company organizational units, such as department, workgroup, and so on. Not all of the preceding, however, are available for all platforms.

The server stores the inventory related data in the database. Therefore values from all computers are available at any time regardless of whether it is currently reachable across the network. But while this information resides in the database it serves no real purpose to you unless it is retrieved and displayed in reports, thus guiding you through the history of your system and helping you to gain a better understanding of what happened in your system. Through a good understanding of past performance, you can prevent problems in the future and ensure efficient operations.

The following topics are provided:

- Inventory Manager overview
- Managing inventory of a device
- Managing inventory of a device group
- Purging
- Collecting inventory remotely via USB for unconnected device
- Getting started with Custom Inventory

Inventory Manager overview

The BMC Client Agent agent collects inventory data of a number of different types. This first section introduces you to the different types of inventory, hardware, software, custom, security and unconnected device inventory. It details the different types of data which can be collected for the individual inventories and explains the forms in which they can be displayed and managed, for individual devices and groups of devices.

The following topics are provided:

- Inventory Types and Licenses
- Inventory availability
- Access rights and capabilities for inventories

Inventory Types and Licenses

The BMC Client Management - Inventory requires a specific license, which is based on the number of devices being audited via agentless or agent based methods. Not all types of inventory in CM are subject to the inventory licenses, because they belong to a specific functionality such as the patch management they are subject to the license of the functionality as explained below. If the license is exceeded no more inventories for devices will be integrated into the master database.

> **Tip**
>
> For a detailed list of attributes scanned by BMC Client Management inventory, see the attached BMC Client Management 12.5 Attribute List.

The following different types of inventories are available and depending on the type subject to specific licenses:

Inventory Type and License	Description
Connectivity (Inventory license)	This type of inventory is generated via an asset discovery scan of the network and displays the asset to which a device is physically connected. This type of inventory is only available if the device is a hardware that can be contacted via SNMP and can connect other hardware devices, for example, a router, a switch, and so on.
Hardware Inventory (Inventory license)	BMC Client Management - Inventory proposes both a standard basic set of hardware inventory data (CPU, OS, memory, disks, ports, etc.) and a WMI-based (Windows Management Instrumentation) inventory for Windows only.On Windows clients the inventory data can be filtered on the agent side to limit the amount of data displayed. These filters are defined in a specific .xml file which can be edited and is distributable from the console or can be accessed upon request from the agent for updates. They enable or disable specific hardware inventory attributes and allows you to modify attribute names and values according to your requirements.
Software Inventory (Inventory license)	The software inventory displays a single list of all software packages found on the remote device. The list is generated by the agent and uploaded into the database at regular intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line.
Custom (Inventory license)	The CM agent compiles custom inventory objects of a remote client for inspection by the administrator. This is based on a periodically generated Custom Inventory list. In addition to the list objects and object instances can be added to the custom inventory locally through the console. If an object is added twice, once manually through the console and via the list, the entry defined by the list will take precedence.
Security Settings Inventory (Inventory license)	The **Security Settings Inventory** node of the console displays a list of all security objects which are verified and collected through the operational rule steps on the remote device. The list is generated by the agent and uploaded into the database at the defined intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line.This type of inventory is not applicable to Mac OS X.
Power Management Inventory (Power Management license)	The **Power Management Inventory** in BMC Client Management - Inventory is a type of custom inventory, for which the agent verifies and collects specific device parameters through the operational rule steps on the remote device. This is based on a periodically generated Power Management Inventory list. The list is generated by the agent and uploaded into the database at the defined intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. For more information about this type of inventory refer to the Power Management topic.This type of inventory is only applicable to Windows systems.
Patch Inventory (Patch Management license)	The CM agent compiles an inventory type called Patch Inventory. This operation compares the list of patches and service packs installed on the device with the list of available patches provided by the ConfigFiles. The resulting patch inventory displays the difference between these lists, that is, all patches and service packs which are available for the device but are *not* yet installed. For more information about this type of inventory refer to the Patch Inventory topic. This type of inventory is only applicable to Windows systems.

Inventory availability

CM distinguishes between different types of devices that, depending on their type, do not have access to all types of inventories:

Device type	Icon	Inventory types
Unknown devices		Custom inventory
Scanned devices		Custom inventory
Unmanaged devices		Hardware, software and custom inventory

Device type	Icon	Inventory types
		
Device with agent		All inventory types

Access rights and capabilities for inventories

To be able to generate and manage the different types of inventories, an administrator needs specific capabilities and access rights for the inventories and their objects.

- The **Inventory** capabilities *view* and *manage* provide access to all inventories included in the inventory license as well as all operations that can be executed on them.
- The **Inventory Filter** capabilities *view, manage* and *assign* allow the administrator to create software and hardware filters for the respective inventory type and assign them to the target devices.
- **Custom Inventory Object Types** do not require either specific capabilities or access rights, they are available by default.
- Access to any individually created objects is restricted via the access rights defined in the object's **Security** tab and any restrictions that are defined the static or dynamic objects of the administrator's security profile.

Managing inventory of a device

The CM agent of the BMC Client Management - Inventory allows you to collect any type of inventory data for the individual computers of your network. The collected information is related to the individual properties of the object and contains extensive information, such as the installed processor and its type, speed, RAM, BIOS name and date, the software installed on the managed devices and any other custom defined attributes, such as the geographical location, the values of registry or of a configuration file entry. Not all of the preceding, however, will be available for all platforms. The different types of inventory can be accessed via the **Inventory** node of each device, either via the Device Topology top node or a device group node of which the respective device is a member.

The inventory for a device is accessed through the device's **Inventory** subnode. It provides access to all different types of inventory that can be collected for a device.

Its information displays via its two tabs **Asset Summary** and **Inventory Status**.

The following topics are provided:

- Viewing inventory details
- Viewing hardware inventory of a device
- Viewing software inventory of a device
- Viewing Custom Inventory
- Viewing security objects
- Viewing connectivity details

- Viewing History
- Hiding elements

Viewing inventory details

The **Asset Summary** node provides direct access to the most important information about a device. It lists the selected device's main information and a summary of the device's hardware, software and security inventory in the respective tabs.

The tab displays the following general information about the device:

Parameter	Description
Network Name	On top of the information the name of the device displays, either as its short network name if available, otherwise as its IP address together with the icon indicating its network status via the color, that is, green if the device is up and running and contactable and its operating system family.
Operating System Name	The name of the operating system installed on the currently selected device.
IP Address	The IP address of the device in its dotted version, such as 194.50.68.255.
Subnet Mask	The subnet mask of the device.
MAC Address	The MAC, that is, the hardware address of the currently selected device.
Domain Name	Displays the full name of the domain the currently selected device belongs to, that is, kirk.enterprise.starfleet.com.
Disk Serial Number	The serial number of the hard disk of the device.
User	This field displays the name of the user, that was logged when the last hardware inventory was generated.
Type	Displays the type of the device, that is, if it is a workstation, a server, a router, a switch, and so on.
Agent Version	The version number of the CM agent installed on the device.
Last Update	Displays the date and time at which the information shown in this tab was last updated.

Immediately generating and uploading the identity and inventories of a device

This button allows you to immediately generate and upload the identity and hardware, software and security inventories of the device. The inventory upload is forced even if the interval defined for the inventory generation has not yet elapsed. This action is only available for devices on which a CM agent with version 10 or later is installed.

Hardware Inventory of a discovered device

The **Hardware Inventory** tab of the **Asset Summary** displays a summary of the complete hardware inventory that displays in the respective inventory subnode. Specifically it lists in a tabular summary information about the device's manufacturer, its OS, BIOS and processor, RAM and hard disk, and the screen, keyboard, mouse and network adapters. This tab is only available if the discovered asset is a PC.

Software Inventory of a discovered device

The software inventory also provides a summary view of the device complete software inventory displayed in its inventory subnode. You can select via a list on top of the table which type of collected information to display, that is, only the software found via the Add/Remove Programs or installed via MSI for a Windows device, of by software type, that is, all web browsers. This tab is only available if the discovered asset is a PC.

Security Settings Inventory summary

The security inventory displays the security objects collected by default and their respective information: the installed antivirus, the installed firewall and the shared resources of a device.

What you have to know about Device Compliance

In this view you can find all compliance rules that are assigned to the currently selected device. On the right hand side of the view a chart displays presenting the global compliance of the device.

What you can do in this view

- You can re-evaluate a single rule by selecting it and clicking **Evaluate** .
- You can re-evaluate all rules by clicking **Evaluate All** .
- You can go to the selected rule by right-clicking and selecting the **Go To** menu item from the pop-up menu.

Evaluate the Compliance Situation

You can newly evaluate the compliance situation of the selected device from this view.

1. To evaluate the situation for only one or some of the assigned rules select them in the table.
2. Click the preceding button above the graph to open the drop-down menu.
3. From the menu list select the desired item:
    - **Evaluate All** Select this item if you want to evaluate the situation for all assigned rules.
    - **Evaluate Selection** Select this option if you have selected some specific rules to evaluate.

The evaluation is executed immediately. Depending on the number of rules to evaluate this might take some time.

Inventory Status for a device

Inventory Status for a device

The **Inventory** node displays the following information about the different types of inventory available for the currently selected device. This tab is not available if no inventories can be generated due to license restrictions.

Parameter	Description
Name	The fields of this column list the available types of inventory.
Last Update	The date and time the respective inventory type was last updated.
Status	This field displays the license status for the inventory type, that is, if it is exceeded or expired. If the field is empty the license is valid. This field is applicable if no inventory has yet been generated. If the license is not valid this type of inventory cannot be generated for the respective device.

Viewing hardware inventory of a device

BMC Client Management - Inventory proposes both a standard basic set of hardware inventory data (CPU, operating system, memory, disks, ports, etc.) and a WMI-based (Windows Management Instrumentation) inventory for Windows only.

The inventory data can be filtered on the agent side to limit the amount of data displayed. These filters are defined in a specific .xml file which can be edited and is distributable from the console or can be accessed upon request from the agent for updates. They enable or disable specific hardware inventory attributes and provide you the possibility to modify attribute names and values according to your requirements. For more information about this subject refer to the respective chapter of the technical reference manual. For more information on attributes, see Hardware Inventory Attributes.

Hardware Inventory Attributes

Hardware inventory results will vary depending on the operating system installed on the managed device, that is, Windows, UNIX or Mac OS, and, of course, on the administrator's choice. When you select one of the objects all its properties will be displayed in tabular format in the right window pane.

The most commonly displayed objects with some examples of their properties are the following:

Attribute	Description
BIOS	Displays information about the **BIOS** , such as the name and manufacturer, the installable languages, the status, version or release date, and so on.
Cache Memory	Displays information about the Cache Memory, such as associativity, block size, installed size, level and location, purpose and write policy, and so on.
CDROM Drive	Displays information about the CDROM Drive, such as availability, drive, ID, media type, status and system name, and so on.

Attribute	Description
Desktop Monitor	Displays information about the Desktop Monitor, such as display type, name, screen width and height, status and system name, and so on.
Disk Drive	Displays information about the Disk Drive, such as caption, index, interface type, media type, SCSI bus, sectors per track, size, status or the total number of cylinders, and so on.
Display Configuration	Displays information about the Display Configuration, such as the device name, the display flags and frequency, dither type, the driver version or specification version, and so on.
Floppy Drive	Displays information about the Floppy Drive, such as the manufacturer name, the status or system name, and so on.
Keyboard	Displays information about the Keyboard, such as the layout, the number of function keys, the power management supported or the status, and so on.
Logical Disk	Displays information about the Logical Disk, such as drive and media type, system name, file system, free space, size, volume name and serial number, and so on.
Motherboard Device	Displays information about the Motherboard Device, such as availability, caption, primary and secondary bus type and the system name, and so on.
Mouse / Pointing Device	Displays information about the Mouse or Pointing Device, such as the device interface, manufacturer, number of buttons, pointing type, status and system name, and so on.
Network Adapter	Displays information about the Network Adapter, such as the adapter type, index, MAC address, product and service name, and the time of the last reset, and so on.
Parallel Port	Displays information about the Parallel Port, such as availability, caption, operating system - autodiscoverable, supported protocols and system name, and so on.
Physical Memory	Displays information about the Physical Memory, such as the bank label, capacity, device locator, form factor, memory type and type details, and so on.
Printer	Displays information about the Printers attached to the device, such as attributes, availability, default priority, driver name, location, print processor, status and vertical resolution, and so on.
Processor	Displays information about the Processor, such as architecture, CPU status, L2 cache size, load percentage, processor type, role, socket designation and stepping, and so on.
Sound Device	Displays information about the Sound Device, such as availability, caption, manufacturer, name and status, and so on.

Viewing software inventory of a device

One of the major functions within the BCM agent is to compile a list of installed software applications on the remote client for inspection by the administrator. This is based on a periodically generated installed software file list, which is passed through a translation file to produce the actual list of installed packages or applications. The installed software file list is generated periodically because the work load required for this operation can be quite high. Therefore it is desirable to have a list already prepared when the Administrator needs to view it. An additional benefit of a periodic update is the possibility of monitoring the changes in the list and thus provide early alerts of virus attacks or unauthorized software installation.

The generation of the installed software file list is based on a number of parameters which are set in the configuration file, SoftwareInventory.ini. Same as the hardware inventory, the list of software inventory can be filtered and limited or extended through an .xml file. This file can be edited and is distributed from the console or can be accessed upon request from the agent for updates. For more information about this subject refer to chapter Software Inventory of the technical reference manual.

You can access the software inventory via the following aspects of it:

- Scanned Applications
- License Units

Scanned Applications

This node displays a single list of all software packages found on the remote device. The list is generated by the agent and uploaded into the database at regular intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. This information is by default updated once a day by default.

The following topics are provided:

- Scanned application information
- Adding as Managed Application
- Creating a software inventory filter definition

Scanned application information

BMC Client Management - Inventory automatically discovers tracks, collects, maintains and manages inventory of client systems assets from miscellaneous sources:

- On Windows operating systems the software inventory scans executable files on the disk and collects Win32 header information to have complete information about installed software. On UNIX operating systems the software inventory is collected through the respective operating system APIs, that is, RPM and DEB for Linux, for MAC OS a system command is used to find all installed packages. Any software which was not installed through these will not be shown in the list. It is also possible to specify in-house or un-discovered applications by listing their characteristics in the .XML translation file.
- All recovered information is then filtered through an .XML file, independently of the operating system, to make sure only the data requested by the administrator is uploaded. You will find more information about this file in the appendix under chapter Software Inventory in the technical reference manual.

The software found on the device and shown in the table can be filtered according to the following criteria via the **Type** drop-down box on top of the table:

- Add/Remove Programs - only the software found via this functionality (Windows only)
- MSI Database - only those applications that were installed via an MSI file (Windows only)

- Application - all types of software that are of type Application
- Web Browser - only the applications of type web browser are displayed
- All - all software of all types and discovery types are displayed

The software inventory displays in tabular version and shows the following information about all software found on the device:

Attribute	Description
Name	The name of the application as extracted from the installed software translation file. This is usually the complete product name, not including manufacturer or version information, for example, FinePrint 2000, InstallShield, Adobe Acrobat.
Version	The version string for the application as extracted from the translation file. This is a text string and contains generally a mixture of digits and letters as required by the entry, for example, 3.0 Rev. B.
Software Manufacturer	The name of the manufacturer of the application as extracted from the translation file. This is a free-form field and may contain the name by which the company is known or its complete registered name, such as Microsoft Corporation, Adobe Systems Incorporated, BMC Software, Inc.
Type	This field defines the type of the software, which may be Application, Web Browser, Communications, and so on.
Installation Date	This field shows the date at which the original installation took place, in the default format defined in the user preferences.
Installation Directory	The fields of this column display the full path of the respective installation directories.
File Count	This field displays the number of files of the software.

Adding as Managed Application

Applications can be managed in BMC Client Management via the **Application Monitoring** node. This means, software applications can be monitored when they are used and how often, they can be prohibited from starting and they may be protected, that is, they will heal themselves if they become corrupted in any way. You can add a software directly from this view to the list of managed applications. Only applications of type **Application** or **Browser** , which contain all required information to be managed, can be added. If an application listed in the software inventory does not provide all necessary information, or its type is **MSI** or **Add/Remove Programs** , this option will not be available. To add an application for managing proceed as follows:

1. In the list of applications select the application(s) to be added to the list of managed applications.
2. Select **Edit > Add as Managed Application** .
   A confirmation window appears.
3. In this window you can define the folder into which the application is to be added. By default it is added directly under the main application list node. To add it to another folder click the icon to the right (...). The **Select Folder** window appears displaying the folder hierarchy. If the desired target folder does not yet exist you can also create new folders. To do so first

select the parent folder of the new one and then select click **New Folder** below the hierarchy. The **Properties** dialog box appears. Enter the desired data into the respective text boxes and then click **OK** at the bottom of the window to confirm the new application list folder. Select the target folder and click **OK** to confirm and to close the window.

4. An Information window will now appear in which you can also directly add the selected application to an existing application list. Click **Yes** to do so, **No** to only add the application to the application catalog.
5. If you selected **Yes** , the **Assign an Application List** dialog box appears providing the list of existing application lists.
6. Select the desired application list from one of the lists available in the window.
7. Click **OK** at the bottom of the window to confirm.
8. If the application list is already assigned to a device or group, a **Confirmation** dialog box appears, in which you can define to directly reactivate the application list for its assigned objects.

Creating a software inventory filter definition

A new filter definition may be created directly for a specific software application. Be aware, that you can only add this new filter definition to an existing software inventory filter, no new inventory filter can be created here. To do so, proceed as follows:

1. Select the software application for which a new filter definition is to be created in the table in the right window pane.
2. Click **Edit > Software Inventory Filter Definition**.
   The Software Inventory Filter Definition Wizard is displayed on the screen.
3. In the first window you need to select the software filter to which the new filter definition is to be added, then click **Next**.
4. In the next window a name for the filter must be specified and the action. Click **Next** to continue.
   The next wizard window defines the MATCHFILE tag conditions.
5. Click **Next** to continue.
   The next wizard window defines the CREATE tag conditions.
6. Click **Finish** at the bottom of the window to confirm all settings and directly create and apply this new filter definition.

Products

This node lists all software that was found on the selected device sorted by the license units it is part of.

Each license unit is composed of the suites it contains, which again are composed of applications, the last level will indicate the files that uniquely identify the license unit.

It provides the following information about the license units:

Parameter	Description
Name	This column shows the names of all license units that might be installed on any of the devices in your network. A license unit in this case is any type of software application, tool or suite.
Manufacturer	This field displays the name of the manufacturer of the respective license unit.
Category Name	This field displays which type of application the license unit belongs to, for example, if it is a browser, an application server software, and so on.
Status	This field shows the status as which it is currently viewed in CM , that is, if it is a unit that is currently managed, either supported or unsupported, or if you have not yet dealt with it (Unidentified)

Viewing Custom Inventory

The BCM agent can also compile custom inventory objects of a remote client for inspection by the administrator. This is based on a periodically generated custom inventory list. In addition to the list objects and object instances can be added to the custom inventory locally through the console. If an object is added twice, once manually through the console and via the list, the entry defined by the list will take precedence.

The **Custom Inventory** list is an xml file which is editable by the administrator and can then be transferred to all clients in the network. The generation of the custom inventory list is based on a number of parameters which are set in its configuration file, **CustomInventory.ini**.

The **Custom Inventory** node of the console displays a list of all custom defined objects on the remote device. Contrary to the hardware and software inventory the custom inventory is generated via operational rule steps and their schedule. Any available inventory data is uploaded to the master once a day by default if not specified differently by a rule step. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. By default the custom inventory is not generated.

The following topics are provided:

- Custom inventory attributes
- Adding an object

Custom inventory attributes

Custom inventory for a device shows a number of objects which should be applicable to all supported operating systems, that is, Windows, UNIX and Linux. Each of these objects will be displayed split up into object specific properties.

Each object property lists the different items it found and clicking one of these displays the type of the object plus some details on this item.

Adding an object

To add a new object to the local custom inventory from the list of existing object types, proceed as follows:

1. With the **Custom Inventory** node selected in the left window pane select **Edit > Add Object**  .
   The **Add Inventory Object Type** pop-up menu appears. The **Available Object Types** drop-down box appears all types of custom inventory objects available in the database and which have not yet been added to the local client.
2. Select the object to add to the local inventory.
3. Click **OK** to confirm the new object and close the window.

Viewing security objects

The BCM agent can also compile a security inventory of any remote client (with the exception of Mac devices) for inspection by the administrator. This is based on the execution of operational rule steps.

The **Security Settings Inventory** list is an .xml file which is compiled by the steps and then is uploaded to the master. The update and upload of the security inventory file is based on a number of parameters which are set in its configuration file, SecurityInventory.ini.

The **Security Settings Inventory** node of the console displays a list of all security objects which are verified and collected through the operational rule steps on the remote device. Contrary to the hardware and software inventory the security inventory is generated via operational rule steps and their schedule. Any available inventory data is uploaded to the master once a day by default if not specified differently by a rule step. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. By default the security inventory is empty.

Security Inventory Attributes

Security inventory for a device shows a number of operating systems specific objects, that is, Windows and UNIX based. Each of these objects displays split up into object specific properties.

The following aspects of device security can be inventoried:

- **Find Service Status**
- **IPTables Parameters Security Center Antivirus**
- **Security Center Firewalls**
- **List of Windows Services**
- **Number of Administrator Accounts**
- **Number of Open Windows Sessions**
- **Open Ports**
- **Process List**
- **Run Level Commands**
- **Shared Resources**
- **Unix Service Status**
- **USB Storage Status**
- **Windows Patches**

- **Windows Registry Extracts**
- **Windows Start-up Programs**
- **Windows Update Status**

Each object property lists the different items it found and clicking one of these displays the type of the object plus some details on this item, found by the respective step.

Security Settings inventory objects

Like hardware and software objects, security inventory objects can have one or several instances and attributes providing further information. These objects are dependent on the security object itself. Below you can see the example for the list of open ports discovered for a device.

Viewing connectivity details

The **Connectivity** for a device displays the asset to which it is physically connected. This type of inventory is only available if the device is a hardware that can be contacted via SNMP and is able to connect other hardware devices, for example, a router, a switch, etc.

This type of inventory can only be generated via an asset discovery scan and it is only available for individual devices/assets not for device groups, deprecated devices are not listed either.

Depending on the type of the device/asset a different information displays:

- PC Device
- Other Hardware Asset

PC Device

A pc device can only be connected to one other hardware asset, such as its switch and this inventory displays the following information about this connection:

Attribute	Description
Name	This field displays the name or IP address of the asset that the pc device is connected to.

Physical Connectivity

The following information displays about the physical connections of an asset:

Attribute	Description
Port	The Ethernet port number of the asset.
Type	The direction of the connection, that is, if the device defined in this line is connected "into" the asset (IN) or if the connection is outgoing, that is, if the selected asset is connected to the listed asset (OUT).
MAC Address	The MAC, that is, the hardware address of the currently selected device.
Name	This field displays the name or IP address of the asset that the pc device is connected to.
User	This field displays the name of the user, that is currently logged on to the system, or the user who was last logged on to the device if currently no user is logged on.

Attribute	Description
Device Type	Displays the type of the autodiscovered asset, such as router, switch, firewall, game console, and so on.
Domain Name	Displays the full name of the domain the currently selected device belongs to, that is, kirk.enterprise.starfleet.com.
NetBIOS Name	The NetBIOS name of the currently selected client. For managed devices which have Linux or MacOS as their operating system this field is empty.
IP Address	The IP address of the device in its dotted version, such as 194.50.68.255.
Subnet Mask	The subnet mask of the device.
Host ID	If the operating system is Window it either displays the asset tag or the BIOS serial number depending on the manufacturer of the client. If the operating system is Linux this is the equivalent of the `hostid` command. If the operating system is MacOS this value displays the system serial number that displays in the **About This Mac** window or in the **System Profiler** .
Topology Type	The topology type of the device, that is, if the managed device is a master, a relay or a simple client. It can also be an unconnected, a scanned, a deprecated or an unknown device.
Operating System Name	The name of the operating system installed on the currently selected device.

If the discovered asset either has an CM agent installed or is otherwise known to and accessible via CM some the following actions can be executed on the selected device (depending on its topology type):

Delete

To delete a device proceed as described in the following. You need write access to the immediate parent, from which the device is being deleted.

1. Select the device to delete in the table to the right.
2. Select **Edit > Delete** .
   A confirmation window appears.
3. Click **OK** to confirm and close the window.

The selected device will be deleted immediately.

Launching an immediate asset discovery scan of a device

This menu option allows you to directly launch an asset discovery scan of the selected device, to generate and upload the latest device information, and a summary of its hardware, software and security inventory. The results are displayed in the **Asset Summary** tab of the device's **Inventory** node.

1. Select **Edit > Audit Now** .

The device scan is launched directly and the data in the **Asset Summary** tab of the device's **Inventory** node will be updated once the scan is finished.

Inventory Summary

Inventory Summary

This function starts an asset discovery process of the device. It's results will be displayed in the **Inventory** view of the device and will show the basic information of the device and an excerpt of its hardware, software and security inventory.

1. Select **Edit > Inventory Summary** .

The focus of the console is moved directly to the device's **Inventory** node with its **Inventory Summary** tab.

Deprecate Device

After a device has reached the end of its lifecycle and will be physically removed from the IT environment it must also be removed from the CM representation of the network. In this case its topology type will become **Deprecated Device** and its GUID will be erased. The basic data of the device, such as its OS, MAC and IP address, and so on, and hardware, software, custom and security inventory will be archived in the CM database, but the device is no longer manageable. It can, however, still be viewed in specific groups. If the device is a relay and still has children, all these will be deprecated, too. To deprecate a device, proceed as follows:

1. Select the device to deprecate in the table in the right window pane.
2. Select **Edit > Deprecate Device** .
   A confirmation window appears.
3. In this window you need to decide if the agent is to be uninstalled from the device via an uninstall rollout if the device has a Windows 32-bit or 64-bit operating system. To uninstall check the **Agent Uninstall** box.
4. Click **OK** to deprecate and archive the device and to close the window.
5. If the agent uninstall was selected, the **Agent Rollout Wizard** will appear on the screen in which you can either select an existing uninstall rollout or create a new one.
6. The icon of the device will now be changed to its deprecated version, an agent and possibly also a Patch Management license, if applicable, will be freed up and its basic data and inventories will be archived.
7. If the agent is not uninstalled, that is, identity information will still be uploaded from that device, a new device will be created with the same GUID and its name will be suffixed with its deprecate index number, for example, (0), (1), and so on.

Using the Direct Access Tools

A number of Direct Access Tools are available for the devices in your network, such as accessing its registry, services, or rebooting the device. The direct access tools are available from the **Device Topology** and the **Device Groups** nodes.

To use the direct access tools, proceed as follows:

1. Navigate to the desired device.

2. Right-click the device.
   A pop-up menu appears.
3. Select **Direct Access Tools** .
   A pop-up menu appears.
4. Select the desired tool from the list.

The device will open on either the subnode representing the selected tool or the main device node, where you can now execute the necessary operations. If you selected an immediate action such as checking the connection or rebooting the device the focus of the console stays at its current location.

Establishing a Remote Control Session

To establish a connection with the selected client proceed as described. It is possible from any point at which a device is selected to establish a remote control session with it.

> **Note:**
>
> Before you connect, however, ensure that you have the corresponding permissions to establish the connection.

1. Right-click the desired target device.
   A pop-up menu appears.
2. Select **Remote Control** .
   If you don't have the corresponding permissions to establish the connection, an **Identification** window will appear on the screen, prompting you for valid system credentials.
3. Enter the required credentials in the respective boxes.
4. Click **OK** to confirm.

The screen of the target device displays in the right window pane. You can now execute any required functions or manipulations or take over the mouse cursor to help the local user.

Other Hardware Asset

Other hardware assets, such as routers or switches, can be physically connected to a number of other assets. These are listed under the subnode **Physical Connectivity** .

Viewing History

The **History** tab displays the inventory delta, if the agent is configured to deliver inventory updates as such. For more information about how to configure the agent for delta upload refer to the chapter of the respective inventory type in the appendix.

The **History** tab provides the following information:

Parameter	Description
View	

Parameter	Description
	This field defines which type of delta to display in the following table. The possibilities are the following: **Complete History** to display all items of the inventory delta, **Added Objects** to display only the objects which were added, **Updated Objects** for all objects for which a value has changed or **Deleted Objects** to display only those items which are no longer part of the inventory.
Object Name	In this drop-down box you can select a specific object, which has experienced any type of modification during a delta upload to be displayed, or you can display all objects (**Any**). If no objects are displayed in the table only the value **Any** will be shown.
Limited View	If you check this box only elements which were added or removed to/from the delta will be displayed.
From	When clicking this field, a calendar displays from which you can select the date from which on the deltas are to be displayed. If the field is left empty, all available value are taken as the starting date.
To	From this calendar you can select the date until which the objects are to be displayed. If it is left empty all objects stored in the database up to the current moment are displayed.
Date Filter Reset	Click this button, to return to the default date settings for filtering, that is, no time restrictions.
Name	This field displays the actual name of the object which was uploaded by the inventory delta.
Instance Name	The instance name of the object.
Property Name	The property name of the object instance.
Old Value	If the object was modified this field will display the old value of the object. If the object is new this field remains empty; if the object was deleted this field contains the value of the deleted object, however, if several instances of an object are deleted, only one line will indicate this and thus this field also remains empty.
New Value	If the object was modified this field will display the new value of the object, if the value was deleted this field remains empty, if it was added this field displays the new object's value.
Date	Displays the date at which the inventory delta was integrated into the database.

Delete Inventory History

To clear this table and remove the complete history of this type of inventory, proceed as follows. Be aware that deleting the elements of this table does not modify in any way the data in the inventory's **Attributes** ' table.

1. Select **Edit > Delete Inventory History** .
   A confirmation window appears.
2. Click **OK** to confirm delete operation or **Cancel** to abandon without changes.

Hiding elements

In this tab an administrator can define inventory objects which are not to appear in the **History** tab of the devices. The selection made in this tab is applicable to all devices. However, these definitions are user based, meaning that the content of the **History** and **Hidden Elements** tabs may be different for different administrators.

The **Hidden Elements** tab provides the following information:

Parameter	Description
Name	This field displays the actual name of the object which was taken off the inventory delta list, such as Network Adapter, Video Controller or Logical Disk.
Property Name	The property name of the object, for example either Free Space, Name or File System for the Logical Disk element.

Hide Element

To add an element to the **Hidden Elements** table, proceed as follows. Be aware that the elements defined here will not be shown any more in the **History** tab of any device for the currently logged administrator, they might still be displayed though for other administrators.

1. Select the **Hidden Elements** tab of the respective inventory in the right window pane.
2. Select the **Edit > Hide Element** .
   The **Add Elements to Hide** pop-up menu appears.
3. Select the elements to be removed from the general **History** tab in the list box of the pop-up menu.
4. Click **OK** to confirm or **Cancel** to abandon without changes and close the window.

The elements will now be displayed in the table.

Managing inventory of a device group

The different types of inventory are also available for the device groups, offering an overview over a specific part of your network, such as the Anti-virus situation of your laptops or the current situation about the RAM of the computers in your development department. The inventory is accessible via the **Inventory** node below the respective device group.

The following topics are provided:

- Viewing hardware inventory of a device group
- Viewing software inventory of a device group
- Viewing Custom inventory of a device group
- Viewing Security settings of a device or a device group
- Security Products for a device or a device group

Viewing hardware inventory of a device group

BMC Client Management - Inventory proposes both a standard basic set of hardware inventory data (CPU, OS, memory, disks, ports, etc.) and a WMI-based (Windows Management Instrumentation) inventory for Windows only.

On Windows clients the inventory data can be filtered on the agent side to limit the amount of data displayed. These filters are defined in a specific .xml file which can be edited and is distributable from the console or can be accessed upon request from the agent for updates. They enable or

disable specific hardware inventory attributes and allows you to modify attribute names and values according to your requirements. For more information about this subject refer to appendix Hardware Inventory in the technical reference manual.

Hardware inventory group Members

Each object lists its properties in its **Members** tab, and clicking one of these displays the names of the computers this property was found on plus some details on this item and the computer.

The hardware inventory for groups shows a number of objects which may or cannot be applicable to all supported operating systems, that is, Windows, Linux and MacOS. The most commonly displayed objects with some examples of their properties are the following:

Attribute	Description
BIOS	Displays information about the **BIOS** , such as the name and manufacturer, the installable languages, the status, version or release date, and so on.
Cache Memory	Displays information about the Cache Memory, such as associativity, block size, installed size, level and location, purpose and write policy, and so on.
CDROM Drive	Displays information about the CDROM Drive, such as availability, drive, ID, media type, status and system name, and so on.
Desktop Monitor	Displays information about the Desktop Monitor, such as display type, name, screen width and height, status and system name, and so on.
Disk Drive	Displays information about the Disk Drive, such as caption, index, interface type, media type, SCSI bus, sectors per track, size, status or the total number of cylinders, and so on.
Display Configuration	Displays information about the Display Configuration, such as the device name, the display flags and frequency, dither type, the driver version or specification version, and so on.
Floppy Drive	Displays information about the Floppy Drive, such as the manufacturer name, the status or system name, and so on.
Keyboard	Displays information about the Keyboard, such as the layout, the number of function keys, the power management supported or the status, and so on.
Logical Disk	Displays information about the Logical Disk, such as drive and media type, system name, file system, free space, size, volume name and serial number, and so on.
Motherboard Device	Displays information about the Motherboard Device, such as availability, caption, primary and secondary bus type and the system name, and so on.
Mouse /Pointing Device	Displays information about the Mouse or Pointing Device, such as the device interface, manufacturer, number of buttons, pointing type, status and system name, and so on.
Network Adapter	Displays information about the Network Adapter, such as the adapter type, index, MAC address, product and service name, and the time of the last reset, and so on.
Parallel Port	Displays information about the Parallel Port, such as availability, caption, operating system - auto-discoverable, supported protocols and system name, and so on.
Physical Memory	Displays information about the Physical Memory, such as the bank label, capacity, device locator, form factor, memory type and type details, and so on.
Printer	

Attribute	Description
	Displays information about the Printers attached to the device, such as attributes, availability, default priority, driver name, location, print processor, status and vertical resolution, and so on.
Processor	Displays information about the Processor, such as architecture, CPU status, L2 cache size, load percentage, processor type, role, socket designation and stepping, and so on.
Sound Device	Displays information about the Sound Device, such as availability, caption, manufacturer, name and status, and so on.

Hardware Inventory of group members

The **Inventory** tab displays the object property information in tabular format:

Attribute	Description
Object Property Name	The fields of this column display the respective values found for the property, for example, the different names of the disk partitions found in the group.
Count	The values in these fields provide the number, how often the property with the name value was found in the group.

Viewing software inventory of a device group

Another of the major functions within the CM agent is to compile a list of installed software applications on the remote client for inspection by the administrator. This is based on a periodically generated installed software file list, which is passed through a translation file to produce the actual list of installed packages or applications. The installed software file list is generated periodically because the work load required for this operation can be quite high. Therefore it is desirable to have a list already prepared when the Administrator needs to view it. The alternative method of creating the list on demand signifies that the managed device would enter a CPU and disk intensive operation, which would result in a slow down of the managed device for up to a minute. An additional benefit of a periodic update is the possibility of monitoring the changes in the list and thus provide early alerts of virus attacks or unauthorized software installation.

The generation of the installed software file list is based on a number of parameters which are set in the configuration file, SoftwareInventory.ini. Same as the hardware inventory, the list of software inventory can also be filtered and limited or extended through an .xml file. This file can be edited and is distributed from the console or can be accessed upon request from the agent for updates.

The **Software Inventory** node of the console displays a single list of all software packages found on the remote device. The list is generated by the agent and uploaded into the database at regular intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line.

Related topics

- Software inventory group Members
- Products of a device group

Software inventory group Members

The software inventory display shows the following information on all listed items according to the following application properties:

- By Name
- By Version
- By Manufacturer
- By Type
- By Installation Date
- By Installation Directory
- By File Count

Related topics

- Software Inventory of group members
- Creating software filter definitions
- Software Properties

Software Inventory of group members

The **Inventory** tab lists all items found on the group members for the respective property.The information displays in tabular format and provides the following information:

Attribute	Description
Property	This field displays the value of the selected property, for example, the list of software manufacturers found on all members of the group when having selected the By Manufacturer property.
Count	This column displays the number of times the individual property was found on the group members. For the preceding example, the number of applications found installed for the respective manufacturer.

Creating software filter definitions

In this tab under the Name property of the software group inventory, a new filter definition can be created directly for a specific software application. Be aware, that you can only add this new filter definition to an existing software inventory filter, no new inventory filter can be created here. To do so, proceed as follows:

1. Select the software application for which a new filter definition is to be created in the table in the right window pane.
2. Click **Edit > Software Inventory Filter Definition** .
   The **Software Inventory Filter Definition Wizard** is displayed on the screen.
3. In the first window you need to select the software filter to which the new filter definition is to be added, then click Next.
4. In the next window a name for the filter must be specified and the action.
5. Click **Next** to continue.
6. The next wizard window defines the MATCHFILE tag conditions.
7. Click **Next** to continue.
8. The next wizard window defines the CREATE tag conditions:

9. Click **Finish** at the bottom of the window to confirm all settings and directly create and apply this new filter definition.

Software Properties

Each application property has one node per item found for it on at least one of the devices of the group.This node displays the following information about the found item:

Attribute	Description
Device Name	The name of the device on which the software application was found. If a software is installed on more than one device there will be one entry per device in this table.
Name	The name of the software application.
Version	The version number of the application.
Software Manufacturer	The name of the manufacturer of the application.

Products of a device group

This node lists all software that was found on at least one member of the selected group displayed by the license units it is part of.

They are listed according to the following criteria:

- **Category**
- **Manufacturer Name**
- **Name**

License Unit Inventory of group members

The **Inventory** tab lists all items found on the group members for the respective property.The information displays in tabular format and provides the following information:

Attribute	Description
Property	This field displays the value of the selected category, for example, the list of license unit types found on all members of the group when having selected the By Category property.
Count	This column displays the number of times the individual property was found on the group members. For the preceding example, the number of applications found installed for the respective manufacturer.

Viewing Custom inventory of a device group

The BCM agent can also compile custom inventory objects of a remote client for inspection by the administrator. This is based on a periodically generated custom inventory list. In addition to the list objects and object instances can be added to the custom inventory locally through the console. If an object is added twice, once manually through the console and via the list, the entry defined by the list will take precedence.

The **Custom Inventory** list is an xml file which is editable by the administrator and can then be transferred to all clients in the network. The generation of the custom inventory list is based on a number of parameters which are set in its configuration file, **CustomInventory.ini** .

The **Custom Inventory** node of the console displays a list of all custom defined objects on the remote device. Contrary to the hardware and software inventory the custom inventory is generated via operational rule steps and their schedule. Any available inventory data is uploaded to the master once a day by default if not specified differently by a rule step. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. By default the custom inventory is not generated.

Custom inventory group Members

Each of these objects will be displayed split up into object specific properties.

Custom Inventory of group members

The **Inventory** tab displays the object property information in tabular format.

Attribute	Description
Object Property Name	The fields of this column display the respective values found for the property, for example, the different IDs of the VESA Manufacturers found in the group.
Count	The values in these fields provide the number, how often the property with the name value was found in the group.

Viewing Security settings of a device or a device group

The BCM agent can also compile a security inventory of any remote client (with the exception of Mac devices) for inspection by the administrator. This is based on the execution of operational rule steps.

The **Security Settings Inventory** list is an .xml file which is compiled by the steps and then is uploaded to the master. The update and upload of the security inventory file is based on a number of parameters which are set in its configuration file, SecurityInventory.ini.

The **Security Settings Inventory** node of the console displays a list of all security objects which are verified and collected through the operational rule steps on the remote device. Contrary to the hardware and software inventory the security inventory is generated via operational rule steps and their schedule. Any available inventory data is uploaded to the master once a day by default if not specified differently by a rule step. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. By default the security inventory is empty.

Security settings inventory objects

Like hardware and software objects, security inventory objects can have one or several instances and attributes providing further information. These objects are dependent on the security object itself. Below you can see the example for the list of open ports discovered for a device.

Security settings inventory group Members

The security inventory display the information about all listed items according to their properties.

Security Settings Inventory of group members

The **Inventory** tab lists all attributes of the selected security object and the respective count for the members of the group. The information displays in tabular format and provides the following information:

Attribute	Description
Property	This field displays the value of the selected property, for example, the list of open ports found on all members of the group when having selected the Open Ports property.
Count	This column displays the number of times the individual property was found on the group members.

Security Products for a device or a device group

The software security products will be listed with their Name, Version and Vendor but only Firewall, Antivirus, Spyware and Browser products, depending on selected ones in the module configuration, will retrieve detailed information.

Purging

All other inventory types may be purged. All inventory data will be deleted in this case. This operation is also taken into account by the Inventory license which will then be incremented again. If the device for which the inventory is purged does not have a BCM agent installed, that is, it is of topology type **Scanned Device**, not only the inventory will be purged but the device itself will be deleted from the BCM database.

To purge a device and all its connected data from the database, proceed as follows:

1. Select the inventory to purge from the list in the left window pane.
2. Then select the **Edit > Purge**.
   A confirmation window is displayed on the screen.
3. Click **Yes** to confirm and delete all hardware inventory data.

Collecting inventory remotely via USB for unconnected device

In an organization's infrastructure most of the time all devices connect themselves at least occasionally to allow for the synchronization of their computer with any type of regulation and data reconciliation. In specific cases it is however possible that an infrastructure contains a number of completely isolated devices, which never connect to the network. BCM provides for just such cases a specific tool with which to collect some basic data on the unconnected devices such as their identity and basic information on the system and its hardware and software inventory via USB. After the data is collected and stored on the USB key, it can be imported to the master database via any other device on which a BCM agent is installed. The custom inventory for the unconnected device, however, can only be created directly in the console.

For more information, see Remote inventory collection via USB.

Remote Inventory Collection via USB

Unconnected devices in BMC Client Management - Inventory are devices of your infrastructure that are never connected to the network. However, CM provides a possibility to inventory (hardware and software) these devices and include the generated inventories in the BCM database . The custom inventory for these devices can only be created directly in the CM console .

Unconnected devices are a specific type of unmanaged devices and are treated in the console as such, that is, in this topic the terms unmanaged and unconnected are treated as synonyms.

Related topics

- Step 1- Preparing for Inventorying Unconnected Devices
- Step 2- Collecting Data on the Unconnected Device
- Step 3- Integrating the Unconnected Device Inventory into the Database
- Displaying Unconnected Device Inventory

Step 1- Preparing for Inventorying Unconnected Devices

Before you can collect data from devices never connected to your organization's network, you must prepare a USB key, via which the data collection is executed and which will transport the data to any other device of the network. For this, you need a USB key on which the tool provided by BMC Client Management - Inventory is installed. You can find it in the downloaded installation archive in the form of a `.zip` file under the directory `tools/UnconnectedDevices` .

1. Go to directory `tools/UnconnectedDevices` of the downloaded installation archive.
2. You will find one `.zip` file per operating system, that is, one for Mac OS, and one each for 32 and 64 bit Windows and 32 and 64-bit Linux. Select the zip file matching the operating system of the unconnected device.
3. Copy the file to the USB key and extract it in its directory.
4. You can put more than one version of the tool on your key, because you can collect the data of more than one unconnected device on a key. The number is only limited by the size of the key.

Step 2- Collecting Data on the Unconnected Device

The second step for inventorying an unconnected device is to locally collect the information. To do so, proceed as follows:

1. Go to the unconnected device and connect the USB key.
2. On the device select the key and the respective directory containing the appropriate tool for the device's operating system.

> Under the directory you can see three executable (`.bat`) files:

`allinventories.bat` : This file collects both types of inventories.
`hardwareinventory.bat` : collects only the hardware inventory of the device
`softwareinventory.bat` : collects only the software inventory of the device.

3. Launch the file of the desired type(s) of inventory.
   A terminal window opens in which you can follow the progress of the data collection. As you can see in the window, in addition to the selected inventories the tool also collects the identity information of the device and further information such as the operating system version and hardware connected information, such as MAC address, disk serial number, and so on.
4. When the terminal window asks you to, close the window.
   If you verify now under the tools directory you can see a newly generated file there, `unconnected.xml` .

The data collection on the unconnected device is now finished.

Step 3- Integrating the Unconnected Device Inventory into the Database

After all the data is on the USB key you must access any device which is connected to your network and has a CM agent installed. From there you can integrate the collected data via the agents browser interface to the master database.

1. Insert the USB key in the device.
2. Open the agent interface, connect as a user with admin rights and go to the **Tools** page.
3. There select the **Unconnected Devices** option.
4. In this page you must select the file to import the data. For this go to the tool's directory on the key and select the `unconnected.xml.` file. This file is the initial file for the data integration process. If you manually modified the file or moved it to another location the process will no longer work.
5. In the same window a new list box appears below displaying the names of all unconnected devices for which you collected data. You can select any number of devices to be integrated.
6. Click **Integrate** to start the process.
   The collected data of the selected devices will now be copied by the agent from the USB key and sent to the master. After there all will be integrated in the CM database.
7. To verify that the integration worked properly, a new browser window opens which lists all devices of which the collected data were correctly sent to the master and thus integrated. The inventories themselves cannot be displayed in the agent interface.

The data integration of unconnected devices is now complete and its results can be viewed in the console.

Displaying Unconnected Device Inventory

The identity and inventory data of unconnected devices, that is, devices without CM agent or unconnected devices, can only be displayed via the console.

Since unconnected devices, as their name implies, are not connected to the network, they will not appear under the **Device Topology** node. They are available in either of the following ways:

1. **Lost and Found**
   If no device groups collecting the unmanaged device topology type, the integrated devices will appear under the **Lost and Found** node.
2. **Search**
   You can also specifically search for unmanaged devices under the **Search** node.
3. **Device Groups**
   If you have a device group collecting ALL devices, or any type of group which includes the unmanaged device type, the unconnected devices of which the data was integrated into the master database will appear among its members.

Unconnected devices are represented by different icons than the other devices in the console, because they are neither unknown, nor is their connection established or lost. Unconnected devices are represented by an orange icon  , which, same as for the other connected devices indicate the operating system of the respective device, if known  ,  , and  . As such devices are not necessarily simple desktop devices, but also other network devices such as routers, switches, printers, and so on, they are represented by their specific icons.

This topic also includes:

- Lost and Found - Unconnected Device Inventory
- Search - Unconnected Device Inventory
- Device Group - Unconnected Device Inventory

Lost and Found - Unconnected Device Inventory

If no group exists to collect the inventoried unconnected devices you can see them all under the **Lost and Found** node.

1. Open the **Global Settings > Lost and Found** node.
   Here you can see the list of all devices that were inventoried by the scanner.

> **Note:**
>
> However, under this node you cannot display any information about the found objects. This is only available under the **Search** node or the device group‘s node.

Search - Unconnected Device Inventory

The **Search** node allows you to search for a specific type of object, that is, unmanaged devices and display their connected information. Proceed as follows:

1. Go to the **Search** node.
2. Here enter the following search criteria:
   - In the **Object** box leave the **Device** value and in the next list box select the option **Objects Found** .
   - From the **Criterion** list select the value **Topology Type** .
   - Leave the **Operator** as it is and select the value **Unmanaged Device** from the list of the **Value** box.
3. Click **Find** .
   The following **Results** box will now list all unmanaged devices which were integrated with the location **Global Settings** / **Lost and Found** / *Unmanaged Device Name* .
4. To access one of the devices and its inventory select the device.
5. Click **Edit > View Node** .
   The selected device displays below the **Search** node displaying its information and the available inventory subnodes, **Hardware** , **Software** and **Custom** .

Device Group - Unconnected Device Inventory

To display the list of unconnected devices and their collected inventory information via a device group, proceed as follows:

1. Create a query collecting all unmanaged devices, for example *Unmanaged Devices* .

   Currently the table is still empty.

2. To define the criteria of the query click **Edit > Add Criterion** .
   The **Select Criterion** is displayed on the screen.

   Note:

   It displays the list of available criteria in its left list field.

3. Select the criterion **Topology Type** .
4. Click **Find** in the following **Criterion Description** panel.
   The **Search Criteria** pop-up appears.

   Note:

It provides the list of all CM topology types.

5. Select the value **Unmanaged Device** and click **OK** .
   The selected option will now be displayed in the **Value** field of the **Search Criteria** window.
6. Click **Add** to add the criterion to the list.
7. Click **OK** to confirm the new query content and to close the window.
8. To activate select the green colored option **active** instead of the currently displayed red option **inactive** in the **Query Status** drop-down field.

> All newly created queries are inactive, thus they must be activated before they can manage a group.

9. Now reselect the new query in the **Members** tab of the main **Queries** node.
10. To directly create a device group based on this query select **Edit > Create Device Group** .
    The new group will be automatically created directly under the **Device Groups** top node with the same name as that of the query, that is, *Unmanaged Devices* .
11. Go to the *Unmanaged Devices* group which is located directly under the main **Assigned Group** node.
    The **Members** tab displays. Here you can see all devices of the address range specified that do not have a CM agent, that were inventoried by a scanner device and for which the inventory was manually collected. If no devices are displayed the group is configured to only display devices with agent.
12. To remedy this, select **Edit > Properties** .
    The **Properties** window appears.
13. Select the **All Devices** value from the **Device Type** drop-down list and click **OK** to confirm.
    Now all inventoried devices are displayed in the members list.
14. Double-click a device in the list.
    This will open the node in the left window pane and you will also find all these devices as subnodes of the group through which you can access the collected information.
15. Select one of the devices.

> This device, contrary to devices with an installed agent only has one subnode, the **Inventory** node.

Here you will see that only the **Hardware** and **Software** nodes are available. The unconnected device's inventories are displayed in exactly the same way as for any other device with agent.

Getting started with Custom Inventory

Contrary to the other types of inventory the **Custom Inventory** needs to be configured for devices and device groups first before its instances can be defined. This requires the following manual operations:

1. Create a new custom inventory object type.
2. Define the attributes of the new object type.
3. Add the new new custom inventory object type to the targets (devices/device groups).
4. Fill in the data of the new custom inventory object on the targets (add instances).

The following topics are provided:

- Creating a New Create Object
- Defining the Attributes of the New Create Object
- Adding the New Create Object to the Custom Inventory of a device
- Providing the Data for the New Custom Inventory Object

Creating a New Create Object

The **Custom Inventory** allows you to create any new object type specifically for the requirements or your organization. When creating a new object type, this new type will be added to the database and thus made available for all clients in the network. In our example here we will create a new object type for the location of a device which will include attributes such as the country, town, office, department, and others. To create it, proceed as follows:

1. Go to node **Global Settings > Custom Inventory Object Types** .
2. Click **Edit > Create Object** .
   The **Create New Object** window appears.
3. Enter the name for the new object, *Location* , into the provided field.
4. Click **OK** to confirm the new object and close the window.

The new object type will be created immediately.

Defining the Attributes of the New Create Object

Once the new object type is created its attributes must be defined, that is, which data of which type it is to store.

1. Select the object type to which an instance is to be added in the left window pane.
2. Click **Edit > Add Attribute** .
   The **Add Attribute** window appears.
3. Enter the required data into the respective boxes.
   - Enter *Country* into the internal **Name** box of the **Attribute** .
   - In the **Data Type** drop-down list you must select the type of data that is to be entered, for our example this will be **String** .

- Enter into the third box the display name of the column. This can but must not necessarily be the same as the **Attribute** name, for our case here it will be, so enter *Country* again.

4. Click **OK** to confirm and close the window.
   The new attribute is directly added to the object type.
5. Repeat the preceding steps for the new attributes *Town* and *Department* .
6. Then repeat the preceding steps again for the new attributes *Asset Tag* and *User ID* but making their **Data Type** an **Integer** .

All attributes for the new object type are now created and it can be used for the **Custom Inventory** .

Adding the New Create Object to the Custom Inventory of a device

Once the new object type is created it must be added to the targets. For our example here we will add it to the *Master* device.

1. With the **Custom Inventory** node selected in the left window pane select **Edit > Add Object** .
   The **Add Inventory Object Type** window appears. The **Available Object Types** drop-down box appears all types of custom inventory object types available in the database and which have not yet been added to the *Master* .
2. Select the *Location* object type.
3. Click **OK** to confirm the new object and close the window.
   The new object type is directly added to the list in the **Attributes** tab.

Providing the Data for the New Custom Inventory Object

The object is now added and all that remains is to provide the device specific data. Contrary to the other types of inventories this is not generated automatically but must be entered manually.

1. Select the object in the left window pane.
2. Click **Edit > Properties** .
   The **Properties** window appears.
3. Enter the desired data for the new instance into the respective text boxes.
   - **Country** : *France*
   - **Town** : *Nantes*
   - **Department** : *Accounting*
   - **Asset Tag** : *124589*
   - **User ID** : *2154*
4. Click **OK** to confirm and close the window.
   The object instance is immediately updated with the new information.

The custom inventory is now updated with all the device relevant information.

Note:

For the master device this object will always only have one instance, however, for example, a laptop can have more than one instance, if the user of the device is traveling between offices and the device can be used at any one of these locations. For this case you might want to add several instances of the object to keep track of the device.

Managing applications

This section guides you through following topics:

- Overview of Application Management
- Getting started with Application Monitoring
- Managing custom applications
- Managing software catalog
- Managing schedule templates
- Managing Application Lists
- Managing software licenses
- Managing licensed software
- Application Management Wizard
- Software License Management Wizard

Overview of Application Management

Application Management provides administrators with visibility on installed applications and link the applications to the business cycle. It allows for the correlation of software inventory data between purchased / licensed software to installed software and used software.

The application management nodes provide different approaches to monitor the applications installed on the remote clients in the network:

- It allows for the monitoring of applications to ensure acceptable performance on the remote clients.
- It allows administrators to monitor which applications are used and to stop the execution of unauthorized software.
- It provides the possibility to define ways of self-healing for the installed applications.
- It allows administrators to match the installed and used application base to the purchased licenses.

The following topics are provided:

- Components
- Application Management licenses
- Application Management capabilities and access rights

Components

Application management is composed of the following components:

Parameter	Description
Software Inventory	The software inventory collected by the CM agent is the basis for most of the application management operations. It provides the list from which the applications to be managed are chosen.
Custom Applications	The **Custom Applications** view is a container for all applications which are to be managed on the devices of your infrastructure, that is to say they are to be either monitored for performance, restricted in their execution, defined for selfhealing or monitored for license surveillance. These applications can be listed directly under the node or be sorted in folders for easier classification.
Software Catalog	The software catalog provides the list of all products, suites and applications that can be managed in their usage and their licenses.
Application List	An application list is a collection of one or more applications that are managed in a certain way. This is defined by the application list type, that is, if these applications are monitored, prohibited or protected.
Application Type	The application list types are the three different types, identified and named after their function: monitored, prohibited and protected applications.
Schedule Template	Applications can either be prohibited from use at all times in which situation the prohibited application can directly be assigned to the targets without further limitation. However, it is also possible to deny the use of application only at specific times and allow the users to launch these, for example for their private use at lunchtime or after regular working hours. The same is true for monitored applications, protected applications, however, are protected all the time and cannot be assigned to a schedule. Schedule templates are a sort of a timetable of time-slots in which the application usage can be denied or allowed or monitored.
Application Management wizard	CM also provides a wizard which guides you through the different stages of creating and managing your applications or to monitor their licenses.
Licensed Software	A licensed software collects all license units that are subject to a specific license. A licensed software can contain as many license unit as are included in the purchased license. After the licensed software is defined it can be assigned to individual devices or device groups for license evaluation. This evaluation verifies, if the assigned devices are in compliance with the license specifications, that is, if the application is only installed on those devices it is supposed to.
License Unit	A license unit is the software that requires license management, the entity that is verified against the license data provided to the licensed software object. This can be either an individual application, such as **Adobe Acrobat X** , a group of applications, such as all versions of **Camtasia** , a suite, such as **Microsoft Exchange Server** , or the complete product, such as **Microsoft Office 2010** or the different flavors of an operating system type.
Product	A product is the most global entity that collects all license suites and their applications of a specific software. For example, **Microsoft Office** contains all different office suites of this product, **Microsoft Office 2003** , **Microsoft Office 2007** , **Microsoft Office 2010** , and so on. For less voluminous products, this might just be the product name, such as **Camtasia** , which then would contain all versions of Camtasia supported by the purchased license.
Suite	A suite is part of a product and contains all the different applications that are part of the suite. For example, **Microsoft Exchange Server** , which contains all different versions of the exchange server, **Microsoft Exchange Server 2003** , **Microsoft Exchange Server 2007** , **Microsoft Exchange Server 2010** , and so on. This level does not exist for the smaller products, such as **Camtasia** or **Adobe Acrobat** , which do not have suites.
Application	

Parameter	Description
	An application is the smallest individual level for which a license can be purchased. For example, the **Microsoft Office 2007** suite contains **Microsoft Excel 2007** , **Microsoft Excel 2007 sp1** , **Microsoft Excel 2007 sp2** , **Microsoft outlook 2007** , **Microsoft Outlook 2007 sp1** , **Microsoft Outlook 2007 sp2** , **Microsoft Word 2007** , and so on. **Adobe Acrobat** , for example, could contain **Adobe Acrobat 9.0** , **Adobe Acrobat 9.3** and **Adobe Acrobat 9.4** for a license for all flavors of Acrobat version 9.

Application Management licenses

Application Management is part of the BMC Client Management - Inventory license and does not require a license of its own. However, Client Management provides two optional licenses that can enhance the **Application Management** functionality:

- **Software Catalog**
  This license activates the software catalog. The software catalog collects all suites and applications that are part of products.
- **Software Catalog Updates**
  This license provides regular updates for the software catalog to ensure that it contains always the most up-to-date information.

Application Management capabilities and access rights

To be able to work with applications and software licenses and their monitoring, an administrator needs specific capabilities and access rights for the different objects.

Application Management

- **Application Management** top node: **Managed Application** - **View** .
- The capability **Managed Application** - **Manage** is required to create and manage custom applications as well as to access and manage the contents of the software catalog.

Schedule Template

- To create, modify, delete and assign schedule templates: capability **Schedule Template** - **Manage** as well as *Write* access rights.

Application List

- To create, modify and delete application lists: capability **Application List** - **Manage** as well as *Write* access rights.
- To assign application lists: capability **Application List** - **Assign** as well as *Assign* access rights.

Licensed Software

- To create, modify and delete software license units: capability **Licensed Software** - **Manage** as well as *Write* access rights.

- To assign software license units: capability **Licensed Software** - **Assign** as well as *Assign* access rights.
- To configure the **Software License Management** : capability **Licensed Software** - **Configure** as well as *Write* access rights.

Devices

- To be able to view and assign the target devices for application and license monitoring the capabilities **Device** and **Device Group** - **View** and *Read* access rights are required.
- To view the inventories of the target devices the **Inventory** - **View** and *Read* access rights are required.

Getting started with Application Monitoring

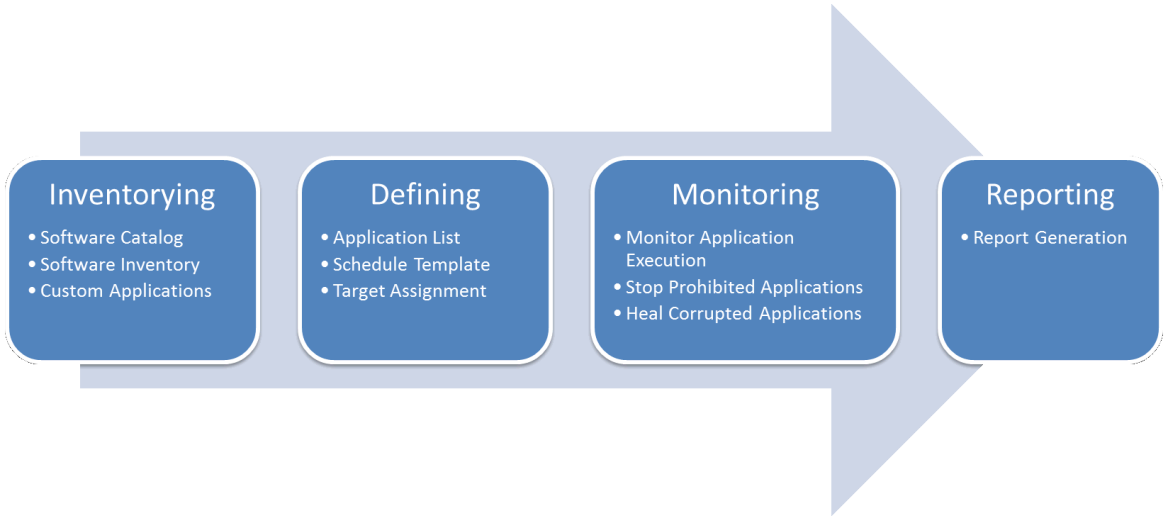
The **Application Monitoring** functionality allows you to create the following different types of monitoring of the applications installed on the remote clients in your network:

- Application execution and usage
- Prohibited applications
- Protected applications that are self-healed when found corrupted.

The following topics are provided:

The four steps of Application Monitoring

Application Monitoring consists of four consecutive steps:



- **Software inventorying** :
  Finding all the applications that are to be monitored in any way via either the
  - Software inventory
  - Software catalog
  - or creating applications via the custom applications
- **Defining** :
  In this second phase the actual applications lists is created, their type defined, that is, if the chosen applications are monitored for their usage, prohibited from execution or monitored for possible corruption and consecutive repairing. In this phase the required schedule templates are create and assigned and they are also assigned to their targets on which they are monitored.
- **Monitoring** :
  In this third step the usage of the application is monitored: it is stopped if illegally launched or repaired if it was found to be corrupted.
- **Reporting** :
  In this last step reports are generated on individual devices, device groups or applications on their usage or launch prohibition.

Automatic Application Monitoring

Automatic Application Monitoring in Client Management is performed via Application Management. The system will automatically discover all applications available for monitoring, prohibiting and selfhealing.

When these are defined and assigned to devices or device groups, tracked and/or prohibited in their usage, they can also be "healed", if they are corrupted.

The main object of this functionality is the **Application List**. It groups software into monitored, prohibited and protected categories in the following different ways:

- **Scanned Application**:
  the application list is populated with individual software applications, found by the software inventory.
- **Software Catalog**:
  the application list is populated with applications provided by the Software Catalog.

> **Note:**
>
> You should have Adobe Acrobat Reader or a similar application installed, as the following topics are based on it. However, you can also execute these examples by replacing them with another application that you installed on your devices.

Related topics

- Defining an Application for Usage Monitoring
- Defining an Application for Usage Monitoring via the Software Catalog
- Defining an Application for Prohibited Launch Detection
- Defining an Application for Prohibited Launch Detection via the Software Catalog
- Defining an Application for File Corruption Protection
- Uploading Application Monitoring Events to the Master
- Generating Application Monitoring Reports
- Defining Applications to Use in Application Management
- Configuring Application Monitoring
- Adding an Application from a Device
- Monitoring Managed Applications

Defining an Application for Usage Monitoring

A monitored application enables customers to query the actual usage of applications on the managed devices. In this node you can define the applications which are to be monitored and on which clients in your network. The actual monitoring will be done by the local agent according to the definitions set up in the respective Monitored Application Model. The agent stores the logged data, the date and time the application was started and ended as well as the duration of the usage, in the local database and uploads these periodically to the master database.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a list of applications to manage** radio button.
3. Click **Next** .
4. In the **Application List** window enter *Monitoring Adobe Reader* into the **Name** field.
5. From the **Type** drop-down list select the **Monitored Application** option.
6. Click **Next** .
7. In the **Applications** window click **Add an application from the inventory list** .
8. To find the application enter all or part of its name into the **Value** field, for example, *Reader* and then click the **Find** button.

   > If your network has different versions of Reader installed you can see here all versions.

9. Select the desired version and click **OK** .
10. Click **Next** .
11. In the **Assigned Objects** window click **Add Device** on top of the list field.
12. Go to the **All** tab of the **Select a Device** window and select the master from the list.

13. Click **OK** .
14. Click **Finish** .
15. In the **Confirmation** dialog box, click **Yes** to confirm the activation.
    The application is defined for monitoring.
16. Now launch and close the *Adobe Reader* application several times on the assigned device (master) and leave it finally running.
17. Open the **Device Topology > Master > Agent Configuration > Module Configuration > Application Monitoring** node.
18. Select the **List** tab.

    It displays all applications that were selected for managing on the local client, monitored as well as prohibited applications. For the moment you will only see the *Adobe Reader* entry.

19. Go to the **Monitored Application Usage Details** tab.

    This table displays the details on the monitoring of *Adobe Reader* . You will see that there are as many entries in the table as you have effected opening and closings of the application. The last opening is not yet counted as the application has neither yet been closed nor has it been open for more than 24 hours.

20. Close the *Adobe Reader* application now and then refresh the console view.
    Another entry was added to the list.

Defining an Application for Usage Monitoring via the Software Catalog

A monitored application enables customers to query the actual usage of applications on the managed devices. In this node you can define the applications which are to be monitored and on which clients in your network. The actual monitoring will be done by the local agent according to the definitions set up in the respective Monitored Application Model. The agent stores the logged data, the date and time the application was started and ended as well as the duration of the usage, in the local database and uploads these periodically to the master database.

Note:

This example requires the Software Catalog license. If you do not have this license refer to example Defining Applications to Use in Application Management , it executes the same operation without the catalog.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a list of applications to manage** radio button.
3. Click **Next** .
4. In the **Application List** window enter *Monitoring Adobe Reader* into the **Name** box.
5. From the **Type** drop-down list select the **Monitored Application** option.
6. Click **Next** .
7. In the **Applications** window click **Add license units from the software catalog** .
8. From the drop-down list below the **Only Show Discovered Software** box select the **Adobe Systems Incorporated** option if this is not yet selected.
   The list box below will now display all Adobe software that was found on at least one of the devices of your network that were already inventoried.
9. Find the *Reader* entry and select it.

> If the Reader is not on the first-level of displayed software open the items to find it.

10. Click the **Add** button.
11. Click the **OK** button to confirm.
12. Click **Next** .
13. In the **Assigned Objects** window click **Add Device** on top of the list box.
14. Go to the **All** tab of the **Select a Device** window and select the master from the list.
15. Click **OK** .
16. Click **Finish** .
17. In the **Confirmation** dialog box, click **Yes** to confirm the activation.
    The application is defined for monitoring.
18. Now launch and close the *Adobe Reader* application several times on the assigned device (master) and leave it finally running.
19. Open the **Device Topology > Master > Agent Configuration > Module Configuration > Application Monitoring** node.
20. Select the **List** tab.

> It displays all applications that were selected for managing on the local client, monitored as well as prohibited applications. For the moment you will only see the *Adobe Reader* entry.

21. Go to the **Monitored Application Usage Details** tab.

This table displays the details on the monitoring of *Adobe Reader* . You will see that there are as many entries in the table as you have effected opening and closings of the application. The last opening is not yet counted as the application has neither yet been closed nor has it been open for more than 24 hours.

22. Close the *Adobe Reader* application now and then refresh the console view. Another entry was added to the list.

Defining an Application for Prohibited Launch Detection

A prohibited application list allows the administrator to disable the launching of specific applications on a managed device using the criteria defined through the Prohibited Application Model. It allows the denial of certain application launches, both on online as well as off-line devices.

The following example prohibits the execution of the Pinball game on the master during working hours.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a list of applications to manage** radio button.
3. Check the **Define a specific schedule to manage these applications** box.
4. Click **Next** .
5. In the **Application List** window enter *Prohibiting Pinball* into the **Name** box.
6. From the **Type** drop-down list select the **Prohibited Application** option.
7. Click **Next** .
8. In the **Applications** window click **Add an application from the inventory list** .
9. To find the application enter all or part of its name into the **Value** box, e.g. *Pinball* and the click the **Find** button.

If your network has different versions of Pinball installed you can see here all versions.

10. Select the desired version and click **OK** .

To prohibit all versions of Pinball select all entries in this window.

11. Click **Next** .
12. In the **Schedule Template** check the **Create a new schedule template** option.
13. Click **Next** .
14. In the **Schedule Template Configuration** window enter the name into the respective text box, e.g. *No Working Hours* .

> The current planning prohibits the execution at all times, indicated by red crosses in all boxes.

15. To allow the execution for non-working hours mark the boxes *Mon-Fri 12:00-13:59* by clicking the first box (Mon 12:00) and dragging the mouse key to the last box (Fri 14:00).
16. Click **Allow Time-slot** to allow the application to execute in this time range.
17. Click **Next** .
18. In the **Assigned Objects** window click **Add Device** on top of the list box.
19. Go to the **All** tab of the **Select a Device** window and select the master from the list.
20. Click **OK** .
21. Click **Finish** .
22. In the **Confirmation** dialog box, click **Yes** to confirm the activation.
    The application is defined for launch prohibition.
23. Now start *Pinball* on the assigned device (master).
    The execution will be stopped and an **Information** window appears telling you that *Pinball* was prohibited from execution.

> **Note:**
>
> If *Pinball* is launched instead of being stopped, maybe you are currently in the allowed timeframe?

24. Click **OK** to close the message box.
25. Open the **Device Topology > Master > Agent Configuration > Module Configuration > Application Monitoring** node.
26. Select the **List** tab.

> It displays all applications that were selected for managing on the local client, monitored as well as prohibited applications. Here you will see now the monitored application *Adobe Reader* (if you have executed the preceding example) as well as the new prohibited *Pinball* . If this is not the case refresh the view.

27. Go to the **Prohibited Application Usage Details** tab.

> This table displays the details on the monitoring of *Pinball* execution and should now show the tentative to launch the software.

Defining an Application for Prohibited Launch Detection via the Software Catalog

A prohibited application list allows the administrator to disable the launching of specific applications on a managed device using the criteria defined through the Prohibited Application Model. It allows the denial of certain application launches, both on online as well as off-line devices.

The following example prohibits the execution of the Pinball game on the master during working hours.

> **Note:**
>
> This example requires the Software Catalog license. If you do not have this license refer to example Defining an Application for Prohibited Launch Detection, it executes the same operation without the catalog.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a list of applications to manage** radio button.
3. Check the **Define a specific schedule to manage these applications** box.
4. Click **Next** .
5. In the **Application List** window enter *Prohibiting Pinball* into the **Name** box.
6. From the **Type** drop-down list select the **Prohibited Application** option.
7. Click **Next** .
8. In the **Applications** window click the **Add license units from the software catalog** icon.
9. Click the **Search** tab button on the left.
10. From the **Type** drop-down list select the **Application** value.
11. Into the **Value** box enter *Pinball* .
12. Click the **Find** icon next to it.
13. Select the *Pinball* entry and click the **Add** button.
14. Click the **OK** button to confirm.
15. Click **Next** .
16. In the **Schedule Template** check the **Create a new schedule template** option.
17. Click **Next** .
18. In the **Schedule Template Configuration** window enter the name into the respective text box, e.g. *No Working Hours* .

    > The current planning prohibits the execution at all times, indicated by red crosses in all boxes.

19. To allow the execution for non-working hours mark the boxes *Mon-Fri 12:00-13:59* by clicking the first box (Mon 12:00) and dragging the mouse key to the last box (Fri 14:00).

20. Click the **Allow Time-slot** icon to allow the application to execute in this time range.
21. Click **Next** .
22. In the **Assigned Objects** window click **Add Device** on top of the list box.
23. Go to the **All** tab of the **Select a Device** window and select the master from the list.
24. Click **OK** .
25. Click **Finish** .
26. In the **Confirmation** dialog box, click **Yes** to confirm the activation.
    The application is defined for launch prohibition.
27. Now start *Pinball* on the assigned device (master).
    The execution will be stopped and an **Information** window appears telling you that *Pinball* was prohibited from execution.

> **Note:**
>
> If *Pinball* is launched instead of being stopped, maybe you are currently in the allowed timeframe?

28. Click **OK** to close the message box.
29. Open the **Device Topology > Master > Agent Configuration > Module Configuration > Application Monitoring** node.
30. Select the **List** tab.

> It displays all applications that were selected for managing on the local client, monitored as well as prohibited applications. Here you will see now the monitored application *Adobe Reader* (if you have executed the preceding example) as well as the new prohibited *Pinball* . If this is not the case refresh the view.

31. Go to the **Prohibited Application Usage Details** tab.

> This table displays the details on the monitoring of *Pinball* execution and should now show the tentative to launch the software.

Defining an Application for File Corruption Protection

The Protection or Selfhealing feature of CM is based on a list of selfhealing applications. Each protected application has a definition that contains all the information necessary to protect that application, that is the list of files which are part of the application, the date and time the file was found belonging to the application as well as its size and checksum at that time. All this information is gathered by the local agent and stored in its database. The agent will then check the file time and size at regular intervals, currently set to 5 minutes. If the time and/or size of the file has

changed the agent will then verify the checksum. If all three values have changed the agent will recover a copy of the original file either from a backup located on the local device or from a copy by another agent with the same file protection scheme.

For this example we will add the application to protect from the Custom Applications. If you have not yet defined any, refer first to example Defining Applications to Use in Application Management in the **Advanced** section to add the Reader application.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a list of applications to manage** radio button.
3. Click **Next** .
4. In the **Application List** window enter *Protecting Adobe Reader* into the **Name** field.
5. From the **Type** drop-down list select the **Protected Application** option.
6. From the **Source** drop-down list select the **Scanned Applications** option.
7. Click **Next** .
8. In the **Applications** window click the **Add an application from the custom applications** icon.
9. Select the *Adobe Reader* application in the list displayed in the **Add an Application from the Custom Applications** window.
10. Click the **OK** button to confirm.
11. Click **Next** .
12. In the **Assigned Objects** window click **Add Device** on top of the list field.
13. Go to the **All** tab of the **Select a Device** window and select the master from the list.
14. Click **OK** .
15. Click **Finish** .
16. In the **Confirmation** dialog box, click **Yes** to confirm the activation.
    The application is defined for corruption selfhealing.

Uploading Application Monitoring Events to the Master

Up to now the event data regarding application monitoring are only available locally on the agent. However, to be able to generate reports on this topic and to view them in the console together with other data these events must be specifically uploaded to the master and its database. Once data on application monitoring is available in your network, you can generate different reports to summarize the general situation or detail specific application lists.

1. Click the **Wizards > Operational Rule Creation** menu item to launch the **Operational Rule Creation Wizard** to create an operational rule uploading the available events.
2. In the **Definition** window enter a descriptive name into the **Name** field, e.g. *Upload Application Monitoring Events* .
3. Click **Next** .
4. In the **Steps** window click **Add Step** .
5. In the **Select a Step** window click the **Event Log Manager** folder.

6. Select the step **Upload Events** and click **Add** .
7. From the **Model Name** drop-down list select the **Monitored Applications** , **Prohibited Application** or **Protected Application** value for the respective list type and leave all other boxes as they are.
8. Click **OK** to confirm the parameters.

> To add the upload for all three types of lists repeat points 3 to 5 for the other two types.

9. Click **OK** again to add the step to the rule.
10. Once all steps are added click **Finish** to confirm the new rule and finish this wizard.
11. In the **Confirmation** dialog box, click **Yes** to continue directly with the distribution of the new rule.
12. In the **Operational Rule** window click **Next** without any modifications.

> In the **Assigned Targets** window you need to define the targets of the rule distribution.

13. Click **Add Device Group** on top of the list field.
14. Select the group containing your target devices, for example *All Devices* from the list box.
15. Click **OK** .
16. Click **Finish** to confirm all settings and finish this wizard..
17. In the **Confirmation** dialog box, check the **Go to Operational Rule** box to change the focus of the console window to the rule distribution view of the assigned group.
18. Click **OK** to confirm the activation.
19. If you did not check the **Go to Operational Rule** box at the end of the wizard select the rule in the left window pane and then the rule's **Assigned Objects > Devices** subnode.

> In the table to the right you can see the entry for each of the assigned devices and you can follow the upload process in the view's schedule **Status** column.

The initial status is `Assignment Sent` and the final stage should be `Executed` . Once this status displays the events are uploaded to the master database.

Generating Application Monitoring Reports

CM provides a number of *predefined reports* for the application monitoring with its out-of-the-box objects. They are all collected in the *Application Usage* folder.

Note:

As this report is based on device groups ensure that you have a device group to run this report on, if not you need to create one first.

1. Open the **Reports > Application Usage** folder.
2. Select a report, for example *Monitored Application Summary by Application Lists* .
3. Click **Generate Report** .
4. To view the report click **View Last Result** .

A new browser window or tab opens and displays the report.

Defining Applications to Use in Application Management

You can manually define an application for management by adding it to the **Custom Applications** . Once it is defined there it can be added to all types of managed as well as for the licensed applications. Applications can be defined in a number of ways from different locations in the console. For our first step we select the easiest method, that is, adding the application from the **Software Inventory** to the **Custom Applications** :

1. Go to the **Device Topology** node and find the device which contains all the software applications you want to define, for example the master server.
2. Select the device's **Inventory > Software > Scanned Applications** node.
3. Find the software application to be managed in the table in the right window pane, for example *Adobe Reader* , and select it.
4. Click **Add as Managed Application** .
5. Click **OK** in the **Confirmation** dialog box.
6. If you already have an application list defined another **Confirmation** windowdisplays. Click **No** .
7. Go to the **Application Management** node and select the **Custom Applications** subnode.Here you will now find an entry for **Adobe Reader** in the list. If this is not the case yet refresh the view.
8. Repeat this procedure to add some more applications for the examples to follow, e.g. add the *Pinball* game and the *Windows 7* operating system to the list.

All applications added here are now ready for usage by the application monitoring and software license management functionalities.

Configuring Application Monitoring

You can specifically configure a number of parameters to adapt certain aspects of the behavior of the application monitoring functionality to your requirements for your device population. This is done via an operational rule.

1. Click the **Wizards > Operational Rule Creation** menu item.
   The **Operational Rule Creation Wizard** dialog box appears.

2. In the **Name** text box enter Application Monitoring Configuration and click **Next** .
3. In the **Steps** view click **Add Step** .
   The **Select a Step** dialog box appears.
4. In the **Available Steps** group box select **Agent Configuration > Application Monitoring Module Setup** and click **Add** .
   The **Properties** dialog box appears.
5. Fill in the following text boxes:
   - **Verification Interval (sec)** : Increase/decrease the number of seconds to modify the interval at which all managed applications, that is all monitored and prohibited applications, are verified for execution.
   - **Stop Application if Prohibited** : Clear this check box if prohibited applications are *not* to be automatically terminated.
   - **Popup Window after Application Termination** : Clear this check box if NO message box is to be displayed to the local user after a prohibited application was stopped.
   - **Event Creation Delay for Unterminated Monitored Applications (hours)** : If required increase/decrease the number of hours after which an event is created, even if the launched application has not yet been terminated. In this case the end date of the generated event will be the same as the start date. Once the application is terminated a new event will be generated with the proper end date filled in.
   - **Local Image File Path (bmp only)** : This parameter allows you to use another image than the default one provided by CM in the notification message box of a terminated prohibited application. Enter into this field the path to the image file which must be of type .bmp. If the image cannot be found, that is, because it is of another type, or it is too small, the default BCM image is used. If the image is too large it is cropped to fit the window. The default size of the BCM image is 460x310 pixels.
   - **Popup Window Message Text** : Enter into this text box the message that is to be displayed in the message box that is to be displayed to the local user after a prohibited application was stopped if you have a teriorly activated this option.
6. Click **OK** to confirm the step and its parameter definitions.
   The dialog closes and the step is listed in the right group box.
7. Click **OK** to add the step to the operational rule.
8. Click **Finish** to create the new operational rule.
   The **Confirmation** dialog box appears.
9. Click **Yes** to distribute the operational rule and continue with the distribution wizard.

   > After creating the operational rule you distribute it to devices in your network.

   The **Operational Rule Distribution Wizard** wizard appears.
10. In the first window leave all preselected values and click **Next** .
11. In the **Assigned Targets** window click **Assign Device** .
    The **Assign to Device** dialog appears.

12. Select the device group to which you want to assign the operational rule, for example *All Devices* and click **OK** .
    The dialog closes and device group is listed.
13. Click **Finish** to distribute the operational rule.
    The dialog box closes and the **Confirmation** dialog box appears.
14. Select the **Go to Operational Rule** radio button and click **OK** .
    The dialog closes and the focus of the console is moved to the device group assigned to the new operational rule.

The operational is now being distributed to all assigned targets. You can follow the distribution in the window to which the focus of the console was switched via the **Status** column.

> **Note:**
>
> If you want to use another image you need to ensure that it is available on ALL target devices; to ensure that you can distribute it, for example, via a separate operational rule or you can add the steps **Directory and File Handling > Check for File** , to verify if this file already exists in this location and **Software Distribution > Install Package** to copy it there if this is not the case.

> **Note:**
>
> You can also configure a device individually by selecting the **Device Topology > Your Device > Agent Configuration > Module Configuration > Application Monitoring** node and editing the parameters of the device directly.

Adding an Application from a Device

To add an application via an executable file of a specific device proceed as follows. Be aware, that an application which does not provide all information required for a managed application cannot be added as such, in this case the following menu option will not be accessible.

1. Select **Add Application from Device** .
   The **Select a Device** window opens on the screen.
2. Select from one of the proposed lists the device on which the desired executable file is located. You must provide access rights to this device if you have not yet done so via another of the console‘s functionalities.
3. Click **OK** at the bottom of the window to confirm the device.
   Now the **Select Executable File** window appears displaying the directory structure of the selected device.

4. Find the executable file in the hierarchy and select it, then click **OK** .
   The **Add User Defined Application** window appears. It provides all the data it can find on the selected executable apart from a name which you need to complete.
5. Click **OK** at the bottom of the window to confirm.
6. If you are defining a **Protected Application** a **Properties** window displays now on the screen, in which you need to define the selfhealing options as previously explained under .

Monitoring Managed Applications

All types of managed applications can be monitored via the respective subnode under the **Agent Configuration** node of the targets.

- Monitored and prohibited applications are monitored under the Managed Applications node.
- Protected application are monitored under the Selfhealing node.

For more information, see Managing Application Lists.

Managing custom applications

The **Custom Applications** view is a container for all applications which are to be managed on the devices of your infrastructure, that is to say they are to be either monitored for performance, restricted in their execution or defined for self-healing. These applications may be listed directly under the node or be sorted in folders for easier classification.

- Adding from the Software List
- Adding an Application from the Software Inventory List

Adding from the Software List

Applications can be added to the list of managed applications via the list of installed software generated by the software inventory. Software applications which do not provide all information required for a managed application will in this case not appear in the list here. To add an application to the list of managed application from the general software inventory list, proceed as follows:

1. Select **Edit > Add from Software Inventory** .
   The **Add from Software Inventory** dialog box appears on the screen. This window appears the list of applications found in the software inventory that can be used for the managing of applications.

> **Note:**
>
> Make sure not to select an application of type Add/Remove Program or MSI, these types can be added to the application catalogue but they cannot be managed via the Application lists as vital information is missing.

2. In this window you can select your application in one of the following different fashions:
   - The **All** tab displays the list of available applications in the form of a table with its name and version number.
   - The **Search** tab allows you to search for a specific application either by its name, version or type attribute. Select the respective value from the **Search Fields** list. Then enter the words which you are sure the respective attribute contains in the **Value** box and select the appropriate operator from the preceding **Operator** box and then click **Find** . The search will query all application name and the following table displays all those which match your condition.
3. Select one or more applications to be added to the list of managed applications.
4. Click **OK** at the bottom of the window to confirm the data for the new managed application or click **Cancel** to abandon without modifications and to close the window.

Adding an Application from the Software Inventory List

1. Select **Add from Software Inventory** .
   The **Add Applications from Software Inventory** dialog box appears on the screen, displaying all applications found in the software inventory.
2. In this window you can select your step in following different fashions:
   - The **All** tab displays the list of available applications in the form of a table with its name and version number.
   - The **Search** tab allows you to search for a specific application either by its name, version or type attribute. Select the respective value from the **Search Fields** list. Then enter the words which you are sure the respective attribute contains in the **Value** box and select the appropriate operator from the preceding **Operator** box and then click **Find** . The search will query all application name and the following table displays all those which match your condition.
3. Select one or more applications to be added to the list of monitored applications.
4. Click **OK** at the bottom of the window to confirm.
5. If you are defining a **Protected Application** a **Properties** window displays now on the screen, in which you need to define the selfhealing options as explained in the Protected Application Fix Details topic.

Managing software catalog

The **Software Catalog** lists all software that was found on the selected device sorted by the product it is part of. You can filter the table according to the following criteria:

Parameter	Description
Only Show Discovered Software	Check this box if the catalog is only to show software of its complete catalog that was discovered on at least one device within your network. If you leave this box unchecked, this list will show all software that is included in the catalog.
Criterion	

Parameter	Description
	Select in this drop-down box according to which of the available criteria you want to sort the table. You can sort according to all criteria.
Operator	Select in this drop-down box the operator that defines how the value to be defined in the next box is to be evaluated.
Value	Enter the expression that you want to search for in the table.

The software catalog table provides the following information about all items:

Parameter	Description
Product	This column shows the names of all products that might be installed on any of the devices in your network. A product in this case is any type of software application, tool or suite.
Manufacturer	This field displays the name of the manufacturer of the respective product.
Category Name	This field displays which type of software the product belongs to, for example, if it is a browser, an application server software, and so on.
Status	This field shows the status, as which it is currently viewed in CM , that is, if it is a product that is currently managed, either supported or unsupported, or if you have not yet dealt with it (Unidentified)

Changing a license unit status

The software products contained in the Software Catalog initially all have the same status, that of `Unidentified` . This indicates that the product is part of the catalog, probably was found on devices in your network, but has not yet been treated. After you have gone through the list of products the catalog provides and identified those that are supported in your organization you can change the status of the selected units as follows:

1. Select the **Application Management > Software Catalog** node in the left window pane.
2. Select the product in the table.
3. Right-click your mouse on it and then select **Change Status** and the desired status option:.
   - `Managed - Supported` , if this product is part of the software inventory of your organization, or
   - `Managed - Unsupported` , if none of the software items of a product are used by any of the devices in your environment.

The status of the product is changed directly.

Managing schedule templates

Applications can either be prohibited from use at all times in which situation the prohibited application can directly be assigned to the targets without further limitation. However, it is also possible to deny the use of application only at specific times and allow the users to launch these,

for example for their private use at lunchtime or after regular working hours. The same is true for monitored applications, protected applications, however, are protected all the time and cannot be assigned to a schedule. Schedule templates are a sort of a timetable of time-slots in which the application usage may be denied or allowed or monitored.

Schedule template folders are created as organizational containers for the different types of templates which are to be assigned to the prohibited/monitored applications. They can contain any number of custom-made schedule template folders and schedule templates for the management of the devices and their applications in your system.

The following topics are provided:

- Creating a Schedule Template
- Defining application time-slots

Creating a Schedule Template

To add a new schedule template to restrict the execution of applications, proceed as follows:

1. Select **Edit > Create Schedule Template** .
   The **Properties** dialog box appears.
2. Enter the name for the new template into the **Name** field.
3. Click **OK** at the bottom of the window to confirm the data for the new schedule template.

Defining application time-slots

Schedule templates are specific schedules which are defined to regulate the use of prohibited applications and define the monitoring of others. As the name template indicates this a planning which can be used for a number of applications which have certain criteria of use in common, such as personal software, which, for example, might be forbidden to be used during regular working hours, but allowed before and after work hours and during lunch time, or a sales software, that travels around the world on the laptops of the sales personnel, is to be monitored.To define or modify the times at which an application can be used or forbidden, proceed as follows. If you assigned a predefined schedule template and want to individually modify it, you can do so. However, you are loosing the link with the predefined template, that is, the **Selected Schedule Template:** box then displays **None** , as no predefined template is assigned to the application any more.

1. Click the box which is to be edited.

   > You can also select a range of boxes by dragging your mouse button over the desired range.

2. Click **Edit > Define Time-slot** to allow the application to execute in the selected time range or **Edit > Deny Time-slot** to deny it for those.

3. Repeat these steps for all other slots or ranges to be defined or modified.

Managing Application Lists

An application list collects all applications that are to be managed in a specific way, that is, their usage is to be monitored, they are to be protected, that is, they are in a position to heal themselves, or their usage is forbidden. An application list can only execute one type of operation, that is, it cannot monitor and prohibit applications at the same time.

The following topics are provided:

- Creating an Application List
- Adding applications to the list
- Monitored Applications and Prohibited Applications
- Protected Application
- Selfhealing applications

Creating an Application List

To add a new application list of any type to manage applications, proceed as follows:

1. Select **Edit > Create Application List** .
   The **Properties** dialog box appears.
2. Enter the name into the respective text box and select the type of application list to create from the drop down box.
3. Click **OK** at the bottom of the window to confirm the data for the new application list.

Adding applications to the list

The **Applications** tab shows the list of all individual applications which are part of this list. The displayed information varies according to the application list type:

- Add Application from Device
- Add User Defined Application

The **List** tab displays all applications that have been selected for managing on the local client, monitored as well as prohibited applications. This list only contains those applications of which the assignment/update was received, not applications with another status.

It shows the following information about the listed applications:

Parameter	Description
Application Name	The name of the managed application, such as it is either found in the software inventory translation file or via MSI.
Application Version	he version number of the application as provided by the software inventory.
	The type of managed application, that is, if the application is monitored or prohibited.

Parameter	Description
Management Type	

Add Application from Device

To add an application via an executable file of a specific device, proceed as described in the following. Be aware, that an application which does not provide all information required for a managed application cannot be added as such, in this case the following menu option will not be accessible.

1. Select **Edit > Add Application from Device**  .
   The **Select a Device** window opens on the screen.
2. Select from one of the proposed lists the device on which the desired executable file is located. You must provide access rights to this device if you have not yet done so via another of the console‘s functionalities.
3. Click **OK** at the bottom of the window to confirm the device.
   Now the **Select Executable File** window appears displaying the directory structure of the selected device.
4. Find the executable file in the hierarchy and select it, then click **OK** .
   he **Add User Defined Application** window appears. It provides all the data it can find on the selected executable apart from a name.
5. Make changes to these if required.
6. Click **OK** at the bottom of the window to confirm.
   A confirmation window appears if the selected application does not yet exist in the application catalogue to which it will automatically be added as well.
7. If the application list is already assigned to a device or group, another Confirmation window appears in which you may define to directly reactivate the application list for its assigned objects.

Add User Defined Application

To add a user defined application to the list of managed applications, proceed as follows:

1. Select **Edit > Add User Defined Application**  .
   The **Add User Defined Application** dialog box appears.
2. Enter the necessary data into the respective boxes.
3. Click **OK** at the bottom of the window to confirm the data.
   A confirmation window appears if the selected application does not yet exist in the application catalogue to which it will automatically be added as well.
4. If the application list is already assigned to a device or group, a Confirmation window appears in which you can define to directly reactivate the application list for its assigned objects.

Monitored Applications and Prohibited Applications

If the application list is of type **Monitored Application** or **Prohibited Application** this tab displays the following information about the members:

Parameter	Description
Name	The fields of this column list the names of all applications that are a member of the currently selected application list.
Version	The version number of the application.
License Count	The number of valid licenses for the application. When the application is newly added to the list this value is set to 0 by default.
Installed Count	The number of times the application is installed on the devices in the network.
File Name	The name of the executable file of the application.
File Checksum	The checksum of the executable file of the application.
File Size	The size of the executable file of the application.

Protected Application

If the application list is of type **Protected Application** this tab displays the following information about the members:

Parameter	Description
Name	The fields of this column list the names of all applications that are a member of the currently selected application list.
Local Backup Copy	Displays if a copy of the protected application is to be stored on the local device.
Protect Sub-directories	This value defines if the protection scheme includes the sub-directories of the application directory. This may be applicable for larger applications having sub-directories with do not only contain user created but application data, such as libraries or filters.
Include File Types	By default all files in the main directory and the sub-directories if specified are included. If you do not want to include all files enter into this field the list of file extension which are to be included in the selfhealing package. The files are a comma separated list with wildcard characters, such as **.exe,**.dll,**.bat, and so on If you are limiting the files to be protected they should not include any type of file that is user created, such as *.doc,**.txt, and so on, as newer files might be erased by older ones in case of a selfhealing operation. You can also exclude these via the next parameter.
Exclude File Types	By default all file types are included for protection and selfhealing. In this field you can specify a list of file types which are not to be protected and thus included in the selfhealing package. The files are a comma separated list with wildcard characters, such as **.txt,**.doc,*.tmp, and so on. For example, in this field you might want to limit any type of file that is user created, such as Word documents, Excel spreadsheet, and so on, as newer files might be erased by older ones in case of a selfhealing operation.

Selfhealing applications

The **Selfhealing** node displays information about the applications which are currently defined as protected applications on the local client. This functionality is only applicable to Windows and Linux devices.

The following topics are available:

- Selfhealing application list
- Protected application fix details

Selfhealing application list

The **List** tab displays all applications that have been selected for selfhealing on the local client. This list only contains those applications of which the assignment/update was received, not applications with another status.

It shows the following information about the listed applications:

Parameter	Description
Application Name	The name of the managed application, such as it is either found in the software inventory translation file or via MSI.

Protected application fix details

This tab provides a log of sorts about the protected applications on the local device. It logs an entry in the table every time a file of an application was repaired with the following information:

Parameter	Description
Event Date	The date and time at which the event about the protected application was logged by the local agent.
Application Name	The name of the protected application.
Application Version	The version number of the protected application.
Fixing Time	The date and time at which the application was repaired on the local client.
Fixed File	The name of the file that was repaired.
Connected User	This field displays the name of the user that was connected at the time when the application was repaired.
Domain	The name of the domain of the connected user. If the network does not have domains, the device name will be displayed here.

Managing software licenses

Managing software licenses include the following operations:

- Getting started with managing software licenses
- Creating a Licensed Software Based on a Query

- Evaluating the Licensed Software for Authorized Software Installations
- Defining a Licensed Software and Monitoring it
- Attaching Files to a Licensed Software
- Configuring Software License Management

Getting started with managing software licenses

Automatic software asset management in Client Management is performed via Application Management. The system will automatically discover applications that are licensable and allow the users to determine license units they would like to manage and track usage of.

When these are assigned to devices or device groups, they are evaluated with regards to the applications installed to define their compliance with a specific license.

The main object of this functionality is the *license unit* . It represents an application, suite, or product that needs tracking, because it requires one or more valid licenses for its execution. It can be populated and evaluated in the following different ways:

- **Scanned Application** :
  the license unit is populated with individual software applications, that are under the same license scheme.
- **Query** :
  The license unit is populated via the result of a query of type *Device* , that is, all devices that answer the software criteria specified in the query.
- **Software Catalog** :
  the license unit is populated with applications of the Software Catalog, that are under the same license scheme.

> **Note:**
>
> You should have Microsoft Windows 7 and Office or some of its applications installed, because the following steps are based on them. However, you can also execute these examples by replacing them with another operating system version and group of applications that you installed on your devices.

Related topics

- Automatically creating a licensed software populated via the Software Catalog
- Creating and evaluating the licensed software
- Creating licensed software via the Software Catalog with applications as license units
- Analyzing the evaluation results
- Manually creating and populating a licensed software via software inventory

Automatically creating a licensed software populated via the Software Catalog

In this first example we create a licensed software for the *Microsoft Office 2010* product that is populated via the Software Catalog. A wizard allows you to execute all the necessary steps at the same time, selecting the software from the Software Catalog:

1. Creating the licensed software and defining the respective licenses.
2. Assigning the licensed software to a group of devices.
3. Evaluating the licensed software based on the data of the assigned group.
4. The only step that remains to be done afterwards is to interpret the evaluation results.

Creating and evaluating the licensed software

The **Application Management Wizard** provides you with two creation possibilities, an automatic and a manual one. In this first exercise we are using the automatic option.

> **Note:**
>
> For the following example an specific license is required, the **Software Catalog** as well as possibly the **Software Catalog Updates** license to keep the catalog up to date. If you do not have this license(s) go to the next example, Manually creating and populating a licensed software via software inventory which explains you how to create your licensed software object without the software catalog.

> **Note:**
>
> Before you start on your licensed software ensure that you have a device group ready that is to be evaluated for license compliance. If not you need to create one first.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window the automatic option is preselected in this step, therefore click **Next** right away.
3. In the **Add License Units** window click the **Add license units from the software catalog** icon above the list box.
4. From the drop-down list below the **Only Show Discovered Software** box select the *Microsoft Corporation* option.
5. The following list box display all Microsoft software that was found on at least one of the devices of your network that were already inventoried. Find the *Microsoft Office 2010* entry or any other entry if you are using another software for this example and check its box. The unit is automatically added to the list of **Selected License Units** to the right.

> **Note:**
>
> To deselect a license unit, clear its box in the right pane under the **Selected License Units** .

6. Click the **OK** button to confirm.
7. Click the **Quantity of Licenses** box and enter the number of licenses you purchased for this unit.
8. Click the **Next** button.
9. In the **Assigned Devices** window click the **Add Device** icon on top of the list box.
10. Select the group containing your target devices from the list.
11. Click **OK** .
12. Click **Finish** .
13. In the **Confirmation Yes** .
    The focus of the console is moved to the newly created object.

The software license object is created, assigned to a device group and defined as a group that is *not* authorized to have this software installed.

Creating licensed software via the Software Catalog with applications as license units

In this example we create a licensed software using the Software Catalog, but we populate it manually and select applications as the license units, in our example, different Acrobat versions.

> **Note:**
>
> For the following example an specific license is required, the **Software Catalog** as well as possibly the **Software Catalog Updates** license to keep the catalog up to date. If you do not have this license(s) go to the next example, Manually creating and populating a licensed software via software inventory which explains you how to create your licensed software object without the software catalog.

> **Note:**
>
> Before you start on your licensed software ensure that you have a device group ready that is to be evaluated for license compliance. If not you need to create one first.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window, select the **Configure a Licensed Software** radio button and then click **Next** .

3. In the **Licensed Software** window, enter a name for the new licensed software in the **Name** box, for example, **Adobe Acrobat version 9** .
4. *(Optional)* Enter in the **Category** box the category to which Acrobat belongs, for example, **Publishing** . If the category to which the software belongs already exists, you can directly select it.
5. *(Optional)* By default all newly created objects are created directly under the main object node. To create it in any other folder click the icon to the right of the field (...). Select the desired folder from the folder hierarchy. If the desired target folder does not yet exist you can also create new folders. To do so first select the parent folder of the new one and then select click the **New Folder** icon below the hierarchy. Enter the desired data into the respective fields and then click the **OK** button at the bottom of the window to confirm the new folder. Select the target folder and click the **OK** button to confirm and to close the window..
6. Click **Next** .
7. In the **License Units** window click the **Add license units from the software catalog** icon above the list box.
8. From the drop-down list below the **Only Show Discovered Software** box select the **Adobe Systems Incorporated** entry.

   Clear the **Only Show Discovered Software** box, if you want to add Acrobat versions to this list, that are not yet installed in your environment.

   The list box displays now all Adobe software, either only the products installed in your environment or all Adobe products.
9. Find the **Adobe Acrobat** entry or any other entry if you are using another software for this example and click its name.
10. Check the boxes for the versions, that you want to add as license units, such as **Adobe Acrobat 9.0** , **Adobe Acrobat 9.3** and **Adobe Acrobat 9.4** .
    The units are automatically added to the list of **Selected License Units** to the right.

    Note:

    To deselect a license unit clear its box in the right pane under the **Selected License Units** .

11. Click **OK** .
12. Click **Next** .
13. Click **Add License** .
    The **Add a License** dialog box appears.
14. Enter the required information in the respective boxes.

> If you do not have the information for all boxes, you do not need to fill everything. But you should at least fill in the **Vendor** , **License Type** , **Product Serial Number** and **Quantity** information.

15. Click **OK** .
16. Click **Next** .
17. In the **Assigned Devices** window click the **Add Device** icon on top of the list box.
18. Select the group containing your target devices from the list.
19. Click **OK** .
20. Click **Finish** .
21. In the **Confirmation Yes** .
    The focus of the console is moved to the newly created object.

The software license object is created, assigned to a device group and defined as a group that is *not* authorized to have this software installed.

Analyzing the evaluation results

The overall results of a license compliance evaluation are displayed in the **Dashboard** tab of the licensed software via a number of charts.

1. Select the **Software License Management** in the left tree hierarchy.
2. Select the subnode for the licensed software, for example *Microsoft Office 2010* in the left window pane.
3. Select its **Dashboard** tab in the right window pane.
   In this view four charts are displayed which provide information about the licensed software and all its members and their respective compliance. Balloon tips are available for each chart displaying explanations.
4. Move your cursor over the **Licenses** chart:
   This chart displays the situation of the licensed software with regards to the purchased license(s) for all assigned objects, that is, all device groups as well as all individually assigned devices. It displays the absolute numbers for the different license status values:

- **Installed** / **Exceeded** :
  the number of remaining licenses. If no more licenses are left, this bar is labelled **Exceeded**
- **In Use** :
  total number of licenses that were used at least once. This will always be *0* if you are not monitoring the usage of the software via an application list. If you move the cursor over one of the bars it displays the exact number for each status.

1. Now move your cursor over the **Authorization** chart:
   Here you can see the repartition of the assigned devices according to their license authorization. These numbers are the cumulative of all devices that are assigned via one or more groups and includes also individually assigned devices. If you move your cursor over a pie part a label displays the number of devices on which the software is authorized, respectively unauthorized with the corresponding percentage value.
2. Now move your cursor over the **Compliance** chart:
   In our example the general status is `Compliant` therefore all devices are compliant on which the software is not installed. Any devices on which the software is installed are `Not compliant` . A label displays the number of compliant/not compliant devices with the corresponding percentage value.

> **Note:**
>
> The **Usage** chart is of no interest yet as we have no data yet to follow up the software usage over some time.

Manually creating and populating a licensed software via software inventory

A licensed software can also be populated via the software inventory instead of using the Software Catalog. For this example we create a licensed software for *Microsoft Office 2010* again that is populated manually with the respective applications.

> **Note:**
>
> Before you start on your licensed software ensure that you have a device group ready that is to be evaluated for license compliance. If not you need to create one first.

1. Select the **Wizards > Application Management** menu item or launch it directly from the dashboard.
2. In the **Introduction** window select the **Configure a Licensed Software** radio button.
3. Click **Next** .
4. In the **Licensed Software** window enter *Microsoft Office 2010* into the **Name** and *Office Applications* into the **Category** field.
5. From the **Evaluation Type** drop-down list select the **Scanned Applications** option.
6. Click **Next** .
7. In the **License Units - Queries - Applications** window click the **Add from Software Inventory** icon.

> To find the applications being part of Microsoft Office enter all or part of their name into the **Value** field, e.g. *Excel* and the click **Find** .

8. Repeat *points 1 - 3* for all other applications that are part of your Microsoft Office license, e. g. Word, Publisher, FrontPage, and so on.
9. Click **Next** .
10. In the **Licenses** window click **Add License** and enter all the necessary information of your license in the respective boxes.
11. Click **Next** .
12. In the **Assigned Devices** window click **Add Device Group** on top of the list field.
13. Select the group containing your target devices from the list.
14. Click **OK** .
15. Click **Finish** .
16. In the **Confirmation** dialog box, click **Yes** .

The software license object is created, assigned to a device group and defined as a group that is *not* authorized to have this software installed.

Creating a Licensed Software Based on a Query

The query on which the licensed application is based must be of type *Device* and finds all devices on which one or more specific software applications are installed. These software criteria must be specified in the query. The resulting list of devices will then be compared, matched and evaluated with the devices assigned to the licensed software via their groups or individually.

Creating a query-based licensed software requires the following steps:

1. Creating the query on which the object will be based.
2. Creating the licensed software, assign it to the query, add the respective licenses and assign it to a group of devices.
3. Evaluating it based on the data of the query and the assigned group.
4. Interpreting the evaluation results.

Steps 2 to 4 are the same as those for an software catalog based licensed software.

The following topics are included:

- Creating a Query Finding All Windows 7 Operating Systems
- Creating, Defining and Assigning a Query-Based Licensed Software

Creating a Query Finding All Windows 7 Operating Systems

Using a query allows you for example to find all devices on which the different flavors of an operating system are installed, that is, Windows 7 Professional, Windows 7 Enterprise, and so on.

To create a licensed software using a query, we must first create such a query.

1. Select the **Queries** node in the left tree hierarchy.

2. Click the **Create Query** icon.
   The **Properties** window appears.
3. Enter the name of the new query into the **Name** field, e.g. *Windows 7 Devices* and click **OK** .
4. Now double-click the query in the table to access it.
5. Select the **Criteria** tab in the right window pane.
6. Click the **Add Criterion** icon.
   The **Select Criterion** window appears.
7. Select the criterion **Operating System** .
8. In the following **Operator** drop-down box select the value **Contains** and enter *Windows 7* into the **Value** field.
9. Click the **Find** button.
10. Select the *Microsoft Windows 7* operating systems in the **Search Criteria** pop-up and click **OK** .
11. Click the **Add** button.
    The selected criterion is added to the list of **Selected Criteria** to the right.
12. Click **OK** to confirm the new query content and to close the window.
13. Activate the query by selecting the option **active** in the **Query Status** drop-down list of the preceding table.

The query is not created and active and can be used with the application license management.

Creating, Defining and Assigning a Query-Based Licensed Software

To create the licensed software process as follows:

1. Select the **Wizards > Application Management** menu item.
2. In the **Introduction** window select the **Configure a Licensed Software** radio button.
3. Click **Next**
4. In the **Licensed Software** window enter *Microsoft Windows 7* into the **Name** and *Operating Systems* into the **Category Name** field.
5. From the **Evaluation Type** drop-down list select the **Query** option.
6. Click the **Next** .
7. In the **License Units - Queries - Applications** window click **Add Query** .
8. Select the query *Windows 7 Devices* from the list (located in the **Operating Systems > Windows** folder).
9. Click **OK** .
10. Click **Next** .
11. In the **Licenses** window click the **Add License** and enter all the necessary information of your license in the respective boxes.
12. Click **OK** to confirm and close the window.
13. Click the **Next** button.
14. In the **Assigned Devices** window click the **Add Device Group** icon on top of the list field.
15. Select the group containing your target devices from the list.
16. Click **OK** .

17. Click **Finish** .
18. In the **Confirmation** dialog box, click **Yes** .

The software license object is now created, assigned to a device group and defined as a group that is *not* authorized to have this operating system.

To evaluate and then analyse the results Refer to the Analysing the Evaluation Results topic.

Evaluating the Licensed Software for Authorized Software Installations

To find the devices on which the applications are authorized to be installed but are *not* installed the status of the group must be changed.

1. Reselect the **MS Office > Assigned Objects > Device Groups** node in the left window pane and the group entry in the table to the right.
2. Click the **Change Status** icon.
3. Click **Yes** in the **Confirmation** dialog box.
   The status is now changed to **Authorized** .
4. Click **Evaluate** .
   The group members will be immediately checked if they have the software installed.
5. To view the evaluation results select the node of the assigned group subnode in the left window pane.
   This view displays all members of the group and the interesting value here can be found in the column **Compliance Status** (the status of this column depends on the values of the **Status** and **Installed** columns):

- The value `Compliant` indicates in this case that the software is installed on this device and that it is allowed to have this software installed.
- The value `Not compliant` indicates in this case that the software is installed on the device but the device is not allowed to have it installed.
- The value `Not installed` indicates that the software is not installed on this device even though it is allowed to have it installed.

Defining a Licensed Software and Monitoring it

The automatic licensed software creation wizard also allows you to specify the new software for monitoring. To do so, proceed as follows:

1. Select the **Wizards > Application Management** menu item.
2. The automatic option is preselected in the **Introduction** window, therefore click **Next** right away.
3. In the **License Units** window click the **Add License Units** icon above the list box.
4. From the drop-down list below the **Only Show Discovered Software** box select the *Adobe Systems Incorporated* option if it is not already preselected.
   The following list box will now display all Adobe software that was found on at least one of the devices of your network that were already inventoried.

5. Select for example the *Adobe Reader* entry or any other software.
6. Click the **Add** button.
   The selected software is now added in the right page.
7. Click the **OK** button to confirm.
8. Enter the number of licenses you purchased for this software into the preselected **Quantity of Licenses** box.
9. Then check the box in the **Monitor** column.
10. Click the **Next** button.
11. In the **Assigned Devices** window click the **Add Device Group** icon on top of the list box.
12. Select the group containing your target devices from the list.
13. Click **OK** .
14. Click **Finish** .
15. In the **Confirmation** dialog box, you have the choice to either go to the monitored application or the licensed software. Check the desired box and click **Yes** .

The software license object is created, assigned to a device group and defined as a group that is *not* authorized to have this software installed.

Refer to the Analysing the Evaluation Results topic to interpret its results.

Attaching Files to a Licensed Software

If you have further information stored in files, such as the file containing the license you can attach these to the licensed software object. This information must not be added before the evaluation as it is not taken into account for any calculations, it has purely informative character.

1. Select the **Attachments** tab of a licensed software.
2. Click **Add Attachment** .
   The **Add an attachment file** window appears.
3. Select the file and click **Open** .
4. To add more attachments repeat points 2 and 3 until all attachments are added.

Configuring Software License Management

Contrary to the application monitoring the software license management is configured in its own **Configuration** node. Here you can specifically configure a number of parameters to adapt certain aspects of its behavior to your requirements for all devices of your population.

1. Select an entry in the table to the right and click **Application Management** .
   The **Properties** window appears.
2. Select the **Application Management > Software License Management > Configuration** node.
3. Make the required changes to the available parameters:

Parameter	Description
Number of days before sending a license expiring alert	Defines the number days that may remain until the license expires to send an alert.

Parameter	Description
License under installation percentage threshold to send an alert	Defines the percentage of uninstalled software licenses under which an alert is sent. This means that if the threshold is set at 50% and 51% of the licenses are installed no alert is sent. If only 50% or less of the available licenses are installed an alert is generated.
Exceeded license usage percentage threshold to send an alert	Defines from which percentage value onwards of used licenses an alert is sent, that is, if the threshold is defined at 80% and 80% or more of the available licenses are used, an alert is sent. If only 79% of the licenses are used no alert is generated.

4. Click **OK** .

The modifications to the parameters are applied immediately and are from now on applicable to all existing software license units.

Modifying the licensed software evaluation schedule

Under the **Configuration** node you can also modify the schedule that manages the evaluation frequency of all defined licensed software units.

1. Select the **Assigned Schedule** tab.
2. Select the entry in the right window pane.
3. Click **Properties** .
   The **Scheduler** window appears.
4. Make the required modifications in the available options.
5. Click **OK** to confirm.

The new schedule takes effect immediately.

Managing licensed software

A licensed software collects all applications that are subject to a specific license. This might just be one single application, it might be a group of applications, such as MS Word, MS Excel, etc., which are part of the Microsoft Office Suite or it might be all different flavors of an operating systems, such as Windows 7. After the licensed software is defined it can be assigned to individual devices or device groups for license evaluation. This evaluation verifies if the assigned devices are in compliance with the license specifications, that is, if the application is only installed on those devices it is supposed to.

- Configuring license management
- Creating a licensed software
- Evaluating assigned objects for license compliance
- Understanding units of a licensed software
- License unit applications
- Assigning a query to a software license
- Licenses

- The Licensed Software Dashboard
- Attachments of a licensed software

Configuring license management

The Configuration node provides you the possibility to configure some specific behavior of the software license management functionality via its tabs. The following parameters can be defined for the software license management:

Parameter	Description
Number of days before sending a license expiring alert	Defines the number days that may remain until the license expires to send an alert.
License underinstallation percentage threshold to send an alert	Defines the percentage of uninstalled software licenses under which an alert is sent. This means that if the threshold is set at 50% and 51% of the licenses are installed no alert is sent. If only 50% or less of the available licenses are installed an alert is generated.
Exceeded license usage percentage threshold to send an alert	Defines from which percentage value onwards of used licenses an alert is sent, that is, if the threshold is defined at 80% and 80% or more of the available licenses are used, an alert is sent. If only 79% of the licenses are used no alert is generated.

Modifying the evaluation schedule

The schedule specified in this view manages the evaluation frequency of all defined licensed software objects.

1. Select the entry in the right window pane.
2. Click **Properties** .
   The **Scheduler** window appears.
3. Make the required modifications in the available options.
4. Click **OK** to confirm.

The new schedule takes effect immediately.

Creating a licensed software

To add a new licensed software to manage licensed applications, proceed as follows:

1. Select **Edit> Create Licensed Software** .
   The **Properties** dialog box appears.
2. Enter the name into the respective field.
3. Then enter the **Category** for the licensed software.
4. Select the **Evaluation Type** for the object.
5. Click **OK** at the bottom of the window to confirm the data for the new licensed software.

The following topics are provided:

- Importing New Software Licenses

- CSV Import File Format

Importing New Software Licenses

Instead of manually updating or adding individual licenses, you can also update/add several licenses at the same time by importing them via a csv file. For more information about the format of this file see the CSV Import File Format topic or click **Sample Import File with Instructions** in the **Import License Data** window.

1. Select **Edit > Import License Data** .
   The **Import License Data** windowdisplays.
2. Click the **Browse** button to locate the csv file containing all the license information.
   An **Open** windowdisplays.
3. Browse the directory hierarchy to the file's location and select it.
4. Click **Open** .
   The structure of the selected file will now be imported into the **Field Mapping** box and display all fields that were recognized in the left column.
5. To use an existing field mapping click the **Save as Default** arrow button and select the **Load Default** option.
   The default mapping will be applied to all fields.
6. To change the mapping of a field select the cell in the **Destination Record** column.
   The cell will change into a drop-down list box.
7. Select the desired destination field.

   Each destination record can be mapped to only ONE source field.

8. To save the mapping as the default for further imports click the **Save as Default** button on top of the table.
   A confirmation windowdisplays.
9. Click **Yes** .
10. Click **OK** to confirm the mapping.
    The **Select Licensed Software from List** windowdisplays. It displays the list of all licenses found in the csv file.
11. If you are adding new licenses select **Add imported items to licenses** .

    In this case the licenses with the same name as already existing licenses will be added as new ones to the existing licenses software item.

12. If you are updating existing licenses select **Replace all existing licenses with imported data** .

> Be aware, that in this case the import will overwrite all existing license data with the new data of the file. If you made manual changes to the license that are not included in the csv file these will be lost.

13. Select the licenses to add or update with the new data. You can select more than one entry by holding the CTRL key. To select all listed licenses click **Select All** .
14. Click **OK** .
    The **Import Results** appears. It provides the list of licenses that were imported togehter with their import status.
15. Click **Close** .

CSV Import File Format

The file via which licenses can be imported is a simple csv file listing all fields and their data that are to be imported. It must contain the comma separated list of field names in the first line and one line per licensed software to be added/updated with the comma separated list of values. The list must not necessarily contain all available values.

The CSV Sample File

To display the csv sample file click **Sample Import File with Instructions** in the **Import License Data** window.

The file shows you via its two tabs the required content of the csv file and its format as well as an example on how this could look.

- How To
- Data

How To

The **How To** tab provides you with some general explanations and the list of all fields that exist for licensed software:

Column	Description
Column Name	This column lists all field names that are used for the licensed software items. You can use these names for your columns or chose your own names with the exception of the the first field name, `LicensedApplicationsName` , which must always be called that and is mapped to the **Name** field. If you are using the default names shown here, they will be automatically mapped to their target fields in the import.
Description	The fields of this column provides some explanation on the respective field content to simplify their mapping.
Type	These fields show the datatype that is expected in the respective field.
Expected Values	These fields provide more information about the expected values, such as their expected format (date format) or which possible values are available for a specific field, and so on, where applicable.

Data

The **Data** tab provides you with an example of how the csv file might look when opened in MS Excel.

Evaluating assigned objects for license compliance

It is possible at any time to launch a manual re-evaluation of the license situation of all objects assigned to an licensed software. To do so, proceed as follows:

1. Select **Edit > Evaluate** .

The scores will now be re-evaluated for all assigned objects.

Understanding units of a licensed software

This tab displays all applications, suites or products that are part of the licensed software. It is only displayed if the units of the license are selected from the Software Catalog.

In the line above the table you can define how the license units are to be included in the licensed software. You have the following choices:

- Select **all** to include *all* listed units in the licensed software. This means that all units listed below must be installed on a device, otherwise this licensed software is not recognized as such and is not decounted in the license count.
- Select **any** to define that if even only one of the license units below is found installed on a device, this is counted as this licensed software and is decounted in the license count.

The **Units** tab displays all license units that are part of the currently selected licensed software. If the license unit is a suite or a product, all applications that are added to this suite or product by the vendor are then automatically added to this license unit, after the **Custom Applications** is updated.

It displays the following information about the license units:

Parameter	Description
Name	This column shows the names of all license units. A license unit in this case is any type of software application, tool or suite.
Version	The version number of the license unit.
Type	The type of the license unit.
Manufacturer	This field displays the name of the manufacturer of the respective license unit.
Category Name	This field displays which type of application the license unit belongs to, for example, if it is a browser, an application server software, and so on.
Suite	This field displays, if the license unit is of type suite.
Product	This field displays, if the license unit is of type product, that is the most encompassign of all possible unit types.

Adding license units from a software catalog

1. Select **Edit> Add License Units** .
   The **Select License Units** dialog box appears.
2. *(Optional)* Check the **Only Show Managed Products** box to only display those products of the catalog that you have defined as managed products.

3. *(Optional)* Uncheck the **Only Show Managed Products** box to only display those products of the catalog that were found installed on at least one device of your infrastructure.

   > If you leave this option checked, you cannot provision for new software that is not yet installed on any device, as the new version or new software is not made available in the list below.

4. Select the vendor of your license unit from the drop-down list.
   The list of **Available License Units** in the box below changes to display all available products for the chosen vendor.
5. To select the license unit you have the following choices:
   a. To select the complete product with all its suites and applications check the box ( ) of the respective product.
      The selected product is added directly to the list of **Selected License Units** in the right box.
   b. To select one or more of the product's suites, click the product and then check the boxes for those of its suites ( ) that are to be part of the license unit.
      The selected suites are added directly to the list of **Selected License Units** in the right box.
   c. To select one or more of the product's applications, click the product, then click the suite and then check the boxes for those of its applications ( ) that are to be part of the license unit.
      The selected applications are added directly to the list of **Selected License Units** in the right box.

      > Your license unit can have one or more of each of the different types.

6. Click **OK** to add the license unit and close the window.

If the licensed software is already assigned to a device or group it is automatically re-evaluated.

License unit applications

The **Applications** tab collects all applications that are part of the currently selected licensed software. This tab is only displayed if the units of the license are selected from the scanned applications list of the software inventory.

The tab provides the following information about the license units:

Parameter	Description
Name	This column shows the names of all license units. A license unit in this case is any type of software application, tool or suite.

Parameter	Description
Version	The version number of the license unit.

The following topics are provided:

- Adding application from custom applications
- Add from software inventory

Adding application from custom applications

To add a new application to the selected application list, proceed as follows:

1. Click **Edit > Add Application from Custom Applications** .
   The **Add an Application from the Custom Applications** dialog box appears. It displays all applications of the application catalogue that are not yet a member of the selected application list and are of a monitorable type, that is, MSI or Add/Remove Program.
2. Select the application to be added from one of the proposed lists.
   You can select more than one application at a time by holding the CTRL button while selecting.
3. Click **OK** at the bottom of the window to confirm.
   If the application list is already assigned to a device or group, a Confirmation window appears in which you may define to directly reactivate the application list for its assigned objects.

Add from software inventory

Applications can be added to the list of managed applications via the list of installed software generated by the software inventory. Software applications which do not provide all information required for a managed application, will in this case not appear in the list here. To add an application to the list of managed application from the general software inventory list, proceed as follows:

1. Click **Edit > Add from Software Inventory** .
   The **Add Applications from Software Inventory** dialog box appears on the screen, displaying all applications found in the software inventory.
2. In this window you can select your step in following different fashions:
   - The **All** tab displays the list of available applications in the form of a table with its name and version number.
   - The **Search** tab allows you to search for a specific application either by its name, version or type attribute. Select the respective value from the **Search Fields** list. Then enter the words which you are sure the respective attribute contains in the **Value** box and select the appropriate operator from the preceding **Operator** box and then click **Find** . The search will query all application name and the following table displays all those which match your condition.
3. Select one or more applications to be added to the list of monitored applications.

4. Click **OK** at the bottom of the window to confirm.
   A confirmation window appears if the selected application does not yet exist in the application catalogue to which it will automatically be added as well.
5. In this window you can define the folder into which the application is to be added. By default it is added directly under the main **Custom Applications** node. To add it to another folder click the icon to the right (...). The **Select Folder** window appears displaying the folder hierarchy. If the desired target folder does not yet exist you can also create new folders. To do so first select the parent folder of the new one and then select click **New Folder** below the hierarchy. The **Properties** dialog box appears on the screen. Enter the desired data into the respective boxes and then click **OK** at the bottom of the window to confirm the new application list folder. Select the target folder and click **OK** to confirm and to close the window.
6. If the application list is already assigned to a device or group, another Confirmation window appears in which you can define to directly reactivate the application list for its assigned objects.

Assigning a query to a software license

If the licensed software is of type query, the **Query** tab will be displayed instead of the **Applications** tab. This tab defines the query whose result will populate the licensed software object, that is, the result of the query represents the population on which the software is installed. Contrary to other CM objects, a licensed software can only be populated by one query at a time and this query will always be viewed as activated, no matter is actual activation status under the **Queries** node.

To assign a query to an licensed software, proceed as follows:

1. Select **Edit > Add Query** .
   The **Assign a Query** dialog box appears.
2. Select the query to be assigned to the licensed software from one of the list boxes.
3. Click **OK** to add the query and close the window.
   If the licensed software is already assigned to a device or group a Confirmation window appears in which you may define to directly re-evaluate the licensed software for its assigned objects. If you choose not to, the evaluation will take place when the scheduled time arrives, until then the status of the licensed software will be **Not Evaluated**.

Licenses

This tab collects all licenses that you have purchased for the defined licensed software.

It displays the following information about the selected licensed units:

Parameter	Description
Vendor	Enter the name of the vendor from which the software and license(s) were purchased. This may be the manufacturer as well as an independent third-party vendor.
	Enter the serial number of the product.

Parameter	Description
Product Serial Number	
License Type	Select the type for the license, for example, if it is a license that covers an entire **site** , if it is limited to a number of users (**Per Seat**), if it is counted by **processor** or by **client access** , is it a **Volume** license. If none of these apply select **Other** .
Quantity	Enter the number of purchased licenses.
Purchase Date	Define the date at which the licenses were purchased by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Purchase Order Number	Enter the order number of the license purchase under which it may be found in your books.
Expiration Date	Define the date at which the licenses expires, if applicable, by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Comments	Any pertinent additional information regarding this license.
Vendor SKU	The unique identifier of this asset as assigned by its vendor (stock-keeping unit).
Purchase Cost	Enter into this field the total purchasing costs of the asset.
Warranty Cost	Enter the total cost for the warranty contract of the asset.
Support Cost	Enter the total cost for the support contract of the asset.
Support Provider	Enter the name company that provides the support for this asset.
Support Provider Phone Number	Enter the phone number under which your direct contact at the support provider can be reached.
Date Received	Select in this field the date at which the asset arrived at its destination. This date must be later than the **Purchase Date** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Service Start Date	Select in this field the date at which the asset went online, that is, was finally up and running. This date must be later than the **Date Received** value. You can clear the field again by clicking the **Erase** icon to the right of the field.

Adding license

1. Select **Edit > Add License** .
2. Enter the required information in the respective boxes of the **Add a License** window.

Vendor	Enter the name of the vendor from which the software and license(s) were purchased. This may be the manufacturer as well as an independent third-party vendor.
Vendor SKU	The unique identifier of this asset as assigned by its vendor (stock-keeping unit).
	Enter the order number of the license purchase under which it may be found in your books.

Purchase Order Number	
Purchase Cost	Enter into this field the total purchasing costs of the asset.
License Type	Select the type for the license, for example, if it is a license that covers an entire site, if it is limited to a number of users (Per Seat), if it is counted by processor or by client access, is it a Volume license. If none of these apply select Other.
Product Serial Number	Enter the serial number of the product.
Quantity	Enter the number of purchased licenses.
Warranty Cost	Enter the total cost for the warranty contract of the asset.
Support Cost	Enter the total cost for the support contract of the asset.
Support Provider	Enter the name company that provides the support for this asset.
Support Provider Phone Number	Enter the phone number under which your direct contact at the support provider can be reached.
Purchase Date	Define the date at which the licenses were purchased by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Date Received	Select in this field the date at which the asset arrived at its destination. This date must be later than the Purchase Date value. You can clear the field again by clicking the Erase icon to the right of the field.
Service Start Date	Select in this field the date at which the asset went online, that is, was finally up and running. This date must be later than the Date Received value. You can clear the field again by clicking the Erase icon to the right of the field.
Expiration Date	Define the date at which the licenses expires, if applicable, by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Notes	This free text field can contain additional information concerning the selected object.

3. Click **OK** to add the license and close the window.

If the licensed software is already assigned to a device or group it is automatically re-evaluated.

The Licensed Software Dashboard

The dashboard contains a number of graphics displaying the license situation of the licensed software, the title line displays the date and time of the last evaluation of the licensed software and its status.

Licenses

This graph displays the general license status via the listed attributes. If you move your cursor over the individual bars a tooltip displays the absolute numbers for the different license status attributes.

- **Purchased** : total number of purchased valid licenses
- **Authorized** : the total number of devices on which the software is authorized to be installed
- **Installed** : the total number of devices on which the software is installed, that is, the number of installed licenses
- **Available** / **Exceeded** : the number of remaining or exceeded licenses, that is, the number of purchased licenses minus number of installed licenses
- **In Use** : the total number of licenses, that were used at least once, that is, the licensed software was started at least once on its device and is still installed on it. This bar will be at value 0, if the licensed software is not monitored via an application list of type **Monitored Application** and thus no usage information is available.

Authorization

This graph displays the device repartition according to their license authorization in the form of a pie chart. These numbers are the cumulative of all devices that are assigned via one or more groups and includes also individually assigned devices. If you move your cursor over a pie part a label displays the number of devices on which the software is authorized, respectively unauthorized with the corresponding percentage value.

- **Authorized** : the total number of authorized installations
- **Not Authorized** : the total number of non-authorized installations

Compliance

This graph displays the device compliance in connection with the authorizations assigned to the licensed softwares. A label displays the number of compliant/not compliant devices with the corresponding percentage value if you move the cursor over the respective pie part.

- **Compliant** : depending on the authorization status this is either that the software is authorized and installed or it is not authorized and not installed
- **Not Compliant** : depending on the authorization status this is either that the software is not authorized but installed or the license authorized but not installed
- **Conflict** : the license is authorized for device in one situation, either individually or as a member of a group and unauthorized for another situation
- **Not Installed** : the software is authorized but not installed
- **Not Evaluated** : the compliance evaluation was not executed

Usage (months)

This graph is only available for application based software license objects. It displays the usage of the licenses for different monthly timeframes with reference to their compliance status. Each bar represents a time interval and displays via its colors the license status for this timeframe. A label displays the total number of devices for the respective status for each bar part. The compliance statuses are the same as those for the **Compliance** graph to the left.

This graph is of no interest if the licensed software is not monitored via an application list of type **Monitored Application** and thus no usage information is available. In this case it will only display one bar for the status **Unknown** with the same repartition as the **Compliance** graph to the left.

Attachments of a licensed software

In this tab you can attach files to the licensed software, that contain specific license information, such as readme.txt or readme.pdf files. The contents of these files can be viewed in a browser window.

The following topics are provided:

- Viewing an attachment
- Adding an attachment

Viewing an attachment

The content of attached files can be displayed in a browser window if they are of type `bmp, jpg, gif, rtf, txt, pdf, html` or `xml` . To display a file, proceed as follows:

1. Select the attachment to display in the table in the right window pane.
2. Select **Edit > View Attachment** .

Your browser opens in a new window or tab displaying the content of the attachment file.

Adding an attachment

If you have further information stored in files, such as the file containing the license you can attach these to the licensed software object. This information must not be added before the evaluation as it is not taken into account for any calculations, it has purely informative character.

To add an attachment to the licensed software, proceed as follows:

1. Select **Edit > Add Attachment** .
   The **Add an attachment file** dialog box appears.
2. Browse your hierarchy to the storing location of the file to attach and select it.
3. Click **Open** to add the attachment and close the window.
4. To add more attachments repeat points 2 and 3 until all attachments are added.

Application Management Wizard

Application lists can be created and used in different ways. The CM wizards are one of the easiest ways to create, parameter and apply new objects and operations for your network in a quick and easy way. The following wizard is available and can be launched from different locations in the console:

The **Application Management Wizard** guides you through the individual steps required to create a new application list. The wizard can be launched from anywhere in the console, via the **Wizards > Application Management** menu item or directly from the dashboard.

The following topics are provided:

- Application List
- Applications
- Schedule Template
- Schedule Template Configuration
- Assigned Devices of application lists

Application List

In this step the application list to be created and its basic parameters must be defined. Proceed as follows to create for example an application list to monitor Acrobat Reader, the software is selected via the Software Catalog.

1. Enter the name into the respective text box, for example, *Monitoring Acrobat Reader* .
2. In the **Type** box select the **Monitored Application** option.

   > To create a prohibited or protected software select the respective option instead.

   Be aware that once you selected the type of list and clicked **Next** you cannot return to this window.
3. In the source box select the **Software Catalog** option.

   > To select the software from the **Scanned Application** list select the respective option instead.

4. Click **Next** .

Applications

In this wizard window you can add one or more applications to the list. If you selected the **Software Catalog** option in the preceeding window, proceed as follows to add the Acrobat Reader:

1. Click **Applications** .
   The **Add an Application from the Custom Applications** window appears. It displays all software products that were discovered on at least one device in your environment.
2. Find the *Acrobat Reader* application in the hierarchy and select it.
3. Click **Add** .
4. Click **OK** .
5. Click **Next** .

The software is now added to the application list.

Schedule Template

In this window a schedule template can be assigned to the new application list. For our example will will create a new schedule template.

> **Note:**
>
> Be aware that schedule templates are not applicable to **Protected Application** .

The following options are available in this window:

- **Create a new schedule template**
  Select this option if no existing schedule template is appropriate for the new list and a new one needs to be created.
- **Assign no schedule template**
  this selection will always execute the operation of the selected application list type. For application lists of type **Protected Application** this is the only possible option.
- **Assign an existing schedule template**
  If you select the option the following list box becomes available. It displays the list of all existing schedule templates. To add one select it in the following list. This option is unavailable if no schedule templates exist yet.

1. Select the **Create a new schedule template** radio button.
2. Click **Next** to continue.

Schedule Template Configuration

This optional window will not be displayed if you selected to not use a schedule template.

- If you selected to create a new schedule template enter the requested information into the respective boxes.
- If you chose to use an existing schedule template this window displays the name and settings of the template and you can make modifications to its schedule.

To define/modify the times at which an application is monitored, can be used or is forbidden, proceed as follows:

1. Enter the name into the respective text box, for example, *Working Hour* .

   > The current planning does not monitor at all, indicated by red crosses in all boxes.

2. To monitor the execution during working hours mark the boxes *Mon-Fri 7:00-12:00* by clicking the first box (Mon 07:00) and dragging the mouse key to the last box (Fri 12:00)..

3. Select **Edit > Allow Time-slot** to monitor the application.
4. Repeat the preceding steps for all other slots or ranges to be defined or modified.
5. Click **Next** to continue.

Assigned Devices of application lists

In this next window you need to define the targets of the application list. You can add either devices or device groups here.

1. Click **Assign a device group to a SCAP job** or **Assign a device to a SCAP job** / on top of the list box..
   The **Assign Target Devices or Groups** pop-up menu appears.
2. Select the device groups or devices from one of the list boxes.
3. Click **OK** to confirm the assignment and close the window.
4. Click **Finish** to confirm all settings and to start the management of the defined application list.

The last option provided by the wizard is to go directly to the application list. Check the box to change the focus of the console window to do so. Then either click **Yes** , to immediately activate the application list, or **No** to just create it, the assignment will in this case be in waiting and must be activated manually for its targets at the respective locations in the console. Click **Cancel** to abandon and return to the wizard.

Software License Management Wizard

The **Software License Management** wizard is part of the **Application Management Wizard** . It guides you through the individual steps required to create a new licensed software. The wizard can be launched from anywhere in the console, via the **Wizards > Application Management** menu item or directly from the dashboard.

The wizard provides you with two different ways to create your software license units:

- **Automatically Manage Software Licenses** : this wizard is half automated and allows you to initiate license management very quickly by entering the minimum amount of information necessary and using default values where possible.
- **Configure a Licensed Software** : this wizard provides you with all the different options that are available for license management.

Related topics

- Creating an automatically managed software license
- Manually configuring a managed software license

Creating an automatically managed software license

This subwizard allows you to almost automatically create your software license units, you are only required to provide the minimum amount of information. The wizard can be launched from anywhere in the console, via the **Wizards > Application Management** menu item or directly from the dashboard by selecting the **Automatically Manage Software Licenses** option.

The following topics are provided:

- Introduction
- Adding software license units
- Asssigning targets

Introduction

In this first step of the wizard you need to define which type of application management you want to create and how you want to create it. For this you have the following choices:

Choice	Description
Automatically Manage Software Licenses	This will allow you to quickly select software in your environment and initiate license management by entering the quantity of purchased licenses.
Configure a list of applications to manage	This will allow you to manually create a list of applications to monitor, prohibit or protect.
Configure a Licensed Software	This will allow you to manually create a licensed software.

1. To create a new licensed software in automatic mode leave the preselected **Configure a list of applications to manage** radio button.
2. Click **Next** to continue.

Adding software license units

In this window you add the license units that you want to manage. You can select either a product with all its suites and applications, a suite with its applications or individual applications.

Two filters are available to limit the list of available software to those you are interested in:

- The **Only Show Discovered Software** box is checked by default. This means that currently only those products are shown that were found on at least one device in your infrastructure. To see all software products provided by the software catalog uncheck this box.
- The **Only Show Managed Products** box is unchecked by default. This means that all products of the catalog are shown, independent if you have already treated them in the software catalog or not. Check this box to display only the products you have already treated.
  You can find more information on this topic in Changing a product status .

This window provides you with three different methods to find the license units to add:

- By default the **Select a software** option is selected, which sorts all license units according to their manufacturer in alphabetical order. You can select your manufacturer from the drop-down list of the **Manufacturer** pane. The tree box below displays all license units of the selected manufacturer according to the selected filters.
- Select the **Category** icon to the left to display the available products according to their category. The content of drop-down list of the **Manufacturer** pane now offers the different main categories of products. A second drop-down list offers subcategories depending on your selection in the first list.
- If you select the **Search** option, you can search for a specific software directly. New drop-down lists appear in the **Manufacturer** pane for further filtering:
  - Select from the **Type** list, if you are searching for a product, a suite or an application.
  - Select from the **Field** list the field, in which the search is to be done, that is if the value to be entered in the text box below is to be searched in the **Name** , **Category** , or **Manufacturer Name** box.
  - Select from the **Operator** list the operator to apply for the search.
  - Enter in the **Value** box the partial or complete value to be searched. All results are displayed in the tree box below.

> **Note:**
>
> If you are using the search to add applications, this can result in a very long list in the **Selected License Units** pane. An application can be part of more than one suites or products, and all of its parents are listed in this box.

1. Click **Add License Units** above the list box.
2. Select your license unit via one of the three possible ways explained above.

> If you found and selected your license unit via the search and it is an application, you need to click the **Add** icon between the two tree boxes. For all other cases the units are added automatically as soon as you select them in the left tree box.

The selected units are added to the **Selected License Units** in the right pane.

> **Note:**
>
> If you find at some time that you need to add more suites or applications to a selected product, you can double-click the product in the right page and the focus of the left pane returns directly to the selected product and its children.

3. Click **OK** to confirm.
4. Enter the number of licenses you purchased for this unit in the **Quantity of Licenses** column.
5. To also monitor the usage of the licensed software click the check box in the **Monitor** column.
6. Click **Next** .

Asssigning targets

In this next window you need to define the targets of the licensed software. You can add either devices or device groups here.

1. Select **Assign** .
   The **Select a Device** pop-up menu appears.
2. Select the device groups or devices from one of the list boxes.
3. Click **OK** to confirm the assignment and close the window.
4. Click **Finish** to confirm all settings and to start the management of the defined application list.

The last option provided by the wizard is to go directly to the licensed software. Check the box to change the focus of the console window to do so. Then either click **Yes** , to immediately activate the licensed software, or **No** to just create it, the assignment will in this case be in waiting and must be activated manually for its targets at the respective locations in the console. Click **Cancel** to abandon and return to the wizard.

Manually configuring a managed software license

This subwizard allows you to manually define each step of the creation of a licensed software unit. The wizard may be launched from anywhere in the console, via the **Wizards > Application Management** menu item or directly from the dashboard by selecting the **Configure a Licensed Software** option.

The following topics are provided:

- Introduction - Configure a Licensed Software Wizard
- Creating the licensed software
- Adding the software license units
- Adding licenses
- Adding attachments
- Assigned devices

Introduction - Configure a Licensed Software Wizard

In this first step of the wizard you need to define which type of application management you want to create and how you want to create it. For this you have the following choices:

Choice	Description
Automatically Manage Software Licenses	This will allow you to quickly select software in your environment and initiate license management by entering the quantity of purchased licenses.
Configure a list of applications to manage	This will allow you to manually create a list of applications to monitor, prohibit or protect.
Configure a Licensed Software	This will allow you to manually create a licensed software.

1. To create a new licensed software manually select the **Configure a list of applications to manage** radio button.
2. If attachments are to be added to the licensed software check the following **Add Attachment** box.
3. Click **Next** to continue.

Creating the licensed software

1. Enter a name for the new licensed software in the **Name** box, for example *Microsoft Office 2010* .
2. *(Optional)* Select from the **Category** box the category to which this software belongs, or enter a new one if none exists yet or none fits the new licensed software. For example, **Office Applications** .
3. In the **Evaluation Type** list select from which source you want to select the software. You have the following choices:

Software Catalog	The licensed software is populated with applications of the Software Catalog, that are under the same license scheme. This option may not be available depending on your licenses.
Query	The licensed software is populated via the result of a query, that is, all devices that answer the software criteria specified in the query.
Scanned Application	The licensed software is populated with individual, scanned applications, that are under the same license scheme.

4. *(Optional)* By default all newly created objects are created directly under the main object node. To create it in any other folder click the icon to the right of the field (...). Select the desired folder from the folder hierarchy. If the desired target folder does not yet exist you can also create new folders. To do so first select the parent folder of the new one and then select click the **New Folder** icon below the hierarchy. Enter the desired data into the respective fields and then click the **OK** button at the bottom of the window to confirm the new folder. Select the target folder and click the **OK** button to confirm and to close the window.
5. Click **OK** at the bottom.

Adding the software license units

In this window you add the license units that you want to manage. You can select either a product with all its suites and applications, a suite with its applications or individual applications.

Two filters are available to limit the list of available software to those you are interested in:

- The **Only Show Discovered Software** box is checked by default. This means that currently only those products are shown that were found on at least one device in your infrastructure. To see all software products provided by the software catalog uncheck this box.
- The **Only Show Managed Products** box is unchecked by default. This means that all products of the catalog are shown, independent if you have already treated them in the software catalog or not. Check this box to display only the products you have already treated.
  You can find more information on this topic in Changing a product status .

This window provides you with three different methods to find the license units to add:

- By default the **Select a software** option is selected, which sorts all license units according to their manufacturer in alphabetical order. You can select your manufacturer from the drop-down list of the **Manufacturer** pane. The tree box below displays all license units of the selected manufacturer according to the selected filters.
- Select the **Category** icon to the left to display the available products according to their category. The content of drop-down list of the **Manufacturer** pane now offers the different main categories of products. A second drop-down list offers subcategories depending on your selection in the first list.
- If you select the **Search** option, you can search for a specific software directly. New drop-down lists appear in the **Manufacturer** pane for further filtering:
  - Select from the **Type** list, if you are searching for a product, a suite or an application.
  - Select from the **Field** list the field, in which the search is to be done, that is if the value to be entered in the text box below is to be searched in the **Name** , **Category** , or **Manufacturer Name** box.
  - Select from the **Operator** list the operator to apply for the search.
  - Enter in the **Value** box the partial or complete value to be searched. All results are displayed in the tree box below.

> **Note:**
>
> If you are using the search to add applications, this can result in a very long list in the **Selected License Units** pane. An application can be part of more than one suites or products, and all of its parents are listed in this box.

1. Click **Add License Units** above the list box.
2. Select your license unit via one of the three possible ways explained above.

If you found and selected your license unit via the search and it is an application, you need to click the **Add** icon between the two tree boxes. For all other cases the units are added automatically as soon as you select them in the left tree box.

The selected units are added to the **Selected License Units** in the right pane.

Note:

If you find at some time that you need to add more suites or applications to a selected product, you can double-click the product in the right page and the focus of the left pane returns directly to the selected product and its children.

3. Click **OK** to confirm.
4. Enter the number of licenses you purchased for this unit in the **Quantity of Licenses** column.
5. To also monitor the usage of the licensed software click the check box in the **Monitor** column.
6. Click **Next** .

Adding licenses

1. Select **Edit > Add License** .
2. Enter the required information in the respective boxes of the **Add a License** window.

Vendor	Enter the name of the vendor from which the software and license(s) were purchased. This may be the manufacturer as well as an independent third-party vendor.
Vendor SKU	The unique identifier of this asset as assigned by its vendor (stock-keeping unit).
Purchase Order Number	Enter the order number of the license purchase under which it may be found in your books.
Purchase Cost	Enter into this field the total purchasing costs of the asset.
License Type	Select the type for the license, for example, if it is a license that covers an entire site, if it is limited to a number of users (Per Seat), if it is counted by processor or by client access, is it a Volume license. If none of these apply select Other.
Product Serial Number	Enter the serial number of the product.
Quantity	Enter the number of purchased licenses.
Warranty Cost	Enter the total cost for the warranty contract of the asset.
Support Cost	Enter the total cost for the support contract of the asset.

Support Provider	Enter the name company that provides the support for this asset.
Support Provider Phone Number	Enter the phone number under which your direct contact at the support provider can be reached.
Purchase Date	Define the date at which the licenses were purchased by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Date Received	Select in this field the date at which the asset arrived at its destination. This date must be later than the Purchase Date value. You can clear the field again by clicking the Erase icon to the right of the field.
Service Start Date	Select in this field the date at which the asset went online, that is, was finally up and running. This date must be later than the Date Received value. You can clear the field again by clicking the Erase icon to the right of the field.
Expiration Date	Define the date at which the licenses expires, if applicable, by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Comments	Enter any pertinent additional information in this free text box.

3. Click **OK** to add the license and close the window.
4. Click **Next** .

Adding attachments

If you have further information stored in files, such as the file containing the license you can attach these to the licensed software object. This information must not be added before the evaluation as it is not taken into account for any calculations, it has purely informative character.

1. Click **Add Attachment** .
   The **Add an attachment file** window appears.
2. Select the file and click **Open** .
3. To add more attachments repeat points 2 and 3 until all attachments are added.
4. Click **Next** .

Assigned devices

In this next window you need to define the targets of the licensed software. You can add either devices or device groups here.

1. Select **Assign** .
   The **Select a Device** pop-up menu appears.
2. Select the device groups or devices from one of the list boxes.
3. Click **OK** to confirm the assignment and close the window.
4. Click **Finish** to confirm all settings and to start the management of the defined application list.

The last option provided by the wizard is to go directly to the licensed software. Check the box to change the focus of the console window to do so. Then either click **Yes** , to immediately activate the licensed software, or **No** to just create it, the assignment will in this case be in waiting and must be activated manually for its targets at the respective locations in the console. Click **Cancel** to abandon and return to the wizard.

Managing financial information for assets

Financial asset management allows you to track the financial data of IT assets (devices) and their impact on the company's business. This information accompanies the device through all the steps of its life in the company:

- Receive newly ordered hardware
- Manage the new hardware once it is being used
- Retire the hardware from the IT park once it has reached its end of life
- Report on steps of the hardware lifecycle.

The following topics are provided:

- Overview of financial asset management
- Financially assessing your devices
- Evaluating a device group's financial data
- Creating relations between assets
- Adding additional information via files
- Editing the financial information of a device
- Viewing calculated values
- Viewing financial information of a device

Overview of financial asset management

The following paragraphs guide you through the steps that are necessary to configure the financial asset management and to evaluate your first device.

Financially assessing your devices

After all financial information is entered, the basic data that applies for your complete infrastructure as well as the specific data for the individual devices the information is directly updated with the new data. The preceding information panel the table is divided into the following parts providing the essential information about the device:

- **Valuation** : The lines in this part display basic device costs:
- **Device Costs** : This is the purchase price of the device itself only.
    - **Rollup Costs** : This amount indicates the total cost of the device plus all other devices that are attached to it, such as a printer, a webcam, a peripheral storage device, and so on.

    - **Current Estimated Value** : This value calculates the remaining monetary value of the device itself, taking into account its purchase price, the estimated live time and the time of this life time that has already elapsed.
- **Support** : The lines in this part provide useful information about the support that is provided for the device, such as the phone number to contact in case of problems and how long the support is still valid.
- **Lifecycle Status** : This chart and the associated data display at which status of its life the device currently is.

Evaluating a device group's financial data

Evaluating the financial data of a device is done via reports. For this CM provides you with a number of predefined reports that you only need to generate.

To do so, proceed as follows:

1. Go to the **Financial Asset Management** folder under the **Reports** node and open it.

   > You will find there a number of predefined reports for this topic.

2. Select a report in the left tree hierarchy, for example, *Total Cost of Asset (Purchase)* .
3. Select its subnode **Assigned Objects > Device Groups** .
4. Click **Assign Device Group** .
5. In the appearing **Assign to Device Group** window select your target device group and click **OK** to confirm.
6. Select the assigned device group in the table to the right.
7. Click **Generate Report** .
8. Click **Yes** in the appearing confirmation window.
9. Select the **Report Results > Device Group Results > Your Device Group** subnode.

   > Here you can see the newly generated report.

10. Select it and click **View** .
    A new browser window/tab opens on the screen and displays the report.

Creating relations between assets

Devices can be organized using a two level hierarchy. This means that a device can have children or can have a parent but cannot have both a parent and children at the same time. This organization will help computing the cost of devices to which child elements are attached such as printers. Therefore, a device's costs includes its own cost plus the costs of all its children.

The following topics are provided:

Adding a parent to a device

To add a parent to a device, proceed as follows:

> **Note**
>
> Ensure that the selected device is not already a child to another device.

1. Make sure that you are located either under the **Device Topology** node or a **Your Device Group** node.
2. Select the desired device.
3. Click **Attach to a parent device** .
   The **Select a Device** dialog box appears.
4. Select the device to add a parent. You can only select one device.
   Make sure that the selected device is not a child of another device. In this case an error message will be displayed.
5. Click **OK** to confirm the new relation.

You have now established a parent-child relation for a devices that is connected to a parent device.

Adding children to a device

To add children to a device, proceed as follows:

> **Note**
>
> Ensure that the selected device is not a child to another device.

1. Make sure that you are located either under the **Device Topology** node or a **Your Device Group** node.
2. Select the desired device.
3. Click **Attach a child device** .
   The **Select a Device** dialog box appears.
4. Select the devices to add as children.
   You can select more than one device. Make sure that the selected devices are not already children of another device or a parent to other children. In this case an error message will be displayed.

5. Click **OK** to confirm the new relation.

You have now established a parent-child relation for devices that are attached to their parent.

Adding additional information via files

In this tab you can view and attach files to the device, that contain specific and pertinent financial information, such as `readme.txt` or `readme.pdf` files. The contents of these files can be viewed in a browser window.

The following topics are provided:

- Viewing an attachment
- Adding an attachment

Viewing an attachment

The content of attached files can be displayed in a browser window if they are of type bmp, jpg, gif, rtf, txt, pdf, html or xml. To display a file, proceed as follows:

1. Make sure that you are located either under the **Device Topology** node or a **Your Device Group** node.
2. Select its **Attachments** tab.
3. Select the desired attachment.
4. Click **View Attachment** .
   Your browser opens in a new window or tab displaying the content of the attachment file.

You have now displayed the contents of an attachment of a device.

Adding an attachment

To add an attachment to a device, proceed as follows:

1. Make sure that you are located either under the **Device Topology** node or a **Your Device Group** node.
2. Select its **Attachments** tab.
3. Select the desired device.
4. Click **Add Attachment** .
   The **Add an attachment file** dialog box appears.
5. Browse your hierarchy to the storing location of the file to attach and select it.
6. Click **Open** to add the attachment and close the window.

You have now added an attachment containing pertinent information to the respective device.

Editing the financial information of a device

To edit the financial information of one or more devices, proceed as follows:

1. Make sure that you are located either under the **Device Topology** node or a **Your Device Group** node.
2. Select its **Default Values** tab.
3. Select the device for which you want to modify the financial information in the right window pane. You can select more than one device by holding the CTRL key pressed while making your selection.
4. Click **Properties** .
   The **Financial Asset Management** dialog box appears.
5. Modify the necessary values.

   - If you modify the **Lifecycle Status** , do not forget to click the icon next to the box to deactivate the automatic update. If you do not deactivate it, the selected value is updated to the calculated one again at the next update.
   - If you are editing the values for more than one device make sure to check the boxes to the left of the parameters that you want to edit. In this case only these are modified, all other unchecked parameters remain for each device as they are.

6. Click **OK** to save the modified financial information.

To define financial information parameters, see Financial asset information.

Financial Asset Information

The following parameters are available to define financial information for the devices of your network:

Parameter	Description
Lifecycle Status	Select the lifecycle status from the list box. The predefined values are: • **On Order** : The asset was already ordered but has not yet arrived at its destination. • **Received** : The asset arrived at its destination. • **In Stock** : The asset has arrived at its destination and is currently located in the warehouse. • **Deployed** : The asset is installed at its final destination. • **Retired** : The asset has arrived at the end of its lifecycle and was removed from the network.If you have defined your own custom status values these are also available in this list.
Asset Tag	Enter the unique identifier of the asset. The identifier can have no more than 64 characters.
Asset Owner	Click the **Add User** icon to the right of the field to select the owner of this asset.
Department	Click the **Add User Group** icon to the right of the field to select the department that is responsible for this device. The department is represented by a user group.

Parameter	Description
Location	The country/region/town/building/geographical area at which the asset is located.
Managed By	Click the **Add Administrator** icon to the right of the field to select the support contact who is responsible for this asset.
Vendor	Enter the name of the vendor of the asset, for example, *Hewlett Packard* or *Dell* .
Vendor SKU	The unique identifier of this asset as assigned by its vendor (stock-keeping unit).
Invoice Number	Enter into this field the number of the invoice.
PO Number	Enter the number of the purchase order for the asset.
Warranty Cost	Enter the total cost for the warranty contract of the asset.
Support Cost	Enter the total cost for the support contract of the asset.
Support Provider	Enter the name company that provides the support for this asset.
Support Provider Phone Number	Enter the phone number under which your direct contact at the support provider can be reached.
Purchase Date	Select in this field the purchase date of the asset. You can clear the field again by clicking the **Erase** icon to the right of the field.
Invoice Date	Enter into this field the date of the invoice. The date must be equal to or later than the **Purchase Date** .
Date Received	Select in this field the date at which the asset arrived at its destination. This date must be later than the **Purchase Date** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Service Start Date	Select in this field the date at which the asset went online, that is, was finally up and running. This date must be later than the **Date Received** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Support Expiration Date	The date at which the support contract for the asset runs out.
Warranty Expiration Date	Select in this field the date at which the warranty for the asset expires. This date must be later than the **Service Start Date** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Purchase	Select this radio button if the asset was purchased.
Purchase Cost	Enter into this field the total purchasing costs of the asset.
Residual Value	Enter into this field the currently remaining value of the asset. The residual value is an estimate of the value of the asset at the time it is sold or disposed of; it may be zero. Residual value is also known as scrap value or salvage value.
Useful Life (months)	Enter into this field the total amount of time that the asset is expected to be up and working in your network in months from the service start date onwards.
Depreciation Type	The method used to calculate the costs:

Parameter	Description
	• **Straight Line** : the most often used method, in which the company estimates the residual value of the asset at the end of the period during which it is used to generate revenues (useful life) and expenses a portion of *original cost* in equal increments over that period. • **Declining Balance** : the book value is multiplied by a fixed rate.
Lease	Select this radio button if the asset is subject to a leasing contract.
Lease Cost of Asset	Enter into this field the total costs for the lease of the asset.
Lease Term (months)	Select from this list the time in months for the leasing contract.
Lifecycle Status	Select the lifecycle status from the list box. The predefined values are: • **On Order** : The asset was already ordered but has not yet arrived at its destination. • **Received** : The asset arrived at its destination. • **In Stock** : The asset has arrived at its destination and is currently located in the warehouse. • **Deployed** : The asset is installed at its final destination. • **Retired** : The asset has arrived at the end of its lifecycle and was removed from the network.If you have defined your own custom status values these are also available in this list.
Manual Status Updates	Be aware, if a device is deprecated, its lifecycle status is automatically set to **Deprecated** , even if the automatic update is deactivated.

Viewing calculated values

The **Financial Asset Management** tab shows different figures about the current value of the selected device:

Parameter	Description
Rollup Costs	The total cost for this device and all its children.
Device Costs	The costs of this device only.
Current Estimated Value	The cost after the depreciation calculation.
Time in Stock (days)	Represents the timeframe between the arrival of the asset at its destination and the date it was up and running in days.
Past Lifetime (days)	The timeframe that the asset has been used in days since its installation up to today.
Remaining Lifetime (days)	The number of days remaining that the asset will most probably still be used within your network.

The following topics are provided:

- Modifying the lifecycle status of a device
- Adding new lifecycle status types for financial device management

Modifying the lifecycle status of a device

Normally the lifecycle status is calculated and maintained automatically with the 5 predefined status values. If the predefined ones are not extensive enough or do not fit your requirements, it is possible to create your own lifecycle status values as explained in the Adding lifecycle status values topic. You can then assign these new custom status values as well to your devices or device groups.

To modify the lifecycle status of one or more devices you have two possibilities:

- If you want to modify other values in addition to the lifecycle status you should proceed as explained in the Editing the financial information of a device topic.
- If you only want to change this value you can do so directly as explained as follows:

1. Select the device for which you want to modify the financial status in the right window pane and right-click.

> - You can select more than one device by holding the CTRL key pressed while making your selection.
> - You can select the devices under the **Device Topology** node or within a device group as well.

2. Select the **Lifecycle Status** option from the appearing pop-up menu.
3. Change the status value to the new status by selecting it from the list that appears.

You have now modified the status of one or more device that have advanced to another step in their lifecycle within your company.

> **Note:**
>
> Changing a status via this method automatically switches from automatic to manual mode, to make sure your selection is not overwritten during the next automatic update.

Adding new lifecycle status types for financial device management

CM comes with 5 predefined financial device status values. If these do not fit your own requirements or you need others you can add to them as follows:

1. Select the **Global Settings > Financial Asset Management** node.
2. Select its **Lifecycle Status** tab.

> This view displays the existing status values in their defined order and you can add new status values. You can also put the already existing values in the proper order according to your requirements.

3. Click **Add Status** .
   The **Add a Status** dialog box appears.
4. Enter the name for the new status in the **Add a Status** window.
5. Click **OK** .
6. Select the newly created status that was appended at the bottom of the list of existing status values and click **Move Up** until it is at the required position in the list.

You created a new financial status value and put it in its correct position of the device lifecycle flow. You can now assign it to your devices and device groups.

> **Note:**
>
> Be aware, that these custom status values are not included in the automatic updates. Therefore, if you assign a custom status to a device, you also need to switch from automatic update mode to manual mode. If you do not do so, you selected custom status reverts to the appropriate predefined status at the next automatic update.

Viewing financial information of a device

This view provides you all the financial information available for the selected device:

Parameter	Description
Lifecycle Status	Select the lifecycle status from the list box. The predefined values are: • **On Order** : The asset was already ordered but has not yet arrived at its destination. • **Received** : The asset arrived at its destination. • **In Stock** : The asset has arrived at its destination and is currently located in the warehouse. • **Deployed** : The asset is installed at its final destination. • **Retired** : The asset has arrived at the end of its lifecycle and was removed from the network.If you have defined your own custom status values these are also available in this list.
Asset Owner	Click the **Add User** icon to the right of the field to select the owner of this asset.
Managed By	Click the **Add Administrator** icon to the right of the field to select the support contact who is responsible for this asset.
Department	Click the **Add User Group** icon to the right of the field to select the department that is responsible for this device. The department is represented by a user group.

Parameter	Description
Vendor	Enter the name of the vendor of the asset, for example, *Hewlett Packard* or *Dell* .
Vendor SKU	The unique identifier of this asset as assigned by its vendor (stock-keeping unit).
PO Number	Enter the number of the purchase order for the asset.
Warranty Expiration Date	Select in this field the date at which the warranty for the asset expires. This date must be later than the **Service Start Date** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Warranty Cost	Enter the total cost for the warranty contract of the asset.
Support Cost	Enter the total cost for the support contract of the asset.
Support Provider	Enter the name company that provides the support for this asset.
Support Provider Phone Number	Enter the phone number under which your direct contact at the support provider can be reached.
Purchase Date	Select in this field the purchase date of the asset. You can clear the field again by clicking the **Erase** icon to the right of the field.
Date Received	Select in this field the date at which the asset arrived at its destination. This date must be later than the **Purchase Date** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Service Start Date	Select in this field the date at which the asset went online, that is, was finally up and running. This date must be later than the **Date Received** value. You can clear the field again by clicking the **Erase** icon to the right of the field.
Purchase	Select this radio button if the asset was purchased.
Purchase Cost	Enter into this field the total purchasing costs of the asset.
Residual Value	Enter into this field the currently remaining value of the asset. The residual value is an estimate of the value of the asset at the time it is sold or disposed of; it may be zero. Residual value is also known as scrap value or salvage value.
Useful Life (months)	Enter into this field the total amount of time that the asset is expected to be up and working in your network in months from the service start date onwards.
Lease	Select this radio button if the asset is subject to a leasing contract.
Lease Cost of Asset	Enter into this field the total costs for the lease of the asset.
Lease Term (months)	Select from this list the time in months for the leasing contract.
Manual Status Updates	Be aware, if a device is deprecated, its lifecycle status is automatically set to **Deprecated** , even if the automatic update is deactivated.

Managing compliance

The following topics are provided:

Overview of Compliance management

BMC Client Management provides you with two different ways to make sure your IT environment is compliant with all necessary rules and regulations:

- **Custom Compliance**
- **SCAP Compliance**

Custom Compliance

Custom compliance in CM allows to evaluate the current situation of the network population about their compliance. The agent collects information about the devices via which it then defines if a device is compliant with company policies and regulations or not. If not, it can restrict its accesses and operations.

The calculation of compliance in BMC Client Management - Compliance Management is based on a number of specifically defined criteria. The values for these are located in the different inventories available in the console and the database. This information is collected by the agent via operational rules that are executed on the devices in your network and then uploaded to the master database. After the information is available, the compliance rules can calculate the compliance of a device about specific aspects of its configuration.

SCAP Compliance

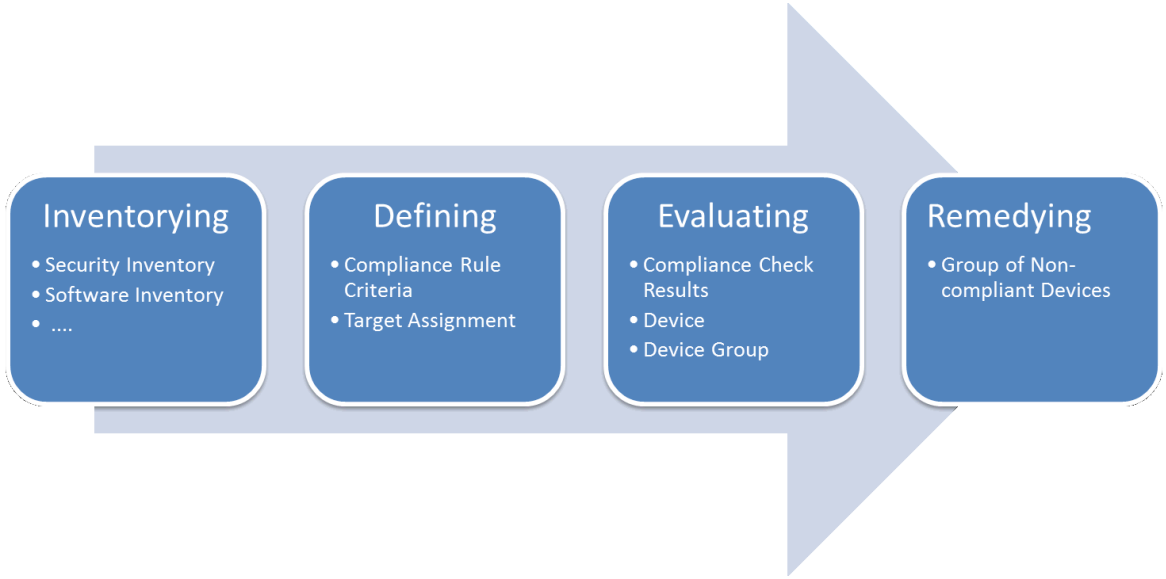
The Security Content Automation Protocol (SCAP) is a specification established by the National Institution of Standards and Technology (NIST). In general, it was established to express and manipulate security data in standardized and automated ways and therefore contains elements of

vulnerability, asset and configuration management. More precisely, SCAP enumerates product names, software flaws and configuration issues, identifies the presence of vulnerabilities and assigns severity scores to vulnerabilities. By that, SCAP makes it easier for organizations to automate ongoing security monitoring, vulnerability management and the reporting of the security policy evaluation.

SCAP 1.2 consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. It is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

The SCAP components were created and are maintained by several entities, including the MITRE Corporation, the National Security Agency and the Forum of Incident Response and Security Teams (FIRST). As a result, the SCAP components are individually maintained specifications which standardize the security information we communicate (content) and how we communicate and use security information (tools/content processing). SCAP also comprises standardized referenced data, for example the National Vulnerability Database (NVD) of the US government.

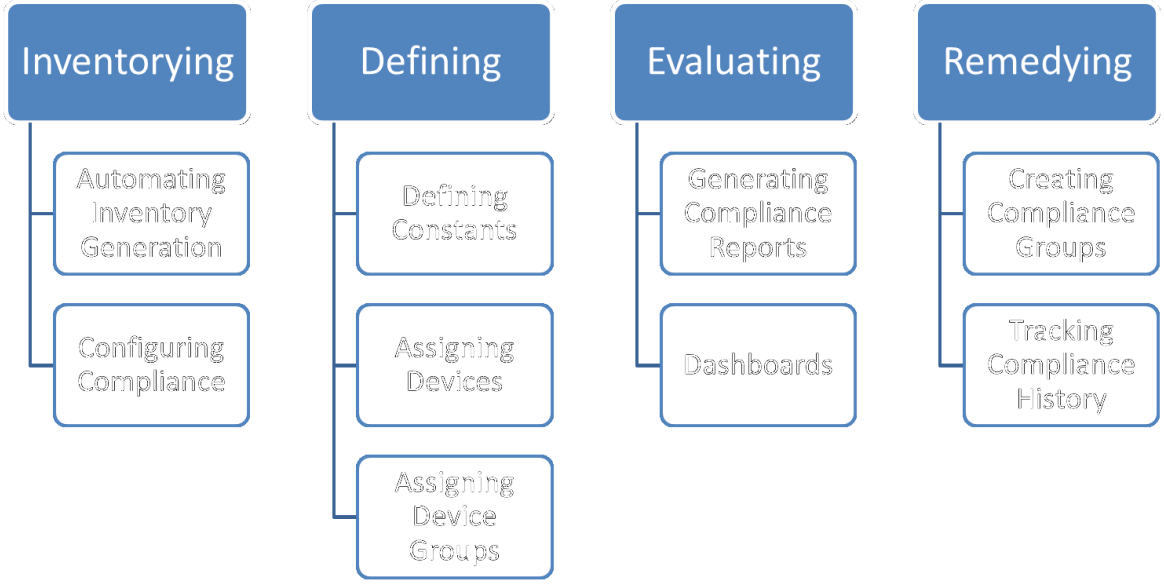
Getting started with custom compliance



Compliance Management consists of four consecutive steps:

- **Inventorying** : Taking stock of the current situation of the devices.
- **Defining** : Defining the criteria that the devices must comply to and assigning it to the devices.
- **Evaluating** : Assessing the results of the compliance check.
- **Remedying** : Correcting the points on which the devices are not compliant, for example by activating a firewall, applying a patch, resolving a security hole, uninstalling a software, and so on.

By executing these four steps you are making sure that your devices comply to all the rules and policies defined within your organization.



You have the following main options for improving your compliance processes:

- **Automating inventory generation** : Setting up CM to automatically and regularly generate the required inventories of the concerned devices.
- **Defining constants** : Defining constants that can be used when setting up the compliance rule criteria.
- **Generating compliance reports** : Generating reports in different formats (PDF, HTML, XML) to visualize and track compliance results.
- **Creating dashboards** : Creating specific dashboards to provide an easy overview over a specific situation or population.

Evaluating your Environment for Compliance with a Basic Rule

The following paragraphs lead you through a first evaluation example of your environment. We will create a rule that checks if a device has a firewall installed and if it is active.

Evaluating a group of devices for their compliance consists of the following steps:

- Collect the different types of inventory on the target devices. Generating inventories is not part of this section, see the BMC Client Management - Inventory section on how to generate the Security inventory for this example.
- Create the compliance rule with its criteria and relation.
- Assign the rule to the target for compliance evaluation.
- Evaluate the compliance results.

Related topics

- Creating a Firewall Compliance Rule
- Assigning the Rule to a Device and Evaluating its Compliance
- Analyzing the compliance rule results

Creating a Firewall Compliance Rule

This compliance rule will verify if the target device has a firewall installed that is active. A compliance rule defines the criteria to which the target population has to correspond to be considered compliant. These criteria are collected in groups, the criteria groups, which can contain any number of criteria. This rule will only have one criteria group containing only one criterion.

1. Click **Create Compliance Rule** .
2. Enter *Firewall* into the **Name** box and then click **OK** .
   The new compliance rule is added to the list of members in the right pane.
3. Double-click the new rule.
4. To add the compliance criteria select the **Criteria** tab to the right.
5. Select **Add Criteria Group** .
   The **Criteria Group** window provides access to the list of available criteria in the **Criteria Group Definition** box. The first line of this box indicates the index number of the criteria group which is about to be defined, that is, *Criteria Group 1* in our case, because we are only creating the first for this rule.
6. Enter *Firewall* into the **Name** box.
7. From the **Class** list select the **Security Settings Inventory** option.
8. Select the table from which the criteria is to be chosen from the **Table** box, that is, in our case this is the value **Security Center Firewalls** .
   The following **Available Criteria** box now displays all criteria available for the selected class and table.
9. Select the criterion **Enabled** .
10. Click **Find** next to the **Value** box.
11. In the **Search Criteria** window change the operator to **Contains** in the **Operator** box.
12. Click **Find** next to the **Value** box again.
13. In the **Results** box select **Yes** and click **OK** to close the window.
14. Click **Add** to add the defined criterion.
15. Click **OK** again to add the criteria group to the compliance rule.
16. To activate the compliance rule, select the green colored option *active* instead of the currently displayed red option *inactive* in the **Status** list.

You have now created a compliance rule that will check if its assigned devices/device groups have a enabled firewall.

Assigning the Rule to a Device and Evaluating its Compliance

The compliance rule is now created and active and must be assigned to the devices which are to be verified for compliance, in our example the master. After the assignment is done, the rule will immediately verify if the device is compliant to the specified criteria and display the result right away in the table.

1. Click the **Assigned Objects** , then the **Devices** node in the left window pane under your newly created compliance rule.
2. Click **Assign Device** .
3. Go to the **All** tab of the **Assign to Device** window and select the master from the list.
4. Click **Evaluate** to immediately check if the master is compliant.

The firewall compliance rule is now assigned to a device and has verified if this device has an enabled firewall.

Analyzing the compliance rule results

You can analyze the details of the compliance results right away in this window, they are available via the **Properties** window of the respective device. To view the result, proceed as follows:

1. Select the device in the right window pane.
2. Click **Properties** .
   The **Compliance Results** window opens on the screen providing compliance information about the device:

- The symbol to the next to the device name indicates if the device complied to the requested criteria group, a green check mark if this is the case, a red x if it is not so.
- The following line displays the operating system and the installed service pack of the device.
- The **Criteria Groups Causing Non-compliance** box offers you to only display those groups containing the criteria which cause the non compliance of the device. If the device is compliant this option is not displayed. The table **Criteria Groups** displays the following details:

Parameter	Description	
Index	This field displays the index value for the defined criteria group.	
Results	These fields indicate if the device complied to the respective criteria group. Be aware, that a group might be evaluated as compliant even if the overall compliance is negative or vice versa if the relation equation has the *not* operator as the final operator.	
Name	The fields of this column display the custom defined names of the criteria groups specified for this compliance rule	
Table		

Parameter	Description	
	The fields of this column display the names of the database table from which the criteria were chosen for the criteria group.	The **Group Relation** box appears the group relation as it was defined when the evaluation took place for which the result displays in this window. The **Description** box shows the details on the criteria defined for the selected criteria group in the preceding table.

1. Click **OK** to close the window.

You have now verified the results of the compliance check for the device's enabled firewall.

Assigning the compliance rule to a device group and evaluating its members

1. Click the **Assigned Objects** , then **Device Groups** node in the left window pane under your newly created compliance rule.
2. Click **Assign Device Group** .
3. Select a device group from the list, for example, *All Devices* .
   The group will be added to the table in the right pane.
4. Select the subnode of the group, for example, *All Devices* .
   It displays all members of the group and their evaluation status.
5. Click **Evaluate** .The group's members are directly evaluated and the overall result is indicated in each device's **Compliance** icon.

> **Note:**
>
> Be aware that this might take a while, depending on the overall load and group size. The newly evaluated data is displayed when you click **Refresh** or after the automatic refresh interval has elapsed.

The group is now assigned to the compliance rule and its members are evaluated for their compliance to the defined criteria.

Creating a Device Group of Non-compliant Devices

After you have analyzed the compliance results, you can create a device group containing all devices which are not compliant with your rules for further treatment. To do so, proceed as follows:

1. Select the rule for which a group is to be created in the right window pane.
2. Click **Create Device Group - Not Compliant** .
   The **Create Device Group - Not Compliant** window appears.

3. Define the properties of the new group, such as another name as the default name, in the **Create Device Group - Not Compliant** window, then click **OK** .

The new group is now created at the defined location, containing all those devices as members of which the evaluation status is *not compliant* .

> **Note:**
>
> Using the same procedure with the respective icons/menu items you can also create a device group containing all compliant devices and a group for all devices that could not yet be evaluated. Because these groups are dynamic, devices currently being a member of the non-compliant group will automatically move to the compliant group once the necessary operations to make them comply to the criteria were executed.

Reporting compliance

After data on the compliance situation on individual devices and the network in general is available, it can be summarized or detailed by reports. CM provides a number of *predefined reports* specifically for compliance management with its out-of-the-box objects. They are all collected in the **Compliance** folder under the **Reports** node. However, it is also possible to directly assign and generate a predefined report under a *compliance rule*.

- Generating your first Report
- Creating Your Own Compliance Report

Generating your first Report

After data on the compliance situation on individual devices and the network in general is available it can be summarized or detailed by reports. CM provides a number of *predefined reports* specifically for compliance management with its out-of-the-box objects. They are all collected in the **Compliance** folder under the **Reports** node. However, it is also possible to directly assign and generate a predefined report under a *compliance rule* .

1. Select the compliance rule for which the report is to be generated in the left window pane.
2. Go to its **Report Results** subnode.
3. Click **Assign Report** .
4. Find the desired report in the displayed hierarchy and select it.
5. Click **OK** .
6. Click **Yes** in the confirmation window to immediately generate the report.
7. To view the report, select the report in the table of the **Report Results** view and then click **View Last Result** .
   A browser window opens on the screen and displays the report.

You have now generated and viewed a first report on device compliance.

Creating Your Own Compliance Report

The CM console provides a number of report templates specifically for compliance management. This task creates and generates some examples of the available templates. You can also create your own style-based reports as explained in the Reports topics.

1. Click the **Wizards > Report Creation** menu item.
2. Enter *CM Agent Installation Directory Compliance* into the **Name** and **Report Title** boxes.
3. Select the **Template-based** option from the **Report Type** list.
4. Select from the **Report Template** box the template **Compliance by Device** .
5. Click **Next** .
6. Click **Next** without any modifications.
7. Click **Assign Compliance Rule** .
8. Select the *CM Client Installation Directory* rule and click **OK** .
9. Click **Next** .
10. Check the **Immediately** radio button in the **Execution Date** panel.
11. Check the **Immediately generate the report** box at the bottom of the window.
12. Click **Finish** at the bottom of the window to confirm the new report and immediately generate it.
13. To view the report, select it and then **View Last Result** .
    A browser window opens on the screen and displays the generated report.

You have now created a template based report, generated it and viewed it.

Managing compliance dashboards

A dashboard offers a global view on a set of compliance results in the form of charts. You can add, remove and move charts to and within your dashboard according to your needs. To not overload the dashboard and still provide enough information no more than four charts are recommended.

You can have charts for compliance rules and specific groups assigned to a compliance rule in a dashboard.

- Adding a new dashboard
- Modifying an existing dashboard

Adding a new dashboard

1. Click **Create Dashboard** .
   The **Properties** window appears.
2. Enter an explicative name into the **Name** box, for example, *Active Firewall Results* .
3. Click **OK** .
   The new dashboard will be added directly under the main Dashboards node.
4. Select the newly created dashboard in the left hierarchy tree.
5. Move your cursor over the left square in the right window pane and click the left mouse button.

6. In the **Add a Chart** window find your compliance rule, for example, *Firewall* and select it.
7. Click **OK** .
   A pie chart will be shown in the left frame displaying the overall compliance status of all device groups assigned to the compliance rule as of the rule's last evaluation results.
8. Now move your cursor to the right frame and click again your mouse button.
9. Reselect the same rule in the **Add a Chart** window and go down to one of its assigned groups, for example, *My Devices* and click **OK** .
   A second chart displays to the right, displaying the compliance status of the selected group as of its last evaluation.
10. To add more charts move to the following line and repeat the preceding steps.

You have now created a dashboard that displays two charts, one displaying the compliance situation for the whole population about a specific rule, the second chart the situation for a specific part of your environment.

Modifying an existing dashboard

It is possible to modify an existing dashboard, that is, to add more charts or remove some, or you can also replace a chart with another. To do so, proceed as follows:

1. Select the dashboard to modify in the left window pane.
2. Move the cursor over the chart to modify in the right window pane. Here you have now the following possibilities:
   - Click **Delete** in the top right corner of the chart to remove the chart from the Dashboard.
   - Click **Properties** in the top right corner of the chart. In this case the Properties window appears in which you can select the item with which to replace the current chart.

If you are not sure that all the latest modifications were already executed before the last evaluation you can reevaluate a rule/target by clicking **Evaluate** within the chart.

Compliance Rules for Compliance Management

Compliance rules in BMC Client Management - Compliance Management are used to define if a device or a group of devices is compliant with the organization's policies and regulations. Based on specific criteria groups that are defined by the administrator the CM agent then checks each target device if it complies to the requirements.

Compliance rules are stored in folders. These folders are for grouping one or more rules according to your own specific type of classification to make organization and the finding of specific rules easier. Compliance rule folders can contain any number of predefined or custom-made compliance rule folders and compliance rule for making sure all devices in your system are compliant to the defined standards and policies.

What is a compliance rule?

A compliance rule defines the criteria groups to which the target population has to correspond to be considered compliant. It specifies in which relation the individual criteria groups stand to each other and displays the conformity results in text and graphical format.

How does device compliance work?

Compliance rules in BMC Client Management - Compliance Management allow to evaluate the current situation of the network population about their compliance. The agent or scanner collects information about the devices via which it then defines if a device is compliant with company policies and regulations or not. If not, it can restrict its accesses and operations.

The calculation of device compliance in BMC Client Management - Compliance Management is based on a number of specifically defined criteria. The values for these are located in the different inventories available in the console and the database. This information is collected by the agent via operational rules that are executed on the devices in your network and then uploaded to the master database. After the information is available, the compliance rules can calculate the compliance of a device about specific aspects of its configuration.

The following topics are provided:

- Compliance Base Information
- Compliance Evaluation
- Compliance Reports
- Report Results
- Criteria
- Compliance Results

Compliance Base Information

The compliance evaluation is based on data collected by the CM agent on the network devices which are stored in the central CM database and made available by the master.

Data

The following types of data stored in the CM database can be used to define the compliance of a device:

- basic device data which is provided directly by the agent of the respective device
- hardware or software information, which can be found in the hardware and software inventories
- security settings, which can be found in the security and patch inventories and
- custom settings, which are collected in the custom inventory.

Some of these inventories such as hardware and software are regularly updated by the agent, others like the custom, security and patch inventory, are filled in with their data by operational rules. Most of the relevant steps for these rules can be found in the following step classes (for more detailed information about the available steps and parameters refer to the respective topic in the Operational Rules section):

- **Security Inventory** - This step class collects specific security information about the Windows group policies such as log settings, administrator privileges, security settings, account settings, and so on It also contains a number of steps collecting Unix based security settings, such as run level commands, and so on All this information is collected in the security inventory.
- **Patch Management** - Via the steps of this class you can establish the patch inventory of a device, that is, collect the list of missing patches. This information is collected in the patch inventory.
- **Custom Inventory** - This class contains any specific type of inventory that you might want to know, such as the registry, ini file or environment values, printer information, and so on All collected information is part of the custom inventory.
- **Monitoring** - The steps in this class collect information about installed software, available disk space, memory usage, and so on All this information is collected in the custom inventory.
- **Power Management** - This class of steps collects the information about the Power Management or GreenIT settings of the devices, that is, hibernation and shutdown settings, and so on All this information is collected in the custom inventory.
- **Windows** - This step class provides steps with which general Windows information and its users can be collected, such as the logged users, registry and service information, and so on All this information is collected in the custom inventory.

The hardware and software inventory and parts of the custom inventory are automatically updated by the CM agent according to a specifically defined schedule. This schedule can be modified in its frequency and specific intermediary updates of the inventories can be requested and executed via operational rules as well. For more information about this subject refer to the Inventory manual.

Classes

All the data available for the compliance criteria as explained in the preceding paragraph is sorted into classes according to their type of origin, that is, by which type of inventory it was collected. In total the following data classes are available:

- Custom Inventory - this class provides the data for all criteria about the company custom defined inventory data, such as location, asset tags, and so on.
- Hardware Inventory - this class provides the data for all hardware related criteria.
- Patch Inventory - this class provides the data for all patch related criteria. Hidden patches will not be taken into account for compliance evaluation.
- Security Inventory - this class provides the data for all device security related criteria.
- Software Inventory - this class provides the data for all software related criteria.

- Basic - this class collects all basic device and general inventory data provided directly by the agent.

Tables

Most of the previously listed classes before collect huge amounts of different types of data. For easier management and usability these were sorted into different tables in a logical way. For example, the hardware inventory is sorted in tables according to the hardware attribute type, that is, BIOS, memory, processor, and so on It is from these tables that the individual criteria are selected for the compliance rules.

Compliance Evaluation

After the base data is collected and available in the database, the rules for compliance can be defined according to your policies. If a device is compliant or not is then evaluated based on the following elements:

- Compliance Criteria Groups
- Criteria Group Relation

The compliance criteria that are defined by the administrator are collected in criteria groups which can be put in relation to each other for logical operations. When the relation is evaluated for the device the result is either yes or no, and a device is considered compliant if the result is yes.

Compliance Criteria Groups

The criteria that must be fulfilled for compliance are collected in groups. A criteria group can contain only one criterion or it might have several. All the criteria defined within a group are connected via the AND operator, that is, the device must comply to criterion 1 AND criterion 2 AND criterion 3 ...

A compliance rule might have only one or several of these compliance criteria groups. The relation between these groups is defined by the function specified in the Group Relation option.

Criteria Group Relation

The relation equation defines how the different groups relate to each other, that is, how the compliance is evaluated. Three operators can be used to define this relation, AND, OR and *not* and any number of parentheses. Criteria groups can also appear more than once in a relation equation. To identify the different groups the equation uses their respective index which is attributed to the groups by their position in the list.

1 AND 2	A device is compliant if it fulfils all criteria of group 1 and all criteria of group 2.
1 OR 2	A device is compliant if it either fulfils all criteria of group 1 or all criteria of group 2.
NOT (1 AND 2)	A device is compliant if it does not fulfil the criteria of group 1 and the criteria of group 2.
NOT (1 OR 2)	Any device that either fulfils all criteria of group 1 OR all the criteria of group 2 is *not* compliant.
(1 AND 2) OR (1 AND 3)	A device is compliant if it either fulfils all of groups 1 and 2 OR all the criteria of groups 1 and 3.

NOT ((1 AND 2) OR (1 AND 3))	Any device that either fulfils all of groups 1 and 2 OR all the criteria of groups 1 and 3 is *not* compliant.

Compliance Reports

To make the compliance situation known also to other members in your company concerned with this subject a number of different reports can be generated and published. These template-based reports display a specific situation represented by a compliance rule. The report templates contain an executive summary, a report about compliance policy by criteria, by device group or by device.

Report Results

Each time a report is generated a new node is created under the **Report Results** node named using the local generation date and time of the computer on which the report is generated for the report as its name. Report results are stored in the database indefinitely. (This value can be modified in the database configuration file, for more information about this subject refer to paragraph CM Database in the Agent Module Parameters topic of the Reference section.)

When selecting a report result in the left window pane, the right window pane displays the following tabs for detailed information on the contents:

Parameter	Description
Name	This column lists all reports that were generated by their generation date and time in the default format defined in the user preferences or by its file name if one was defined in its properties.
XML Status	This field indicates the current status of the generated report in the XML format. Only reports with the status Available can be displayed and viewed. This field is only applicable to template-based reports.
HTML Status	This field indicates the current status of the generated report in the HTML format. Only reports with the status Available can be displayed and viewed. This field is only applicable to template-based reports.
PDF Status	This field indicates the current status of the generated report in PDF format. Only reports with the status Available can be displayed and viewed. This field is only applicable to template-based reports.
Report Name	This field displays the name of the report as defined in its properties.
Public Report	Defines if the report is to be generally accessible via the **Report Portal** .

Criteria

The **Criteria** tab displays the following information about the criteria groups of the selected compliance rule:

Parameter	Description
Status	This field displays the status of the compliance rule. When a compliance rule is newly created it will automatically be **inactive** . When a compliance rule is modified in any way, that is, criteria groups are added, removed or modified the compliance rule automatically becomes **inactive** . This means that all groups and devices, to which the compliance rule is currently assigned will not re-evaluate their scores anymore. This also means that any report of which at least one subreport is based on this compliance rule, or which is assigned to a group with this compliance rule will not be executed. After the compliance rule modification finished, you can manually reactivate the compliance rule by selecting the **active** value from the list.

Parameter	Description
Default Operator	This field defines the default relation that is established between the individual criteria groups when they are added to the rule, possible values are AND and OR.
Index	This field displays the index value for the defined criteria group.
Name	The fields of this column display the custom defined names of the criteria groups specified for this compliance rule.
Table	The fields of this column display the names of the database table from which the criteria were chosen for the criteria group.
Group Relation	This field defines the relation between the individual criteria groups. To uniquely identify the respective groups the syntax uses the Index value, which is assigned to the group due to its position in the list. Whenever new criteria groups are added to the rule they are automatically added as well to this relation field with the preselected default operator at the end of the equation. Groups can be related either by the AND or the OR operator, they can be grouped with parenthesis and they can be inversed via the *not* operator. Also, the criteria groups can be used more than once in the syntax, for example, *not* ((1 AND 2) OR 3) OR (1 AND 2 AND 3). The syntax must ALWAYS be verified that it is correct before activating the compliance rule, otherwise it cannot be activated.

Compliance Results

The **Results** tab displays the result of the compliance test of all assigned objects, that is, devices or groups in form of a pie chart with some further information. The pie chart is displayed in red, green, blue and gray, green representing all devices which are compliant, red all non-compliant devices, blue all devices that could not be evaluated due to missing data and gray those that have not yet been evaluated.

> **Note:**
>
> Be aware that any evaluation might take a while, depending on the overall load and group size. The newly evaluated data is displayed when you click **Refresh** or after the automatic refresh interval has elapsed.

Dynamic Groups in Compliance Management

The **Dynamic Groups** node provides access to all types of groups which are dynamically populated by another object. It can have one of the following subnodes:

- Device Groups being populated by the compliance rule
- Compliance Rule populating the device group

The following topics are provided:

- Evaluating dynamic groups for compliance
- Dynamic Device Groups in Compliance Management
- Compliance Rule

Evaluating dynamic groups for compliance

It is possible at any time to launch a manual re-evaluation of the device or of all members of the device group assigned to a compliance rule. This functionality is not available under a report. To do so, proceed as follows:

1. Select **Edit > Evaluate** .

The scores are now re-evaluated for all assigned devices and the display is updated once the evaluation has finished.

> **Note:**
>
> Be aware that only one compliance rule can be evaluated at a time by the master and depending on the overall load and group size this might take a few moments. The newly evaluated data is displayed when you click **Refresh** or after the automatic refresh interval has elapsed.

Dynamic Device Groups in Compliance Management

The **Device Groups** node displays the list of device groups that a compliance rule populates.

The table in the right window pane shows the following information about the device groups:

Parameter	Description
Status	The current status about the compliance license. If the license is valid this field remains empty, if there is a issue with the license it this field displays the reason for it, either License expired if the license is no longer valid, License exceeded, or Maximum License Count, if the maximum number of devices to evaluate were reached.
Name	This column displays the list of names of all device groups that the compliance rule populates.
Compliance	This field displays the type of population for the group, that is, if the group contains all devices compliant to the rule, the non-compliant ones or those that could not be evaluated for specific reasons.
Last Evaluation	This field displays the date and time of the last compliance evaluation of the object.

Assigning device groups to compliance management

To assign an existing device group to a compliance rule to populate it, proceed as follows. Be aware that only those device groups can be populated by a compliance rule that are not already populated by either a query or a directory server.

1. Select the compliance rule which is to populate a device group in the left window pane.
2. Select **Edit > Assign Device Group** .
   The **Assign to Device Group** pop-up menu appears.
3. Select the device group from the window.

4. Click **OK** to confirm the assignment.
   The **Desired Compliance** window appears.

> **Note:**
>
> Here you must select the type of the population for the group.

5. Select the respective radio button to have a group collecting all compliant, not compliant or all devices for which the evaluation was impossible.
6. Click **OK** to confirm and close the window.
   The device group will be added to the table of assigned device groups.

Under the main **Device Groups** node the icon of the group will change to its compliance rule populated one and the members of the group will now be managed by the results of the rule.

Compliance Rule

The **Compliance Rule** node provides access to the compliance rule populating the currently selected device group. Compliance rules can define the group membership according to different criteria, that is, a compliance rule can populate a group with all devices which are compliant with the rule, all devices which are not compliant, or those devices which could not be evaluated.

Parameter	Description
Name	This field displays the name of the currently selected object.
Compliance	The value in this field displays the criteria which defines the group membership, that is, if the group members are compliant, non-compliant or those which could not be evaluated.
Last Evaluation:	This field displays the date and time of the last compliance evaluation of the object.
Evaluation Status	This field displays the evaluation status of the compliance rule, possible values are Inactive, Evaluated, Evaluation Failed, Not Evaluated, Evaluating and Evaluation Scheduled.

Assigning compliance rules to device groups

To assign a compliance rule to a device group proceed as follows:

1. Select the **Compliance Rule** node in the left window pane.
2. Select the **Edit > Assign Device Group** icon.
   The **Assign a Compliance Rule** pop-up menu appears.
3. Select the device group from the window.
4. Click **OK** to confirm the assignment.
   The **Desired Compliance** window appears.

> **Note:**

Here you must select the type of the population for the group.

5. Select the respective radio button to have a group collecting all compliant, not compliant or all devices for which the evaluation was impossible.
6. Click **OK** to confirm and close the window.
   The device group will be added to the table of assigned device groups.

Under the main **Device Groups** node the icon of the group will change to its compliance rule populated one and the members of the group will now be managed by the results of the rule.

Overview of SCAP compliance

This topic includes:

About SCAP compliance in BCM

BMC Client Management is a certified USGCB and FDCC scanner.

- It can provide compliance assessment against all security checklists in USGCB and FDCC.
- Assessments can be done at a group or device level and details can be provided so remediation actions are obvious to understand.
- Reports can be generated to show the compliance or non-compliance of devices, as well as show the reason for non-compliance.

BMC Client Management allows the desktop administrator to review the output of specific SCAP jobs that were automatically performed. It provides different views, from a high-level dashboard with results for all security checklists (SCAP packages) and drilling down into one of them, as well as views on either results for an individual device, or results for a whole package or a specific check (rule). For a particular rule, the administrator can get a full description, including details, fix details, links available in the checklist, and so on. This allows the administrator to prove to an auditor that the rules are correctly performed by showing the history of compliance and remediation for a given device. It also provides the reason why a device is or is not compliant with a rule (that means, the value that was found at scan, on what date, using what version, and so on).

This data allows the administrator to make a decision, on what changes are needed to make the computers compliant again, whether via CM or another solution. It also allows the administrator to test that the applied fixes actually fix the targeted compliance issue(s), for example by triggering a

rescan of the target computer(s). SCAP compliance in CM also allows the administrator to roll out the changes to all affected devices and measure the progress in reaching compliance, for example by newly scanning the fixed hosts. If the fix can be done via CM , the administrator can create an automated remediation rule that dynamically applies to all affected devices.

The reporting feature, integrated with SCAP compliance allows the administrator to expose the findings to emanagement, to allow them to check the compliance status. Whenever a computer becomes non-compliant (which could be caused by an SCAP template update, or because the computer settings have changed), the administrator is notified proactively.

SCAP compliance allows the Client Management administrator to select the security checklists to scan the environment. It allows him to scan the right sets of computers with the right checklists and to schedule these scans as required. CM SCAP compliance allows the administrator to import new and updated security checklists when they become available, and to delete old checklists that are not used anymore or for which compliance history is no longer needed. The integrated reporting feature allows to create and configure reports with various levels of details depending on the target audience, such as a desktop administrator or a manager.

BMC Client Management allows the desktop administrator to review the output of specific SCAP jobs that were automatically performed. It provides different views, from a high-level dashboard with results for all security checklists (SCAP packages) and drilling down into one of them, as well as views on either results for an individual device, or results for a whole package or a specific check (rule). For a particular rule, the administrator can get a full description, including details, fix details, links available in the checklist, and so on. This allows the administrator to prove to an auditor that the rules are correctly performed by showing the history of compliance and remediation for a given device. It also provides the reason why a device is or is not compliant with a rule (that means, the value that was found at scan, on what date, using what version, and so on).

This data allows the administrator to make a decision, on what changes are needed to make the computers compliant again, whether via CM or another solution. It also allows the administrator to test that the applied fixes actually fix the targeted compliance issue(s), for example by triggering a rescan of the target computer(s). SCAP compliance in CM also allows the administrator to roll out the changes to all affected devices and measure the progress in reaching compliance, for example by newly scanning the fixed hosts. If the fix can be done via CM , the administrator can create an automated remediation rule that dynamically applies to all affected devices.

The reporting feature, integrated with SCAP compliance allows the administrator to expose the findings to management, to allow them to check the compliance status. Whenever a computer becomes non-compliant (which could be caused by a SCAP template update, or because the computer settings have changed), the administrator is notified proactively.

SCAP compliance allows the Client Management administrator to select the security checklists to scan the environment. It allows him to scan the right sets of computers with the right checklists and to schedule these scans as required. CM SCAP compliance allows the administrator to import new and updated security checklists when they become available, and to delete old checklists that are

not used anymore or for which compliance history is no longer needed. The integrated reporting feature allows to create and configure reports with various levels of details depending on the target audience, such as a desktop administrator or a manager.

CM SCAP compliance allows managers to review reports of the current situation for the different security checklists that must be applied as well as to review the compliance status history for a given checklist.

Compliance Components

The BMC Client Management implementation includes the following components:

- Extensible Configuration Checklist Description Format (XCCDF)
  The XCCDF is an XML specification for structured collections of security configuration rules used by OS and application platforms. It specifies security checklists, benchmarks and configuration documentation. This file defines the rules to which all devices in the network must comply and against which they are checked. This is the benchmark.
- Open Vulnerability and Assessment Language (OVAL)
  The OVAL is an XML specification for exchanging technical details on how to check systems for security-related software flaws. It is used to encode and transmit security information and system details. This is the actual execution of the compliance tests.
- Asset Reporting Format (ARF)
  ARF is an open specification that provides a structured language for exchanging per-device assessment results data between assessment tools, asset databases, and other products that manage asset information.
- Asset Identification
  One of the primary requirements for performing asset management is the ability to identify assets based on some set of data known about them. Asset identification, the use of attributes and methods to uniquely identify an asset, allows for correlation of data across multiple sources, reporting of asset information across different organizations and databases, targeted actions against specific assets, and usage of asset data in other business processes.
- Common Platform Enumeration (CPE)
  The CPE is a naming convention for hardware, OS and application products present among an enterprise's assets. For identifying these assets, the CPE system also uses identifiers. The identification process then triggers IT management tools to make fully or partially automated decisions regarding the assets. This defines what is applicable to what, that is, which rule is for which OS or application, and so on.
- Common Configuration Enumeration (CCE)
  These lists provide unique identifiers to security-related system configuration issues in order to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools.

- Common Vulnerabilities and Exposures (CVE ®)
  This is a dictionary of common names (that is, CVE Identifiers) for publicly known information security vulnerabilities. CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other.
- Common Vulnerability Scoring System (CVSS)
  CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability.
- Common Configuration Scoring System (CCSS)
  This is a system for measuring the relative severity of system security configuration issues. BMC Client Management supports CCSS scores when that score is used in the @weight attribute within XCCDF rules.
- Trust Model for Security Automation Data (TMSAD)
  This is a specification for using digital signatures in a common trust model applied to other security automation specifications. BMC Client Management can import SCAP content with Trust Model for Security Automation Data (TMSAD) signatures but does not verify them. The generated XML report does not include TMSAD signatures.

Common Use Cases of SCAP

- Security configuration verification
- Comparing settings in a checklist to a system's actual configuration
- Verifying configuration before deployment, auditing/assessing/monitoring operational systems.
- Mapping individual settings to high-level requirements
- Verifying patch installation and identifying missing patches
- Checking systems for signs of compromise
- Known characteristics of attacks

Compliance licenses

SCAP compliance as well as the custom compliance are both part of the compliance license.

To be able to remedy some of the discovered compliance faults you most probably also need the patch license.

Compliance capabilities and access rights

To be able to work with SCAP compliance and its remediation, an administrator needs specific capabilities and access rights for the different objects involved with compliance.

Compliance Management

- The capability **Compliance Management** - View is required to access the compliance feature.
- The capability **Compliance Management** - Manage is required to to import/remove checklists, to create/delete SCAP jobs and to add/remove checklists to/from SCAP jobs.
- The capability **Compliance Management** - Assign is required to assign/unassign devices /device groups/reports to a SCAP job.
- The capability **Compliance Management** - Schedule is required to schedule the actual execution of a SCAP job.

If you also have the patch license for remedying vulnerabilities you need the patch capabilities as well. These are detailed in the patch manual.

Scap job wizard

The **SCAP Compliance Wizard** wizard guides you thought the creation, definition and scheduling of the individual SCAP jobs.

The wizard is available directly on the main **Wizards** menu from anywhere in the console, and in the specific functionalities of the **SCAP Compliance** .

The following topics are provided:

- Defining the SCAP job
- Defining the SCAP job targets
- Defining the SCAP job identity
- Defining SCAP job deviations
- Defining the SCAP job schedule
- Defining SCAP report generation

Defining the SCAP job

In this first step, the SCAP job and all its specific parameters must be defined.

> **Note:**
>
> Be aware, that you need to already have downloaded the package you want to use, for example from the [NVD (National Vulnerability Database) of the NIST (National Institute of Standards and Technology)|http://web.nvd.nist.gov/view/ncp/repository] website, before you can define a SCAP job. It would even be easier, if you had not only downloaded but already imported it into CM , however, this is not mandatory, it can also be done during the SCAP job wizard.

To do so, proceed as follows:

1. Enter a self-explicatory name for the new SCAP job into the **Name** box.

> If you leave this text box empty, it is automatically filled with the name of the benchmark once you selected it.

2. *Optional:* Enter some additional explanation into the **Notes** box.
3. *Optional:* Select the directory in which the new SCAP job is to be created in the **Folder** box. By default it is created directly under the main node.
4. Define which SCAP package to use. For this you have two options, either to use a package you already downloaded and put at disposal or you can download a new one. To use an existing one proceed as follows:
    a. Click **Use an existing package** .
    The **Select a SCAP Package** displays displaying all packages that are currently available for scanning.
    b. Select the package from the list.
    c. Click **OK** .
    The package is added into the **Name** box and all following fields are filled in automatically, if only one choice is available for each. If several choices are available for fields, you need to individually select them.
    d. *Optional:* Select the data stream to use in the **Data Stream** box if the package has more than one and you want to use another than the preselected data stream.
    e. *Optional:* Select the benchmark to use in the **Benchmarks** box, if the package has more than one and you want to use another than the preselected benchmark.
    f. *Optional:* Select the profile to use in the **Profile** box, if the package has more than one and you want to use another than the preselected profile or no profile at all. If you select no profile, all rules in the package are executed. If you select a profile, only the rules included in the profile are run.
5. To import a new package proceed as follows:
    a. Click **Import a new package** .
    The **Select an SCAP Package** appears.
    b. Browse to the directory into which you downloaded the new package and select it.
    c. Click **OK** .
    The package is unzipped, parsed, added to CM , and added as well into the **Name** box in this window, and all following fields are filled in automatically, if only one choice is available for each. If several choices are available for fields, you need to individually select them.
    d. *Optional:* Select the data stream to use in the **Data Stream** box, if the package has more than one and you want to use another than the preselected data stream.
    e. *Optional:* Select the benchmark to use in the **Benchmarks** box, if the package has more than one and you want to use another than the preselected benchmark.

f. *Optional:* Select the profile to use in the **Profile** box, if the package has more than one and you want to use another than the preselected profile or no profile at all. If you select no profile, all rules in the package are executed. If you select a profile, only the rules included in the profile are run.

6. If the package is all new, click the **Validate SCAP Package** button, to ensure that the package is compliant with the Schema and Schematron rules.

> It is possible to download SCAP packages from many different sources, therefore it is possible that the downloaded data is not 100% compliant with the Schema (XSD) and Schematron rules. It is therefore important to ensure that the content is compliant, and this validation operation verifies all these Schema and Schematron rules.

> If the package is already verified, the information in the **SCAP Package Validation** panel indicates it together with the date and time at which the package was verified.

If the package is not valid, an error window opens. To see the errors click the **See Details** button. A browser page opens and displays the detailed eror report. If the package is of version 1.0 or 1.1, the **SCAP Package Validation** window appears. Select the use case for which the package is to be used and click **OK** .

> **Note:**
>
> The use case is normally preselected. Selecting another might lead to a failed package verification.

7. Select the use case to attribute to this package from the **Use Case** list.
8. Click **OK** .
9. Click **Next** to continue with the target selection.

Defining the SCAP job targets

In this step, the target devices and device groups are selected. A SCAP job can contain device groups and individual devices at the same time.

To assign a device or device group to the SCAP job, proceed as follows:

1. Click **Assign a device group to a SCAP job** or **Assign a device to a SCAP job** / on top of the list box.
   The **Assign Target Devices or Groups** pop-up windows appears, displaying all available devices and groups.
2. Select the desired devices or device groups or both from the window.
3. Click **OK** to confirm the assignment and close the window.
   The selected targets will be added to the list.
4. Click **Next** to continue with the next step.

Defining the SCAP job identity

In this view you can define with which user credentials the tests are run. This might be important for certain tests that need to access specific information that is not available for any type of user.

1. Select the radio button for the respective user.

   > **Note:**
   >
   > The system user is the default selection and should be used for most of the tests. It has the necesary permissions to recover most information apart from some very specific registry hives.

2. Click **Next**.

Defining SCAP job deviations

This step allows you to specify SCAP rule deviations. A rule deviation is a rule for which it does not matter, if it succeeds or fails on the targets, as its scan results are considered as passed in global compliance.

Some rules that are included in the benchmarks can be specified as deviations, because, for example, they are not applicable to a specific operating systems, or a specific rule currently is not applicable for your internal regulations, and so on.

These deviations can be modified at any moment and can also have a deadline. This means that for example a rule is considered a deviation until December 31st, because until then a specific requirement is not applied in your organization, but from the 1st of January onwards it will be. Once the expiration date is reached, the deviation is automatically removed and the rule result included in the global compliance.

> **Note:**
>
> Be aware that this does not impact any scans and reports already run before the expiration date, these remain as they are.

To declare a rule a deviation proceed as follows:

1. Click **Add SCAP Rule Deviation** on top of the list box.
   The **SCAP Rule Deviation** dialog box appears.
2. Select the rule to specify as deviation.

   > You can select more than one rule at a time by holding the CTRL key while selecting.

3. *Optional:* Click the calendar icon, if the rule deviation is to expire at a specific date. If the deviation is unlimited, do not modify this box.

   > To clear the expiration date click .

4. Enter an explanation into the **Notes** box, why this rule is to be a deviation.

   > The contents of this text box is used in the SCAP job result report for explanation.

5. Click **OK** to add it to the list of deviations and close the window.
6. Click **Next** to continue with the definition of the SCAP job schedule.

Defining the SCAP job schedule

This step of the wizard concerns the scheduling of the SCAP job on the targets. This dialog box appears either the predefined schedule of an existing group or the default schedule for a new group.

1. Define the date and time at which the assignment of the SCAP job to the targets is to be effected in the **When do you want to run this job?** box.
2. Define the date and time at which the actual scan of the SCAP job is to take place in the **Do you want to configure a window in which this job can run?** box.
3. (Optional) Depending on this choice you might have to fill in more boxes and make more selections to define your execution schedule.
4. (Optional) Check the **Do you want to run a report after this scan?** to generate a specific report after the scan has finished.
5. Click **Finish** if you do not want to define a report or click **Next** to continue with the next step to define the report to generate.

Defining SCAP report generation

This step of the wizard allows you select a SCAP report and to schedule its generation at regular intervals for the current SCAP job. By default the first time this report is generated is one day after the SCAP job was launched. This dialog box appears the predefined schedule for reports.

1. Select the report to generate from the **Which report do you want to run?** box.
2. Define at which moment the report generation is to start by selecting the respective option in the **When do you want this report to run?** box.
3. *(Optional)* Depending on this choice you might have to fill in more boxes and make more selections.
4. *(Optional)* If the report is to be generated at regular intervals select when this schedule is to start in the **Do you want to configure a window in which this report can run?** box.
5. *Optional:* Depending on this choice you might have to fill in more boxes and make more selections to define your generation schedule.
6. Click **Finish** .

SCAP Implementation Statement

The SCAP features in BMC Client Management comply with the Technical Specification for the Security Content Automation Protocol (SCAP): Version 1.2.

Using features in the BMC Client Management console, you import SCAP content from third-party sources, such as the NIST NVD National Checklist Program repository.

The imported content, known collectively as a SCAP Benchmark, is an organized collection of the following SCAP components: security checklists in Extensible Configuration Checklist Description Format (XCCDF), configuration assessments in Open Vulnerability and Assessment Language (OVAL) and platform-specific content in a Common Platform Enumeration dictionary (cpe-dictionary) file. Starting from SCAP 1.2, the DS or data stream collection format is an additional XML file format used for expressing the SCAP Benchmark. Key goals are to group all the other files together and to provide catalog capabilities so each component can reference the others.

Validation against the SCAP schemas and schematrons occurs during the import. An imported benchmark is a well-formed XCCDF-expressed data stream. You can import multiple SCAP Benchmarks, named SCAP packages, in the BMC Client Management console.

After importing the SCAP Benchmarks, you create, run, and manage SCAP Compliance Jobs. Each job selects a data stream in the collection, an XCCDF checklist in the data stream and, optionally, an XCCDF profile in the checklist and targets (devices or device groups or both). Both data stream and data stream collection are new concepts in SCAP 1.2. BMC Client Management creates a data stream and a data stream collection when processing SCAP 1.0/1.1. Therefore, users can still manage these entities whatever the underlying SCAP content version. SCAP compliance jobs are fully integrated into the BMC Client Management product and include all standard job features of the product, such as dynamic groups to automatically collect target

devices based on rules; GUI-based job editing; automatically recurring job scheduling; automated email notifications and events to report job results; and role-based access control (RBAC) on all activities.

OVAL checks are processed on the targets. Their results are used by BMC Client Management in forming the final ARF and XCCDF results (ARF for SCAP 1.2 only, XCCDF for all versions). The BMC Client Management console shows the result state for each rule. Results are organized in several views:

- a dashboard providing an overview of the rule results
- one view shows results by target
- another view shows results for each rule across all targets
- a report showing the results in a browser in HTML format

Rule results can be one of nine values, including Pass, Fail, Error, and Unknown.

Results are generated as XML files that are compliant with both the SCAP (for ARF) and XCCDF specifications. An HTML report is automatically generated by applying an XSLT file to the XCCDF report. All of these files can be either downloaded (XML) or visualized using a Web browser (HTML).

The following topics are provided:

Capabilities and Platforms

BMC software, Inc. asserts that BMC Client Management (BMC Client Management) version 12.00.00 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.0, 1.1 and 1.2 as described in NIST IR 7511 Revision 3 for the following SCAP capabilities and supported platform family:

Capabilities

- Authenticated Configuration Scanner
- Common Vulnerabilities and Exposures (CVE) Option

Platform Families:

- Microsoft Windows 7, 64 bit

- Microsoft Windows 7, 32 bit
- Microsoft Windows Vista, SP2
- Microsoft Windows XP Pro, SP3
- Red Hat Enterprise Linux 5 Desktop, 64 bit
- Red Hat Enterprise Linux 5 Desktop, 32 bit

BMC Client Management additionally provides SCAP capabilities for systems such as MAC OS X and other Windows/Linux flavors, but these are not certified.

Compatibility

SCAP 1.2 Compatibility

BMC Client Management conforms to the specifications of the Security Content Automation Protocol, version 1.2 (SCAP 1.2), as outlined in NIST Special Publication (SP) 800-126 rev 2. As part of the SCAP 1.2 protocol, BMC Client Management assessment capabilities were expanded to include the consumption of source data stream collection XML files and the generation of well-formed SCAP result data streams.

To exercise this capability, users can download the SCAP 1.2 content from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.2 compliant content, and perform assessments in a similar manner as with BMC Client Management custom compliance.

The following table provides a summary of the individual SCAP Component Standards supported by BMC Client Management as is required by the SCAP 1.2 specifications:

Component	Version	Description
AI	1.1	Asset Identification (AI) is a format for uniquely identifying assets based on known identifiers and/or known information about the assets. Utilizing the AI standard, BMC Client Management is capable of reporting the necessary information to uniquely identify assets based on known identifiers and/or known information about the target systems being assessed.
ARF	1.1	The Asset Reporting Format (ARF) is a format for expressing the transport format of information about assets and the relationships between assets and reports. ARF describes a data model for expressing information about assets and the relationships between assets and reports. The BMC Client Management ARF report will contain component results (XCCDF, check results), information about the target asset (utilizing the Asset Identification, or AI, data model as described above), and the SCAP source data stream collection.
CCE	5	BMC Client Management supports the Common Configuration Enumeration (CCE). XCCDF rules may reference one or more CCE identifiers. These identifiers can be visualized through the properties pop-up dedicated to the XCCDF rules details. This pop-up is available where XCCDF rules are enumerated, including the SCAP jobs results view which provides execution status for each XCCDF rule. To display this information, double-click the rule or click **Edit > Properties** . The displayed pop-up will include the list of CCE identifiers associated to the XCCDF rule, and may display additional information such as description, dates and NIST SP 800-53 compliance mappings. In order to get this additional information, the correct CCE lists must be imported in the product (see section Import CVE and CCE lists for more information). CCE is a nomenclature and dictionary of software security configurations.
CCSS	1.0	BMC Client Management supports the Common Configuration Scoring System (CCSS). CCSS is a system for measuring the relative severity of system security configuration issues. Whereas CVSS represents a scoring system for software flaw vulnerabilities, CCSS addresses software security

Component	Version	Description
		configuration issue vulnerabilities . Per NIST SP800-126r2, CCSS data is not directly useful in the same way as CVSS data. CCSS data needs to be considered in the context of each organization's security policies and in the context of dependencies among vulnerabilities. BMC Client Management supports CCSS scores when those scores are used in the @weight attribute within XCCDF rules.
CPE	2.3	BMC Client Management supports the Common Platform Enumeration (CPE). The BMC Client Management SCAP engine implements the required CPE standards (Naming, Name Matching, Dictionary and Applicability Language) but does not natively contain CPE dictionaries. Instead, it makes use of CPE definitions included in SCAP source data streams CPE is an SCAP nomenclature and dictionary of hardware, operating systems, and applications. The SCAP source data stream that BMC Client Management uses for SCAP compliance scans must include CPE content. In the SCAP result data stream produced by BMC Client Management , when a rule applies to a specific hardware, operating system, or application, those objects are identified using CPE nomenclature. In the XML results file, to identify BMC Client Management as the benchmarking tool, the <TestResult> element sets the test-system attribute to cpe:/a:bmc:bca:12.0.0.
CVE	n/a	BMC Client Management supports the SCAP Common Vulnerabilities and Exposures (CVE) enumeration. XCCDF rules may reference one or more CVE identifiers. These identifiers can be visualized through the properties pop-up dedicated to the XCCDF rules details. This pop-up is available where XCCDF rules are enumerated, including the SCAP jobs results view which provides execution status for each XCCDF rule. To display this information, double-click the rule or click **Edit > Properties** . The displayed pop-up will include the list of CVE identifiers associated to the XCCDF rule, and may display additional information such as description, dates and references with links to security advisories. In order to get these additional information, the correct CVE lists must be imported in the product (see section Import CVE and CCE lists for more information). CVE is an SCAP nomenclature and dictionary of security-related software flaws and vulnerabilities.
CVSS	2.0	BMC Client Management supports the SCAP Common Vulnerabilities and Exposures (CVE) enumeration. The Common Vulnerability Scoring System (CVSS) is a system for measuring the relative severity of software flaw vulnerabilities. BMC Client Management displays the CVSS impact-metric value associated with a rule in the exported results file. CVSS is a SCAP specification that describes the characteristics and impacts of IT vulnerabilities. The SCAP source data stream that BMC Client Management uses for SCAP compliance scans can optionally include impact-metric values for rules. If a rule in the imported benchmark includes an impact-metric value, that value is included in the SCAP result data stream.
OVAL	5.10.1	BMC Client Management supports the Open Vulnerability and Assessment Language (OVAL). OVAL is an SCAP XML language for representing system configuration information, assessing computer state, and reporting assessment results. A proprietary OVAL interpreter based on the open-source OVAL Definition Interpreter (ovaldi) processes the OVAL tests. The OVAL interpreter is bundled with the BMC Client Management agent, a BMC Software component installed on every computer managed by BMC Client Management . OVAL content is imported into the BMC Client Management console as part of the SCAP data stream. OVAL content only with optional OVAL variables may also be supplied. OVAL is used to identify vulnerabilities and issues. Common examples of the use of OVAL files are: • the checking language referenced from a separate XCCDF file, • the checking language referenced from a checklist component of a SCAP source data stream, • the checking language referenced from a CPE dictionary component of SCAP source data streamThe OVAL component will contain the definitions, tests, and the state a target system is expected to exhibit. When BMC Client Management encounters a reference to an OVAL definition, it parses the specific OVAL components/files and uses those referenced definition identifiers to look up the appropriate tests to be executed. Each OVAL definition may be comprised of one-to-many OVAL tests; the results of which can be logically combined to

Component	Version	Description
		enumerate an overall definition result. The BMC Client Management evaluation engine is the controller for parsing the required tests, collecting the appropriate system characteristics, evaluating the collected information against the expected state, and recording the success, failure, or any error conditions of a given test. BMC Client Management supports components specified using versions 5.3 to 5.10 of the OVAL language.
TMSAD	1.0	BMC Client Management can import SCAP content with Trust Model for Security Automation Data (TMSAD) signatures but will not verify them. The generated XML report will not include TMSAD signatures.
XCCDF	1.2	BMC Client Management supports the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a language for authoring security checklists/benchmarks and for reporting results of evaluating them.. The source data stream that BMC Client Management uses for SCAP compliance scans must be well-formed XCCDF. The result data stream that BMC Client Management produces is well-formed XCCDF. BMC Client Management 's capabilities include the ability to assess a target system based on rules defined using XCCDF, versions 1.1.4 and 1.2. XCCDF is used throughout BMC Client Management as the required XML schema for benchmarks, as well as the checklist definition schema within SCAP source data streams. This ensures that outside compliance benchmarks/data streams, such as those provided by the NIST National Checklist Program, Federal Desktop Core Configuration (FDCC), or the US Government Configuration Baseline (USGCB), can be used alongside custom or CIS benchmarks. The XCCDF format specifies the required tests for one or more profiles. At SCAP job configuration time, a user will be able to select any of the given profiles specified in a XCCDF, and BMC Client Management will assess the configuration rules included in the selected profile. With BMC Client Management , an evaluation check can be specified in two ways: • Through a separate Open Vulnerability Assessment Language (OVAL) file, or • Through a reference to OVAL definitions contained in the same SCAP data stream.The relevant descriptions, CCE ID's and other related artifacts entered in the XCCDF will be preserved and included in the XML and HTML results produced by a BMC Client Management assessment.

SCAP 1.0 and 1.1 Compatibility

BMC Client Management natively supports the older SCAP 1.1 and 1.0 specifications. It does this by detecting the version of OVAL or XCCDF specified in the content and then processing it based on the selected OVAL probes. The user does not need to do anything special; support is automatic.

SCAP 1.1 support includes:

- The eXtensible Configuration Checklist Description Format (XCCDF), version 1.1.4
- The Open Vulnerability and Assessment Language (OVAL), version 5.8
- The Common Configuration Enumeration (CCE), version 5
- The Common Platform Enumeration (CPE), version 2.2
- The Common Vulnerabilities and Exposures (CVE)

- The Common Vulnerability Scoring System (CVSS), version 2

SCAP 1.0 support includes:

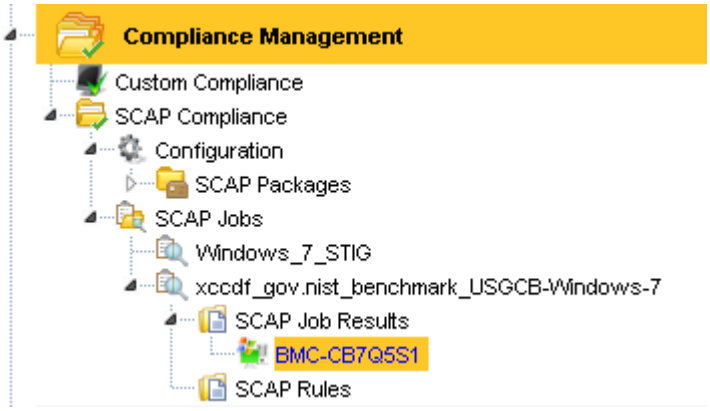
- The eXtensible Configuration Checklist Description Format (XCCDF), version 1.1.4
- The Open Vulnerability and Assessment Language (OVAL), version 5.3 and 5.4
- The Common Configuration Enumeration (CCE), version 5
- The Common Platform Enumeration (CPE), version 2.2
- The Common Vulnerabilities and Exposures (CVE)
- The Common Vulnerability Scoring System (CVSS), version 2

Unsupported check systems handling

BMC Client Management SCAP implementation supports the Open Vulnerability and Assessment Language (OVAL) check system. As a consequence, the engine can process XCCDF checks referencing OVAL definitions and will not process those for which the checking system is all but OVAL. When processing an XCCDF rule, the engine will verify each associated check and reject entries that either cannot be resolved or that have an unsupported check system. Then, rules for which all the entries are rejected cannot be checked and are managed accordingly. The SCAP job log file provides a first indication in this case. Below is a log extract for rules associated to the unsupported Open Checklist Interactive Language (OCIL):

```
...
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Enable_screen_saver)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Password_protect_the_screen_saver)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Screen_Saver_timeout)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Turn_off_Help_Ratings)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Do_not_preserve_zone_information_in_file_attachments)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Hide_mechanisms_to_remove_zone_information)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Notify_antivirus_programs_when_opening_attachments)
2014/06/24 16:46:24 ScapLib I   [10552] Processing Rule.NotChecked (xccdf_gov.
nist_rule_user_setting_OCIL-Prevent_users_from_sharing_files_within_their_profile)
...
```

Product output makes it possible to determine which rules have not been processed. The SCAP Job Results view applied to targets may include such rules with status 'Not Checked':



Do not preserve zone information in file attac...	Not Checked
Enable screen saver	Not Checked
Hide mechanisms to remove zone information	Not Checked
Notify antivirus programs when opening atta...	Not Checked
Password protect the screen saver	Not Checked
Prevent users from sharing files within their ...	Not Checked
Screen Saver timeout	Not Checked
Turn off Help Ratings	Not Checked

OVAL Only SCAP Content

It is required for SCAP consumers to be able to process OVAL only contents. OVAL only content includes a single OVAL definitions file and may include one additional external OVAL variables file. While this goal can be achieved manually using the mtxoval binary through either a Windows console or Unix terminal, CM SCAP implementation makes it possible to import, validate and display results in console for such content.

In order to realize this task, the import operation creates a virtual benchmark and several XCCDF rules, one for each OVAL definition. Because the process does not create a profile, all the rules are selected by default. The imported content is initially declared SCAP 1.0 unless OVAL version 5.8 is detected. In that case, it is turned into SCAP 1.1. Note, that since the SCAP version is either 1.0 or 1.1, other virtual entities are created, including a data stream collection and a data stream. As a consequence, administrators can visualize all these components from console, up to the XCCDF rules connected to the OVAL definitions. For easing this task, both the OVAL definitions title and description are copied into their corresponding XCCDF rules.

The import operation shall respect the import rules. If a single OVAL definitions file must be imported, then operation can be applied on this single file. If an external OVAL variables file must be imported at the same time, then an archive file including the OVAL definitions file and the OVAL variables file must be imported instead. Note, that default scoring is applied to the virtual benchmark where all the rules are identified with a default 1.0 weight.

OVAL Variable Export

BMC Client Management SCAP implementation does not support OVAL variable export with multiple values. While this mechanism is not supported, SCAP content using multiple values export can be consumed but only the last exported value is taken into account, which can cause unexpected results.

Required settings

BMC Client Management SCAP implementation does not require special settings in order to execute. To fulfill this assertion, the product includes two versions of the OVAL engine for Windows systems. Default binary **mtxoval.exe** implements all the OVAL tests enumerated in section [SCAP OVAL tests|Tools#id10AFB0DH05Z] but requires Microsoft .NET Framework 4 to be installed on target systems. If this component is not installed, the lightweight binary **mtxoval_u.exe** is used instead. As a consequence, all the OVAL probes are supported except the Windows cmdlet. When using **mtxoval_u.exe** , OVAL definitions making reference to the Windows cmdlet OVAL probe are returned with status unknown.

File organization

The SCAP engine is a SCAP content consumer. Therefore, it processes SCAP 1.0, 1.1 or 1.2 content and produces results files accordingly. During the scans, the engine generates different outputs such as log files, temporary files, and so on.

Each SCAP content is processed through a SCAP job. These jobs own a private identifier which at the same time defines a proprietary folder. For Windows systems, the default jobs folder is located in **C:\Program Files\BMC Software\Client Management\Client\data\ScapInventory\jobs** . This folder, which is initially empty, will be populated with subfolders each time a new job is assigned to the device. Folders are recursively removed if the underlying SCAP jobs are unassigned.

The job subfolder is created when a new SCAP job is assigned to the device, and more precisely when the content to execute is delivered. The subfolder originally includes the **scap.bin** file, which is a ciphered version of the SCAP package to process. In other words, the SCAP content is delivered through a secured channel since the **scap.bin** file cannot be used except by the BMC SCAP engine. This secured content is created during the package import and cannot be altered during distribution. This is a guaranty offered to customers to control the SCAP data, from the package import (and optionally validation), to the package execution.

When the SCAP job schedule triggers execution, attached content is deciphered and extracted as **package.zip** file. This ZIP archive includes the real SCAP content. Note, that content can be either a single XML file (when processing SCAP 1.2 content) or may include several XML files. Thereafter, **package.zip** is inflated and content is extracted in the **package** subfolder. All of these operations are performed each time a scan must be executed. As a consequence, updating the **package** folder content between two runs is useless since the next execution will regenerate its content from the ciphered file.

The SCAP scan is executed, using the **package** folder content as input. It then generates different files:

mtxscap.log file	This log file includes details about the SCAP scan execution such as CPE evaluation, XCCDF profile operation and so forth. Note, that this log file is available from the console UI.
xccdf-results.xml file	This XML file includes the XCCDF results. It is generated for any content unless errors occur. Note, that only XCCDF TestResult is provided and reference to the source XCCDF benchmark is registered.
xccdf-summary.json file	This JSON file includes a subset of the XCCDF results. It has a proprietary format and is mainly used for updating the results in the console UI.
arf-results. file	This XML file includes the ARF results. It is generated for SCAP 1.2 content only.
ScapInventory.xml file	This XML file includes a subset of the XCCDF results. It has a proprietary format and is mainly used for updating the results in the console UI.

temp folder

The **temp** folder is dedicated to the various OVAL evaluations. The SCAP engine wrapped by the **mtxscap.exe** binary makes use of **mtxoval.exe** for OVAL evaluation. As a consequence, the **mtxoval.exe** binary is executed several times at different stages of the scan. These temporary folders are organized using two levels. The first-level defines a temporary folder for each OVAL definitions content while the second level defines a temporary folder for each **mtxoval.exe** execution applied to the OVAL definitions content. Note, that OVAL definitions content can be either a file (SCAP 1.0 and 1.1) or a component (SCAP 1.2). The first temporary folder includes two static files which provide indication of the OVAL definitions content:

scap_file.txt file	This plain text file includes the path to the OVAL definitions file. This can be a dedicated OVAL file (for SCAP 1.0 and 1.1 content) or the data stream collection file (for SCAP 1.2 content).
scap_component.txt file	

	This plain text file includes the component identifier used for retrieving the OVAL definitions content in the SCAP 1.2 data stream collection. This information is not used for SCAP 1.0 and 1.1 content, in which case the file remains empty.

When **mtxoval.exe** is executed, a dedicated temporary folder is created and assigned to the execution. These temporary folders are created inside the folder dedicated to the underlying OVAL content. For instance, if OVAL content references folder **01c276fecc79418a46978e86549539bb** , then the first **mtxoval.exe** execution will be assigned to **01c276fecc79418a46978e86549539bb\1** , the second execution to **01c276fecc79418a46978e86549539bb\2** and so forth. These OVAL dedicated temporary subfolders may include different files:

mtxoval.log file (**ovaldi.log** during execution)	This file will include the detailed logs generated by **mtxoval.exe** .
oval_directives.xml file	This XML file includes the OVAL directives to be used during execution. These directives can be configured using the predefined values (full with system characteristics, full without system characteristics or thin) applied to the ScapInventory module.
system-characteristics.xml file	This XML file includes the gathered system characteristics. Because we create a temporary folder each time **mtxoval.exe** is run, the system characteristics files cannot be reused. Instead, the content is written once during the binary execution.
oval_definitions.xml file	This XML file includes the list of OVAL definitions to evaluate. Note, that this file is optional in which case all of the OVAL definitions are processed.
oval_variables.xml file	This XML file includes the OVAL external variables. Note, that this file is optional if no OVAL external variable is required for the **mtxoval.exe** execution.
oval_results.xml file	This XML file includes the final OVAL results which are then consumed by the SCAP engine. This result file content depends on **oval_directives.xml** , **oval_definitions.xml** and **oval_variables.xml** files.

Tools

The BMC Client Management SCAP implementation includes different components, either dynamic libraries or command line tools. Most of them are located in **<agent_dir>/bin** .

libMtxScap.dll (libMtxScap.so for Linux and Mac OS X)	This dynamic library actually implements the different SCAP standards except OVAL.
mtxscap.exe (mtxscap for Linux and Mac OS X)	This command line tool is a wrapper for the library above.
mtxoval.exe (mtxoval for Linux and Mac OS X)	This binary (which is a fork of the OVALDI open source software) actually implements the OVAL standard.

mtxscap.exe Options

This command line tool is a wrapper for the libMtxScap library. It makes it possible to parse, display or evaluate SCAP 1.0/1.1/1.2 content. BMC Client Management uses this binary for processing SCAP scans but the binary can also be used by end users through a Windows console or Unix terminal. The tool accepts different command line switches, divided in two parts. The first

group of switches is aimed at enabling/disabling features. These all start with a single ‘~~“ character (ex: -p). The second group of switches expects a parameter directly following the switch keyword. These all start with a double “~~ character (ex: --scap-file scap_gov.nist_USGCB-Windows-7.xml). Below is the list of command line switches:

Command line switch	Purpose	Default
--mtxoval-path	Path to the mtxoval.exe (mtxoval under Linux and Mac OS X systems).	mtxoval.exe (mtxoval under Linux and Mac OS X)
--temp-path	Temporary path where temporary files required by the underlying process will be created.	temp
--oval-directives	The desired OVAL results output. This switch accepts the following values: • full-with-system-characteristics • full-without-system-characteristics • thin	full-with-system-characteristics
--xml-path	Path to the various XML schemas. This parameter may be omitted in which case the input SCAP files will not be validated.	
--scap-file	Path to the SCAP file to process. In case of SCAP 1.0/1.1 content, multiple files can be supplied. In this case, the switch must be repeated for each file to supply (ex: --scap-file file1.xml -scap-file file2.xml)	
--data-stream-id	Identifier of the data stream to process. This parameter is mainly required when processing SCAP content having more than a single data stream. If the SCAP content includes a single data stream, this parameter can be omitted.	
--checklist-id	Identifier of the XCCDF checklist to process. This parameter is mainly required when processing a data stream having more than a single checklist. If the data stream includes a single checklist, this parameter can be omitted.	
--profile-id	Identifier of the XCCDF profile to apply. This parameter is optional regardless of the number of profiles registered in the checklist to process. If this parameter is omitted, then no profile is applied.	
--xccdf-exceptions-file	Path to an optional file where XCCDF rule identifiers are registered. These are exceptions and shall be taken into account in order to alter the scan results. As a consequence, the rules enumerated in this file will always have the status "pass", indicating exceptions to the official results.	
--arf-results-file	Path to the output ARF results file. This parameter will be ignored unless the supplied SCAP content is version 1.2.	
--xccdf-results-file	Path to the output XCCDF results file. This parameter is always available, whatever the processed SCAP version.	
--error-path	Path to the output error file where key error code may be written. This file will only be emitted under certain conditions. For example, when the supplied SCAP content is not applicable to the system.	

Command line switch	Purpose	Default
--log	Path to the desired output log file. This parameter accepts the special value "stdout", in which case, log lines will be written directly to console or terminal.	
-parse	Request a SCAP content parsing operation. Depending on the xml path command line switch, this can be either a validating or non-validating parsing operation.	
-print	Request a SCAP content print operation. This includes parsing the supplied SCAP content and displaying summary.	
-eval	Request a SCAP content evaluation operation. Depending on the various switch values, ARF and /or XCCDF results files can be generated.	
-quiet	Provides a mechanism for reducing the amount of data written to the console or terminal.	
-no-banner	Avoid writing the banner to the console or terminal.	

mtxoval.exe Options MD5Hash

This binary (which is a fork of the OVALDI open source software) actually implements the OVAL standard. This tool can either be used internally by mtxscap or called by end users through a Windows console or Unix terminal. Depending on the target SCAP version, the tool must be applied on an OVAL definitions file or on a SCAP 1.2 data stream collection document. In this case, the component identifier for the underlying OVAL definitions should be supplied. Below, the list of command line switches:

Command line switch	Purpose	Default
-o <path>	Path to the oval-definitions XML file.	definitions.xml
-b <identifier>	Identifier for the OVAL definitions component to retrieve. This parameter is mandatory when processing SCAP 1.2 content and should be omitted otherwise.	
-v <string>	Path to the file where OVAL variables are configured.	external-variables.xml
-f <path>	Path to the file containing a list of OVAL definitions to be evaluated.	
-m	Do not verify the input file with an MD5 hash.	
-c <path>	Path to the Schematron OVAL definitions file. If this parameter is omitted, then no validation will be performed on the input file.	xml\oval-definitions-schematron.xsl
-a <path>	Path to the various XML schemas.	xml
-i <path>	Path to the system characteristics file to be used. If this parameter is omitted, then mtxoval will create a new system characteristics content.	
-d <path>	Path to the output file where system characteristics should be written.	system-characteristics.xml
-g <path>	Path to the OVAL directives to be used.	directives.xml
-r <path>	Path to the output file where OVAL definitions results should be written.	results.xml

Command line switch	Purpose	Default
-s	Do not apply stylesheet to the results file.	
-t <path>	Path to the stylesheet document to apply on results.	xml\results_to_html.xsl
-x <path>	Path to the file where transformed results must be written.	results.html
-j <path>	Path to the Schematron OVAL system characteristics file.	xml\oval- system-characteristics-schematron.xsl
-k <path>	Path to the Schematron OVAL results file.	xml\oval-results-schematron.xsl
-p	Provides verbose output.	
-l <integer>	Activate the desired log level: • DEBUG = 1 • INFO = 2 • MESSAGE = 3 • FATAL = 4	
-p	Provides verbose output.	

SCAP OVAL tests

The following OVAL tests are supported:

- ind-def:environmentvariable_test
- ind-def:environmentvariable58_test
- ind-def:family_test
- ind-def:filehash_test
- ind-def:filehash58_test
- ind-def:filemd5_test
- ind-def:ldap_test
- ind-def:textfilecontent_test
- ind-def:textfilecontent54_test
- ind-def:unknown_test
- ind-def:variable_test
- ind-def:xmlfilecontent_test
- linux-def:dpkginfo_test
- linux-def:iflisteners_test
- linux-def:inetlisteningservers_test
- linux-def:partition_test
- linux-def:rpminfo_test
- linux-def:rpmverify_test

- linux-def:rpmverifyfile_test
- linux-def:rpmverifypackage_test
- linux-def:selinuxsecuritycontext_test
- linux-def:selinuxboolean_test
- unix-def:file_test
- unix-def:inetd_test
- unix-def:interface_test
- unix-def:password_test
- unix-def:process_test
- unix-def:process58_test
- unix-def:runlevel_test
- unix-def:shadow_test
- unix-def:sysctl_test
- unix-def:uname_test
- unix-def:xinetd_test
- win-def:accesstoken_test
- win-def:activedirectory_test
- win-def:auditeventpolicy_test
- win-def:auditeventpolicysubcategories_test
- win-def:cmdlet_test (This test is not supported by lightweight mtxoval_u.exe binary. This component will be used in place of mtxoval.exe when Microsoft .NET 4 Framework is not installed.)
- win-def:dnscache_test
- win-def:file_test
- win-def:fileauditedpermissions_test
- win-def:fileauditedpermissions53_test
- win-def:fileeffectiverights_test
- win-def:fileeffectiverights53_test
- win-def:group_test
- win-def:group_sid_test
- win-def:interface_test
- win-def:lockoutpolicy_test
- win-def:metabase_test
- win-def:passwordpolicy_test
- win-def:port_test
- win-def:printereffectiverights_test
- win-def:process_test
- win-def:process58_test
- win-def:registry_test
- win-def:regkeyauditedpermissions_test
- win-def:regkeyauditedpermissions53_test
- win-def:regkeyeffectiverights_test
- win-def:regkeyeffectiverights53_test

- win-def:serviceeffectiverights_test
- win-def:sharedresource_test
- win-def:sid_sid_test
- win-def:sid_test
- win-def:user_test
- win-def:user_sid_test
- win-def:user_sid55_test
- win-def:volume_test
- win-def:wmi_test
- win-def:wmi57_test
- win-def:wuaupdatesearcher_test

Managing SCAP Jobs

A SCAP job is the actual scan, that is, test and verification, of the target devices against a specified checklist. It can only be assigned to one SCAP package, data stream, benchmark and profile. You can select which benchmark and which profile - if any - will be used during the scan. If, for example, you need to run a SCAP scan for different profiles of the same package you need to create a separate SCAP job for each profile.

Under this node you can create, manage and delete SCAP jobs. SCAP jobs can also be sorted into different SCAP job folders in BMC Client Management , depending on your company's requirements.

The following topics are provided:

- Creating new SCAP jobs
- SCAP Job

Creating new SCAP jobs

SCAP jobs are created via a wizard, that guides you through the steps that require definition.

> **Note:**
>
> Before you can create SCAP jobs you need to have downloaded at least one security checklist within your network that can be imported as an SCAP package.

To create a new SCAP job, proceed as follows:

1. Click **Wizards > Scap Job** or the corresponding icon .
   The **SCAP Compliance Wizard** window opens on the screen.
2. Enter the required information into the text boxes and make the selections in the selection boxes as required.

> See topic SCAP job wizard for more detailed information about the individual options.

3. Click **Finish** in the last window to confirm the new SCAP job.

The new SCAP job is defined and scheduled for execution.

SCAP Job

A SCAP job is the actual test and verification of the target devices according to a specified checklist in combination with a data stream, a benchmark and optionally a profile. It should be assigned to only one SCAP package. You can select which benchmark and which profile will be used during the scan.

A SCAP job in BMC Client Management is created via the **SCAP Compliance Wizard** .

In the view of a SCAP job you can review the settings of the scan in the upper half of the window and make modifications to its parameters as well as its execution schedule, and in the lower half of the window you can see the deviations as well as the targets of the scan via the following tabs:

- Assigned Devices
- Assigned Device Groups
- Deviations

An overview over the SCAP jobs results is available via the following tab:

- Dashboard

The following subnodes provide more detailed information about the results:

- SCAP Results
- SCAP Rules
- SCAP Reports

Modifying SCAP job parameters

To modify one or several parameters of an existing SCAP job, proceed as follows:

> **Note:**
>
> Be aware, that if you modify the package, all result history and data associated with previous executions of this scan are purged.

1. Click the **SCAP Package** link on top of the SCAP job recap panel.
   The **SCAP Job** panel of the **SCAP Compliance Wizard** appears.

2. Make the required changes in the respective boxes.
3. Click **Next >** to continue or click **Finish** to terminate your modifications.
   In the appearing **Assigned Targets** panel of the **SCAP Compliance Wizard** you can change the target population of the SCAP job.
4. Click **Assign** or **Unassign Device or Device Group** / .
5. Click **Next >** to continue with schedule changes or click **Finish** to terminate your modifications.
   The **Schedule** panel of the **SCAP Compliance Wizard** appears.
6. Make the necessary changes to the execution schedule.
7. Click **Finish** to confirm all modifications.
8. To apply the changes you need to reactivate the SCAP job with its new data and population by clicking **Activate SCAP Job** .

> It is then reassigned to all selected targets and run according to the defined schedule.

The SCAP job is then reassigned to all selected targets with its new parameter values and run according to the defined schedule. If you modified the package, all data associated with previous executions of this job are deleted from the database.

Modifying the schedule of a SCAP job

To modify the execution schedule of a SCAP job proceed as follows:

1. Click the **Schedule** link on top of the SCAP job recap panel.
   The **Schedule** panel of the **SCAP Compliance Wizard** appears.
2. Make the necessary changes to the execution schedule.
3. Click **Finish** to confirm the new schedule.
4. To apply the changes you need to reactivate the SCAP job with its new schedule by clicking **Activate SCAP Job** .

> It is then reassigned to all selected targets and run according to the defined schedule.

Devices assigned to a SCAP job

The **Assigned Devices** tab displays a list of all devices that are assigned to the current SCAP job, either directly or via a device group assignment.

To limit the list of displayed devices you can filter them according to their device groups. For this select the desired device group in the **Filter by Device Group** box on top of the table. The list is filtered immediately and now only shows the members of the selected group in the table below.

To limit the list of displayed devices you can filter them according to their device groups. For this select the desired device group in the **Filter by Device Group** box on to of the table. The list is filtered immediately and now only shows the members of the selected group in the table below.

It is not possible to assign or unassign devices from the SCAP job in this view. Changes to the assigned population can only be done via the wizard and the **SCAP Package** link in the panel above.

The table shows the following information about the assigned devices:

Parameter	Description
Device	This column displays the list of names of all devices that the SCAP job is assigned to.
Primary User Name	The fields of this column display the name of the primary user of the respective device.
Inherited from Group	This column displays if the device inherited the assignment through a device group and if yes through which. If the device is directly assigned the field is empty.
Status	The fields of this column display the execution status of the SCAP job on each device.
Last Status Update Time	The fields of this column display the date and time at which the status of the SCAP job was updated for the last time.

Viewing the SCAP job log file

Logging of SCAP job is not included in the general logging in the **mtxagent.log** file, it is written in its own specific log file, the **mtxscap.log** , which is located in the **<Installation Directory>/master/data /ScapInv/jobs/<jobId>** directory. It is possible to directly access the log file of a specific client assigned to the currently selected SCAP job. To do so, proceed as follows:

1. Select the device in the right window pane.
2. Select **Edit > View SCAP Log File** .

A new window appears, displaying the contents of the log file of the managed client for inspection.

The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as ERR for error or T for trace, etc. as well as the description itself.

Activating a SCAP job

If you made modifications to the SCAP job parameters, such as adding new targets or modifying its schedule, or you defined the SCAP job without activating the schedule you need to manually activate it. This will then assign or reassign it to the targets and apply the modified parameter values and execute according to the defined schedule. You can activate the job for either all target devices or device groups, one of them or several specific devices or groups.

1. To activate for some specific devices or device groups select these in the table. To (re) assign all targets do not select anything.

> You can select several targets by holding the CTRL key while selecting.

2. Click **Edit > Activate SCAP Job** .

The SCAP job is (re)assigned to the selected targets and will run according to its defined schedule.

Assigning additional or removing SCAP job targets

Once a SCAP job was defined and run a few times you can still edit its parameters and add new targets or remove currently assigned targets. Once these modifications done you need to reactivate the job with its new data and population by clicking **Activate SCAP Job** .

To modify the target population proceed as follows:

1. Click **Edit > Edit SCAP Job** .
   The **Assigned Targets** wizard window appears on the screen.
2. Make the necessary alterations to your targets.
3. Click **Finish** to confirm the modifications.

The modifications are now reflected in the **Assigned Devices** and **Assigned Device Groups** tabs. To apply the changes you need to reactivate the SCAP job with its new data and population by clicking **Activate SCAP Job** . It is then reassigned to all selected targets and will run according to the defined schedule.

Device groups assigned to a SCAP job

The **Assigned Device Groups** tab displays a list of all device groups that are assigned to the current SCAP job.

It is not possible to assign or unassign device groups from the SCAP job in this view. Changes to the assigned population can only be done via the wizard and the **SCAP Package** link in the panel above.

The table shows the following information about the assigned device groups:

Parameter	Description
Group	This column displays the list of names of all device groups that the SCAP job is assigned to.
Status	The fields of this column display the overall execution status of the SCAP job on the group. This means it is the status of the member device on which the assignment or execution is least advanced.

SCAP job deviations

The **Deviations** tab displays the list of rules that are contained in the benchmark but declared as deviations. A rule deviation is a rule for which it does not matter, if it succeeds or fails on the targets, as its scan results are not included in the global compliance.

The table shows the following information about the deviations:

Parameter	Description
SCAP Rule ID	This column displays the list of rule IDs that were selected as deviations for this SCAP job.
Rule Name	This column displays the list of rule names that were selected as deviations for this SCAP job.
Comments	This field displays any comments concerning the rule deviation, that explains for example why it is considered a deviation or any other pertinent information.
Expiration Date	This column displays the date and time at which the deviation expires. From this time onwards the result of the rule is no longer ignored but included as part of the global compliance.

Adding SCAP rule deviations

A rule deviation is a rule for which it does not matter, if it succeeds or fails on the targets, as its scan results are not included in the global compliance.

Some rules that are included in the benchmarks can be specified as deviations, because, for example, they are not applicable to a specific operating systems, or a specific rule currently is not applicable for your internal regulations, and so on.

These deviations can be modified at any moment and can also have a deadline. This means that for example a rule is considered a deviation until December 31st, because until then a specific requirement is not applied in your organization, but from the 1st of January onwards it will be. Once the expiration date is reached, the deviation is automatically removed and the rule result included in the global compliance.

> **Note:**
>
> Be aware that:
>
> if you add or remove deviations, you need to rerun the scan on the target group for these deviations to be taken into account.
> this does not impact any scans and reports already run before the expiration date, these remain as they are.

To specify a rule deviation proceed as follows:

1. Click **Edit > Add SCAP Rule Deviation** .
   The **SCAP Rule Deviation** dialog box appears.
2. Select the rule to specify as deviation.

> You can select more than one rule at a time by holding the CTRL key while selecting.

3. *(Optional)* Click the calendar icon, if the rule deviation is to expire at a specific date. If the deviation is unlimited, do not modify this box.

   To clear the expiration date click .

4. Click **OK** to add it to the list of deviations and close the window.

The deviation is immediately added to the list. Rerun the scan on the device to create an up-tp-date result.

The SCAP job Dashboard

On the **Dashboard**, four charts are displayed which provide information about the SCAP job results and all its members and their respective compliance:

- Current State of Devices
- Device Trend
- Top 10 Failed Rules
- Top 10 Failed Devices

Balloon tips are available for each chart displaying explanations.

Current State of Devices

This graph displays the current general compliance state of all scanned devices in percentage values. If you move your cursor over the individual pie slices a tooltip displays the absolute numbers for the different device states.

- `Compliant` : the percentage of devices that are completely compliant with all requirements of the SCAP package.
- `Not compliant` : the percentage of devices that are not compliant for at least one of the conditions of th SCAP package.
- `Not Scanned` : the percentage of devices on which the compliance evaluation was not run. This might be due to the device being switched off or not reachable via the network.
- `Not Applicable` : the percentage of devices for which the package is not applicable, for example, the package contains Windows 7 rules and the target has a Windows Vista operating system.

Device Trend

This graph displays the compliance trend of the SCAP job targets, that is, it shows, how the compliance situation of a specific population advances within a specific timeframe, by default this is the last 10 results.

Note:

By default one result per day is generated, this this trend is shown per day. You can modify this value in the **Vision64Database.ini** file in the **[SCAPCompliance]** section.

- `Compliant` : the number of devices that are completely compliant with all requirements of the SCAP package.
- `Not compliant` : the number of devices that are not compliant for at least one of the conditions of the SCAP package.
- `Not Scanned` : the percentage of devices on which the compliance evaluation was not run.
- `Not Applicable` : the percentage of devices for which the package is not applicable, for example, the package contains Windows 7 rules and the target has a Windows Vista operating system.

Top 10 Failed Rules

This graph displays the 10 rules that have the highest rate of non-compliance on all target devices.

The bar chart shows the names of the rules and the number of devices on which it failed.

Top 10 Failed Devices

This graph lists the 10 devices with the highest number of failed compliance rules.

The bar chart shows the names of the devices and the number of rules which failed on each.

SCAP job exceptions

The **Exceptions** tab displays the list of rules that are contained in the benchmark but declared as exceptions. A rule exception is a rule for which it does not matter if it succeeds or fails on the targets, as its scan results are not included in the global compliance.

The table shows the following information about the exceptions:

Parameter	Description
Rule Name	This column displays the list of rule names that were selected as exceptions for this SCAP job.
Comments	This field displays any comments concerning the rule exception, that explains for example why it is considered an exception or any other pertinent information.
Expiration Date	This column displays the date and time at which the exception expires. From this time onwards the result of the rule is no longer ignored but included as part of the global compliance.

Adding SCAP rule exceptions

A rule exception is a rule for which it does not matter if it succeeds or fails on the targets, as its scan results are not included in the global compliance.

Some rules that are included in the benchmarks can be specified as exceptions, because, for example, they are not applicable to a specific operating systems, or a specific rule currently is not applicable for your internal regulations, and so on.

These exceptions can be modified at any moment and can also have a deadline. This means that for example a rule is considered an exception until December 31st, because until then a specific requirement is not applied in your organization, but from the 1st of January onwards it will be. Once the expiration date is reached, the exception is automatically removed and the rule result included in the global compliance.

> **Note**
>
> Be aware that this does not impact any scans and reports already run before the expiration date, these will remain as they are.

To specify a rule exception proceed as follows:

1. Click **Edit > Add SCAP Rule Exception**.
   The **Select an SCAP Rule** dialog box appears on the screen.
2. Select the rule to specify as exception.
   You can select more than one rule at a time by holding the CTRL key while selecting.
3. *optional:* Click the calendar icon if the rule exception is to expire at a specific date. If the exception is unlimited do not modify this box.
4. Click **OK** to add it to the list of exceptions and close the window.

The results of a SCAP job

This view provides detailed information about the results of a SCAP job via its two tabs:

- **Current Results**
- **Device Trend**

In addition **xccdf-result.xml** and **arf-result.xml** (version 1.2 and later only) files are generated and provided for download.

Downloading the xml result files

Both the **xccdf-result.xml** and **arf-result.xml** (version 1.2 and later only) files are generated and provided for download, to do so proceed as follows:

1. Select the device for which to download the result file(s) in the right window pane.
2. Click **Edit > Download XCCDF xml** or **Edit > Download ARF xml** .
   The **Assigned Targets** window appears on the screen.
3. Select the directory in which to safe the file.
4. Click **OK** .

The file is saved in the specified location and ready for further usage.

Viewing the rule details report of a SCAP job result

The rule details report of a SCAP job result displays the contents of the result xml file; that is, the results of the SCAP scan in user-friendly format in the form of an HTML page.

To display the result report in HTML format proceed as follows:

1. Select the device under the SCAP job result for which to display the report in the right window pane.
2. Click **Edit > View Rule Details** .

A browser opens a new tab on the screen and displays the rule details results report for the selected device.

> **Note:**
>
> If you are using Google Chrome as your default browser, saving this report will replace all relative links with absolute links, and the navigation within the report is broken.
> If you are using Microsoft Internet Explorer you should use the option save as **Webpage, HTML only** , otherwise all relative links will be replaced with absolute links, and the navigation within the report is broken.

Viewing the test details report of a SCAP job result

The test details report of a SCAP job result provides detailed information concerning the OVAL tests, including the expected and actual values. The tests are themselves are organized in order to build the OVAL definitions with logical operators. These definitions are also explained in the report.

To display the result report in HTML format proceed as follows:

1. Select the device under the SCAP job result for which to display the report in the right window pane.
2. Click **Edit > View Test Details** .

A browser opens a new tab on the screen and displays the test details results report for the selected device.

> **Note:**
>
> If you are using Google Chrome as your default browser, saving this report will replace all relative links with absolute links, and the navigation within the report is broken.
> If you are using Microsoft Internet Explorer you should use the option save as **Webpage, HTML only** , otherwise all relative links will be replaced with absolute links, and the navigation within the report is broken.

The Current Results tab of a SCAP job

This view lists all devices on which the SCAP job was executed with their respective compliance results:

Parameter	Description
Device	This column displays the list of names of all devices that were scanned by this SCAP job.
Operating System	The fields of this column display the operating system of the respective device.
Scan Date	This column displays the date and time at which the scan was run on the device.
% Compliant	This column displays percentage of compliance for the device.
Failed Rules	This column displays the number of rules that failed on the device.
Passed Rules	This column displays the number of rules that had a successful result on the device.
Others	This column displays the number of tests run on the device with any status other than `Pass` and `Failed` .
Compliance Status	This column displays if the device is compliant with the rules of the SCAP job. Possible values are `Compliant` , `Not compliant` , `Not Scanned` if the compliance evaluation was not run, possibly due to the device being switched off or not reachable via the network, or `Not Applicable` if the package is not applicable to the device, for example, the package contains Windows 7 rules and the target has a Windows Vista operating system.

The Device Trend tab of a SCAP job

This view shows the evolution of the device compliance of a specific SCAP job with more detail than the chart on the dashboard. It adds one line per day showing the SCAP scan results with the following information:

Parameter	Description
Last Evaluation	This column displays the date and time at which the SCAP job results were last evaluated.
Number of devices	The fields of this column display the total number of devices on which the job was run.
Compliance	This column displays the total number of devices that are compliant.
Not Compliant	This column displays the total number of devices that are not compliant.
Not Scanned	This column displays the total number of devices that could not be scanned. This might be due to the device being switched off or not reachable via the network.
Not Applicable	This column displays the total number of devices for which the SCAP job rules were not applicable. For example, the package contains Windows 7 rules and the target has a Windows Vista operating system.

Purging the SCAP job history

Once you are done with a specific part of the SCAP job and the existing history is no longer needed you can delete it. Only the results of the last scan will be kept in the database. To purge the history proceed as follows:

1. Click **Edit > Purge History** ⊘ .
   A confirmation window appears.
2. Click **Yes** to confirm and delete SCAP job history.

SCAP job results for an individual device

This view provides detailed information about the SCAP job results of a specific device. It shows all rules included in the SCAP job and the result for each of them in the **Rules** tab. It also allows you to define exceptions for this specific device. In the **Exceptions** tab you can see all exceptions defined for this device.

Rules of a SCAP job results for an individual device

Exceptions of a SCAP job results for an individual device

Adding SCAP rule exceptions

Removing SCAP rule exceptions

Rules of a SCAP job results for an individual device

This view provides detailed information about the rules of a SCAP job run on a specific device. It shows all rules included in the SCAP job and the result for each of them. Double-clicking a rule opens the **Properties** window, displaying details about the selected rule.

Parameter	Description
Rule Name	This column displays the list of names of all rules that were verified by this SCAP job.
SCAP Rule ID	This column displays the unique identifier of all rules that were verified by this SCAP job.
Description	The fields of this column display a more detailed description of the contents of each rule.
Status	This field displays the compliance result for this rule on this device.

SCAP job result status values

Following are the possible status values for a SCAP job result:

Status	Description
Pass	The target system or system component satisfied all the conditions of the rule.
Failed	The target system or system component did not satisfy all the conditions of the rule.
Error	The evaluation could not be completed, therefore the status of the target's compliance with the rule is not certain. This could happen, for example, if the SCAP job was run with insufficient privileges, and could not gather all of the necessary information.
Unknown	The SCAP job encountered some problem and the result is unknown. This could happen, if, for example, the SCAP job was unable to interpret the output (the output has no meaning to the SCAP job).
Not Applicable	The rule was not applicable to the target device of the scan. For example the rule might were specific to a different version of the target OS, or it might were scanned against a platform feature that was not installed.
Not Checked	

Status	Description
	The rule was not evaluated by the SCAP job. This status is designed for rule elements that have no check elements or that correspond to an unsupported checking system. It can also correspond to a status that is returned, if the checking engine does not support the indicated check code.
Not Selected	The rule was not selected in the benchmark, that is it was not included in the profile that was selected for this SCAP job.
Informational	The rule was checked, but the output from the SCAP job is simply information for auditors or administrators, it is not a compliance category. This status value is designed for rule elements whose main purpose is to extract information from the target rather than test the target against a rule.
Fixed	The rule had failed during the last SCAP job execution, but has since been fixed.

Adding SCAP rule exceptions

Rule exception are similar to deviations, but on a device level, not for a group. An exception is a rule, for which it does not matter, if it succeeds or fails on the target, that is, it's real result does not impact the device compliance. This means, that its scan results are included in the device compliance, the rule appears in the list of executed rules, but its result is always displayed as successful.

Some rules that are included in the benchmarks can be specified as exceptions, because, for example, they are not applicable to a specific operating systems, or a specific rule currently is not applicable for your internal regulations, and so on.

These exceptions can be modified at any moment and can also have a deadline. This means that for example a rule is considered an exception until December 31st, because until then a specific requirement is not applied in your organization, but from the 1st of January onwards it will be. Once the expiration date is reached, the exception is automatically removed and the rule result included in the global compliance.

> **Note:**
>
> Be aware that:
>
> if you add or remove exceptions, you need to rerun the scan on the device for these exceptions to be taken into account.
> this does not impact any scans and reports already run before the expiration date, these remain as they are.

To specify a rule exception proceed as follows:

1. Click **Edit > Add SCAP Rule Exception** .
   The **Select an SCAP Rule** dialog box appears.
2. Select the rule to specify as exception.

> You can select more than one rule at a time by holding the CTRL key while selecting.

3. *(Optional)* Click the calendar icon, if the rule exception is to expire at a specific date. If the exception is unlimited, do not modify this box.

> To clear the expiration date click .

4. Click **OK** to add it to the list of exceptions and close the window.

The exception is immediately added to the list. Rerun the scan on the device to create an up-to-date result.

Exceptions of a SCAP job results for an individual device

This view provides detailed information about the SCAP exceptions for a specific device. It shows all rules that are defined as exceptions in the SCAP job and some details about them. Double-clicking a rule opens the **Properties** window, displaying details about the selected rule exception.

Parameter	Description
Rule Name	This column displays the list of names of all rules that were verified by this SCAP job.
SCAP Rule ID	This column displays the unique identifier of all rules that were verified by this SCAP job.
Description	The fields of this column display a more detailed description of the contents of each rule.
Status	This field displays the compliance result for this rule on this device.

Removing SCAP rule exceptions

Removing a rule exception signifies that, for a specific reason, an up to now unimportant rule now has become significant and its compliance outcome must be included in the result.

> **Note:**
>
> Be aware, that if you remove exceptions you need to rerun the scan on the device for these exceptions to be taken into account.

To remove a rule exception proceed as follows:

1. Click **Edit > Remove SCAP Rule Exception** .
   A **Confirmation** dialog box appears.
2. Click **Yes** to remove the exception and close the window.

The exception is immediately removed from the list. Rerun the scan on the device to create an up-tp-date result.

SCAP Rules

This view lists all rules that are part of the SCAP job that were verified during the scan.

The view displays the following information about the rules:

Parameter	Description
Rule Name	This column displays the list of names of all rules that were verified by this SCAP job.
SCAP Rule ID	This column displays the unique identifier of all rules that were verified by this SCAP job.
Description	The fields of this column display a more detailed description of the contents of each rule.
Compliant	This column displays if the number of scanned devices found to be compliant with this rule.
Not Compliant	This column displays if the number of scanned devices found to be not compliant with this rule.

Viewing the SCAP rule information

To display more detailed information about a specific rule proceed as follows:

1. Select the rule for which you want more information in the right window pane.
2. Click **Edit > Properties** .
   The **Properties** window appears. It displays all the information available in its different tabs. Depending on the type of rule, that is, if it is CVE or CCE, the content of the window changes. If the rule has several CVEs or CCEs or both, there is one panel per CVE or CCE, each of which can be expanded and collapsed.

   > **Note:**
   >
   > If this window does not show any additional information you have not downloaded the respective CVE or CCE. Refer to Importing CVE and CCE lists to import them.

3. Click **Close** to close the window.

Individual SCAP rules

This view shows the information about all devices on which the selected rule was run. It provides the following information:

Parameter	Description
Device	This column displays the list of names of all devices that were verified for this SCAP rule.
Operating System	This column displays the operating system of the device.
Scan Date	The fields of this column display the date and time at which the scan was run on the device.
Status	This column displays the compliance result for this device. The possible values for this field are `Pass` , `Failed` , `Unknown` , `Error` and `Not Selected` .

SCAP Reports

This view provides the following information about all reports that are assinged to this SCAP job:

Parameter	Description
Name	The fields of this column display the names of the report.
Report Title	This field displays the title of the report.
Activation	This field shows the condition on which the report will be generated.
Schedule	The fields of this column display the frequency with which the report will be generated.
Termination	This field displays on which condition the report will definitely terminate its generation cycle.

This node also allows you to access the assigned reports individually via the left hierarchy tree.

Assigning a report to a SCAP job

To assign a report to a SCAP job proceed as follows:

1. Select the **Compliance Management > SCAP Compliance > SCAP Jobs > Your SCAP Job > SCAP Reports** in the left window pane.
2. Click **Edit > Assign Report** .
   The **Assign a Report** dialog box appears on the screen.
3. Select the report to assign from the list in the dialog box.
4. Click **OK** to confirm the assignment.

The selected report is now assigned to the SCAP job.

Generate Report

It is possible to directly launch the generation of a report. In this case the report is always only generated once and only for the assigned SCAP job. To generate a report proceed as follows:

1. Select the **Compliance Management > SCAP Compliance > SCAP Jobs > Your SCAP Job > SCAP Reports** in the left window pane.
2. Select the report to generate in the table in the right window pane.
3. Click **Edit > Generate Report** .
   A confirmation window appears. This window allows you to select in which format the report is generated. You have the choice between HTML, XML and PDF, you can select only one or two or all of the formats.
4. Check the boxes for the required report formats.
5. Click **OK** to confirm the generation or **Cancel** to abandon.

The report is created directly and made available under the report's subnode.

Individual SCAP report

This view provides information about the generated versions of the SCAP report:

Parameter	Description
Name	Displays the name of the generated report. It consists of the local generation date and time of the computer on which the report was generated.
XML Status	Displays the status of the XML version of the respective report, if an xml version was generated.
HTML Status	Displays the status of the HTML version of the respective report if an html version was generated.
PDF Status	Displays the status of the PDF version of the respective report if a pdf version was generated.
Public Report	Defines if the respective report is to be generally accessible via the **Report Portal** . By default this option is set to **No** .

Viewing a generated SCAP report

To display the generated result for a SCAP job report, proceed as follows:

1. Select the **Compliance Management > SCAP Compliance > SCAP Jobs > Your SCAP Job > SCAP Reports > Your SCAP Job Report** in the left window pane.

   > In the right window pane you can now see in which format the report was generated and is available.

2. Click **Edit > View** .
3. *(Optional)* If the report is available in more than one format the **Select Display Format** dialog box appears. Select the format in which to display the report from the **Available Formats** box.
4. Click **OK** .

CM opens the progam matching the selected report format, that is either a pdf reader or the default browser, and displays the report.

Assigning compliance rules to device groups -- O

To assign a compliance rule to a device group proceed as follows:

1. Select the **Compliance Rule** node in the left window pane.
2. Select the **Edit > Assign Device Group** icon.
   The **Assign a Compliance Rule** pop-up menu appears.
3. Select the device group from the window.
4. Click **OK** to confirm the assignment.
   The **Desired Compliance** window appears.

> **Note:**

Here you must select the type of the population for the group.

5. Select the respective radio button to have a group collecting all compliant, not compliant or all devices for which the evaluation was impossible.
6. Click **OK** to confirm and close the window.
   The device group will be added to the table of assigned device groups.

Under the main **Device Groups** node the icon of the group will change to its compliance rule populated one and the members of the group will now be managed by the results of the rule.

Deploying Operating Systems

The operating system deployment (OSD) functionality of BMC Client Management uses the Pre-boot eXecution Environment (PXE) industry standard for its operation. This standard allows to install an operating system on a device without the need for an operating system to be present on the local disk of the target device.

This allows IT departments to deploy operating systems with the possibility to remotely (re-)install individual devices, groups of devices and even complete subnets of the infrastructure; the target devices either already have an operating system installed or they are "virgin" devices.

This topic includes:

License considerations

OS Deployment is a limited module and requires a specific license.

System restrictions

The OSD system relies on Windows dependent tools for the creation of OSD projects, therefore the OSD Manager functionality is only available for Windows devices. However, the other two OSD roles, *Image Repository* and *Network Boot Listener* , are independent from Windows. This allows any relay in your infrastructure to execute either or both of these roles if they have a Linux or Mac OS X operating system.

OSD Modes

The operating system deployment functionality allows for a number of different possibilities to execute these deployments:

Mode	Description
Setup Mode	Using the setup mode allows you to execute a regular installation of the operating system on the remote devices or targets via the operating system's setup executable file. The use of an unattended file makes the installation silent and automatic.
WIM Image Capture	The WIM capture mode allows you to create your own WIM images to be deployed via the WIM mode within your network. You may also use this mode create images of other, non-booting disks, such as drives that contain only applications or data and deploy these via the WIM mode to other devices within your infrastructure. The WIM mode also supports the new Sysprep Microsoft technology and thus provides the categories of WIM images.
Standard WIM Image	This mode is used to create a standard WIM image without the Sysprep tool.
Windows XP/Server 2003 Sysprep WIM Image	This mode is used to create a WIM image for Windows XP and 2003 Server using the Sysprep tool. Sysprep is a Windows system presentation tool that facilitates image creation and preparation of an image for deployment to multiple computers. After the initial image is created it runs a wizard after the device restart, prepares the device for cloning and copies an image to the computer.
Windows Vista / 7 / 8 / 10 Sysprep WIM Image	This mode is used to create a WIM image for Windows Vista and 2008 Server using the Sysprep tool.
WIM Image Mode	The WIM mode allows you to deploy the new operating systems or images of other non-booting disks to the targets via a WIM image, that is either delivered on the operating system disk or via a custom created WIM image. This mode can only be used if the target hardware is compatible to the hardware of the source device. All explained categories of WIM images can be used by this mode.
Custom Mode	This mode allows you to use other applications with which snapshots of existing installations can be created and then be "duplicated" on other devices, such as for example ghost images.

Related topics

- Prerequisites for OSD
- Performing advanced OSD tasks
- Managing OSD Managers
- Managing Image Repository
- Configuring Network Boot Listener
- Managing OSD Drivers
- Managing OSD Images
- Managing OSD Disk Configurations
- Managing OSD target lists
- Managing targets
- Managing OSD Projects
- Managing OSD multicast sessions
- Creating an OSD PXE Menu
- Managing OS Deployment via the wizards

Prerequisites for OSD

To be able to execute the examples described for operating system deployment, a number of general Client Management and OS deployment prerequisites must be fulfilled, which are listed in the following two paragraphs. The examples then guide you step by step through the different possible procedures installing a new operating system on a remote device or creating a new image to be deployed. The procedures, however, only refer to parameters that need to be filled in or must be modified, any parameters of which the prepopulated default values are used are not mentioned here. You can find detailed information about these parameters in the knowledge center of this functionality.

If you are upgrading from 12.0 or earlier version, see What's new for OSD in version 12.1

Before actually deploying a new operating system to new devices in your network, you must ensure that the components and devices listed here are available and configured.

> **Note:**
>
> Be aware that operating systems cannot be deployed to devices with IPv6 addresses.

The following prerequisites are noted for OSD:

- OSD Manager
- Network boot listener
- Sysprep deployment
- Storage device
- Target devices
- Ghost images

OSD Manager

The OSD Manager is a device of the CM infrastructure, it must have a Windows operating system. By default, it is the master, as it is for our examples.

If your master is a Linux device, you must first select another device as the OSD Manager.

The following prerequisites apply to this device:

- The OSD Manager must have a CM agent installed and have the OSD module loaded.
- The operating system must be one of the following:
  - Windows 7 Service Pack 1
  - Windows Server 2008 R2 SP1
  - Windows Vista SP1
  - Windows Server 2008 family

  - Windows 7 family
  - Windows Server 2008 R2 family
  - Windows 8 family
  - Windows 8.1 family
  - Windows 2012 family
  - Windows 2012 R2 64 bit
  - Windows 10 family
  - Windows 2016 family
- The Windows ADK (Windows Assessment and Deployment Kit) must be installed on the OSD Manager/TFTP server device.
  If you want to manually install it, you can download it from the Microsoft site at https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit . On the Microsoft website you can find official installation instructions for the setup.
  The **Configuration** node allows you to automatically download and install the new Windows ADK.

Image repository

At least one image repository must be defined, it can be the same device as the master. It is recommended to have one image repository per physical location. The operating system of the image repository can be any of the supported systems.

Network boot listener

At least one network boot listener must be defined, it can be the same device as the image repository.It is recommended to have one network boot listener per subnet. The operating system of the network boot listener can be any of the supported systems.

Sysprep deployment

The Sysprep deployment has a number of limitations as follows:

- a uniprocessor/core image can only be deployed on other uniprocessor/core devices.
- a multiprocessor/core image can only be deployed on other multiprocessor/core devices.
- the operating system language is fixed by the initial capture.
- no static IP address can be used.
- the administrator logon/password of the captured system must be the same as the one specified in the deployment parameters in the unattended information tab. If this is not the case an invalid login or password Windows error is generated.

Storage device

At least one device with network shares on which the OS setup, image and ghost are to be deployed can be stored. For this you can use the OSD Manager or the DHCP server, however, BMC recommends that you use a dedicated device. In our examples we deploy the 32-bit version of Windows Vista, therefore these setup and image files must be copied to a share called /Vista32, a ghost image is to be copied to a directory called /Ghosts32. This directory must contain the ghost

executable file and the ghost image. Be aware, that Windows XP has a limit for concurrent SMB connections per share so a linux server with a samba share or a Windows Server Edition is advised.

Target devices

The target devices must have PXE boot set as the first boot device in the BIOS.

Ghost images

If you want to use ghost images the following prerequisites apply:

- the `ghost32.exe` (executable found in the install folder of the win32 install) and the `GHOSTCDR.DLL` library must be located in the folder where the `.iso` image is stored.
- the account specified in the image configuration *must* be the same specified in the OSD manager configuration (Windows limitation).

This example restores a device that was installed via a ghost.

Path: `\\hotline\OS Setup\personnalise\GhostOsdSupport261009\ghost.GHO`

Command line: `ghost32.exe -clone,mode=restore,src=ghost.GHO,dst=1:0 -SURE`

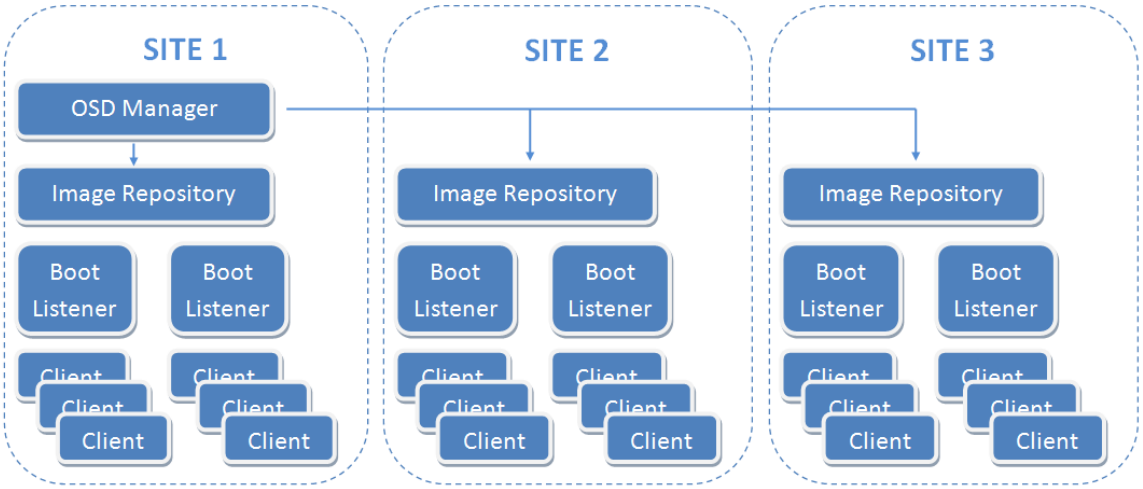
The path mounts a network share (`W:`) which is used to find `ghost32.exe` and `ghost.gho` (do not use UNC paths, these don't work). The dst option indicates which disk/partition to restore the image on.

The following topics provide more information about prerequisites for OSD:

- OSD architecture and components
- Windows Sysprep distributions
- The phases of OSD
- Considerations when upgrading OSD to version 12.1 and later

OSD architecture and components

The new OSD architecture is based on one single OSD Manager and image repositories at each physical site with one network boot listener per subnet. The image below shows an example for such an architecture:



Operating system deployment in the BMC Client Management - Software Distribution requires a number of different components and objects working together:

- OSD agent
- OSD manager
- Image repository
- Network boot listener
- Storage device
- Projects
- OSD wizard

OSD agent

An OSD agent is any type of CM agent on which the OSD module is loaded. This means it can either be the *OSD Manager*, if it is a Windows device, or an *Image Repository* or a *Network Boot Listener* or both, for any type of operating system.

OSD manager

The OSD Manager is a device within a subnet that is responsible for the creation of the deployment projects and their publication. It is recommended to only have one OSD Manager, but multiple OSD Managers are possible. The OSD Manager is by default also *Image Repository* and *Network Boot Listener* . The *Image Repository* role is mandatory as it is the parent of all the subsequent image repositories. The network boot listener for the subnet is optional and can be deactivated.

> **Note:**
>
> For legacy installations, if you have more than one OSD Manager, these can still exist in parallel, but it is recommended to consolidate them into one single OSD Manager and replace the other OSD Managers with image repositories.

Image repository

Image repositories are the bridge between the OSD Manager and the targets. They are assigned OSD objects (projects, images and so on), that is, the repositories store the objects in their cache and thus require large amounts of disk space to store the data. Each repository should have several *Network Boot Listeners* , one per subnet. It is recommended to use relays as the image repositories. The parent of an image repository should be either the OSD Manager, or another repository in more complex environments. An image repository can be deactivated if there is no child to the node, it then becomes a network boot listener.

Network boot listener

Formerly called *OSD Proxy* . It cannot have children. The network boot listener for the subnet is optional and can be deactivated. If the image repository role is activated as well, it becomes an image repository and can have children. The network boot listener executes the actual deployment: it informs the targets and provides the link to the source data for the installation.

Storage device

This is a device with network shares on which the OS setup files, WIM images and custom images to be deployed can be stored. Be aware, that Windows XP has a limit for concurrent SMB connections per share so a Linux server with a samba share or a Windows Server Edition is advised. The storage device can be an independent device or it can be located on the DHCP or TFTP server.

Projects

The project is the central point which collects all the different elements that are required for an operating system deployment. Via these elements, it receives all the information which is then compiled during the project build process. After this process has terminated with success, the project becomes active and published, that is, all required information is made available to the target devices for installation.

OSD wizard

BMC Client Management - Software Distribution also provides a wizard which guides you through the different steps of creating the individual OSD components or even a complete OSD project for all different types of distribution.

Windows Sysprep distributions

The BMC Client Management - Software Distribution allows you to use Windows Sysprep distributions. The System Preparation (Sysprep) tool prepares an installation of Windows for duplication, auditing, and customer delivery.

Duplication, also called imaging, enables you to capture a customized Windows image that you can reuse throughout an organization. Audit mode enables you to add further device drivers or applications to a Windows installation. After you install the additional drivers and applications, you can test the integrity of the Windows installation. Sysprep also enables you to prepare an image to be delivered to a customer. When the customer boots Windows, Windows Welcome starts.

Sysprep must be used only to configure new installations of Windows. You can run Sysprep as many times as required to build and to configure your installation of Windows. However, you can reset Windows activation only up to three times. You must not use Sysprep to reconfigure an existing installation of Windows that has already been deployed. Use Sysprep only to configure new installations of Windows.

If you intend to transfer a Windows image to a different computer, you must run `sysprep /generalize` , even if the computer has the same hardware configuration. The `sysprep /generalize` command removes unique information from your Windows installation, which enables you to reuse that image on different computers. The next time you boot the Windows image, the specialized configuration pass runs. During this configuration pass, many components have actions that must be processed when you boot a Windows image on a new computer. Any method of moving a Windows image to a new computer, either through imaging, hard disk duplication, or other method, must be prepared with the `sysprep /generalize` command. Moving or copying a Windows image to a different computer without running `sysprep /generalize` is not supported.

Benefits of Sysprep

Sysprep provides the following benefits:

- Removes system-specific data from Windows. Sysprep can remove all system-specific information from an installed Windows image, including the computer security identifier (SID). The Windows installation can then be captured and installed throughout an organization.
- Configures Windows to boot to Audit mode. Audit mode enables you to install third-party applications and device drivers, as well as to test the functionality of the computer.
- Configures Windows to boot to Windows Welcome. Configures a Windows installation to boot to Windows Welcome the next time the computer starts. In general, you configure a system to boot to Windows Welcome immediately before delivering the computer to a customer.
- Resets Windows Product Activation. Sysprep can reset Windows Product Activation up to three times.

Limitations of Sysprep

Sysprep has the following limitations:

- You must use only the version of Sysprep that is installed with the Windows image that you intend to configure. Sysprep is installed with every version of Windows and must always be run from the `%WINDIR%/system32/sysprep` directory. (Windows 7 and later)
- Sysprep must not be used on upgrade installation types. Run Sysprep only on clean installations.

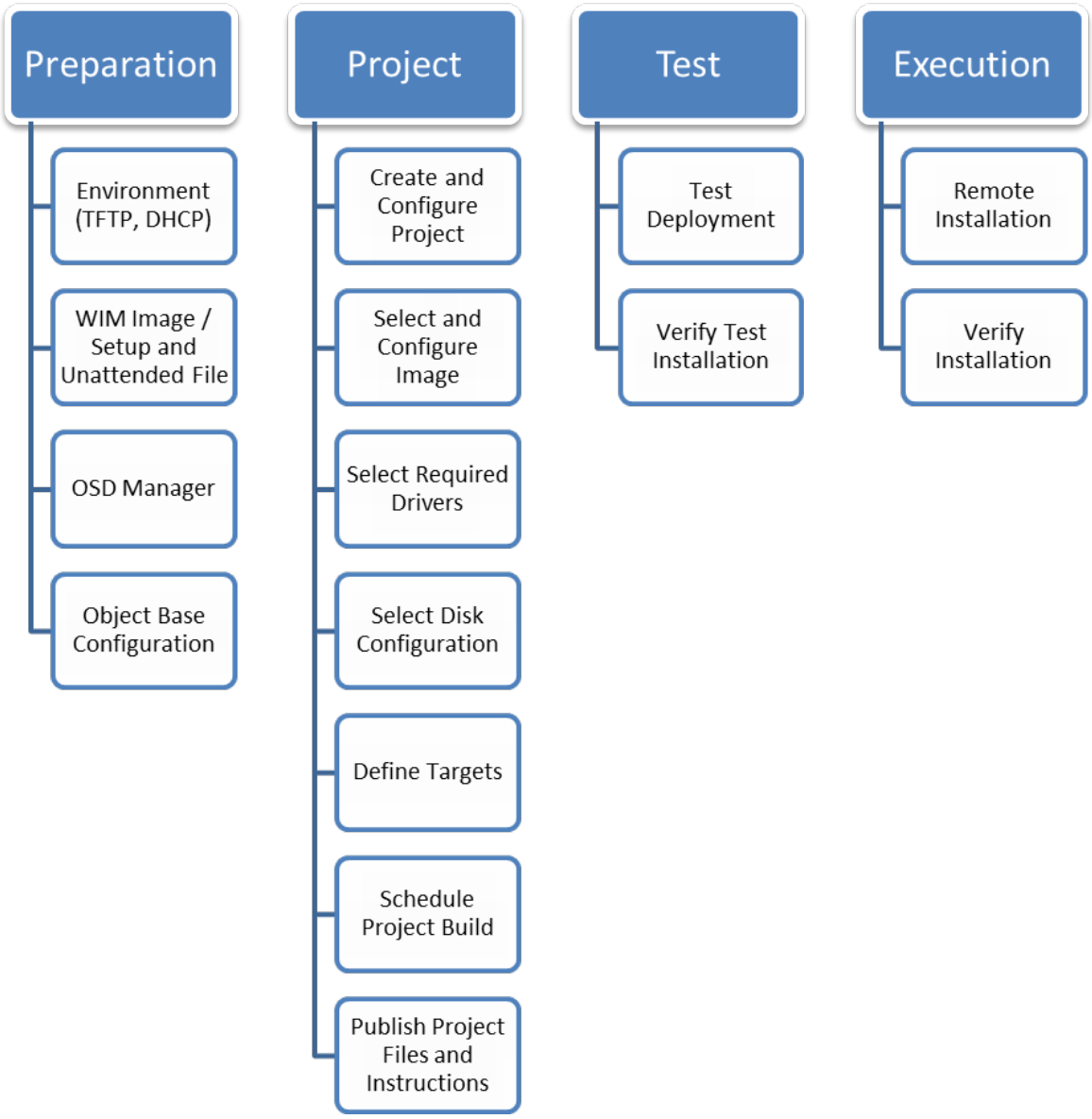
- If you plan to use the `imagex /apply` command to apply a Windows image to a computer, the partition layout on the reference and destination computers must be identical. For example, if you capture a customized Windows image on drive D, you must always deploy that image onto drive D of the destination computer. The following list describes the partition settings that must be identical across the reference and destination computers when you use the `imagex /apply` command.
    - The partition number where Windows 7 is installed must match the original computer layout.
    - The partition type (primary, extended, or logical) must match the original computer layout.
    - If the partition is set to active on the reference computer, the destination computer must also be set to active.

      In some cases, customized applications that are installed before the Windows image is recaptured might require a consistent drive letter. Some applications store paths that include the drive letter of the system. Uninstallation, servicing, and repair scenarios might not function appropriately if the drive letter of the system does not match the drive letter specified in the application. Deploying customized Windows images to different drive letters is not supported.

      The recommended practice is, if you are installing customized applications, to deploy your Windows image to the same drive letter.
- The Plug and Play devices on the reference and destination computers, such as modems, sound cards, network adapters, and video cards, do not necessarily have to be from the same manufacturer. However, the drivers for these devices must be included in the installation.
- If you run Sysprep on an NTFS file system partition that contains encrypted files or folders, the data in those folders becomes completely unreadable and unrecoverable.

The phases of OSD

BMC Client Management - Software Distribution allows the administrator to remotely install or deploy operating systems on new devices or reinstall broken devices within the network. The operating system deployment can be divided into the three major phases, with several steps each.



The following paragraphs provide more information about the phases of OSD:

- The preparation phase
- The project phase
- The execution phase

The preparation phase

The preparation phase is the preparing of the environment needed by the OSD Manager as well the preparation of the files required for the actual deployment. It also comprises the configuration and creation of the components required by OSD, such as the drivers, disk configuration, and so on.

1. Prepare the environment - TFTP server, DHCP server, storage location, OSD Manager.
2. Create the WIM image *or* prepare the setup files and the unattended file.

3. Prepare the base configurations for the necessary drivers, images, disk and partition configurations, and maybe the target lists.

The project phase

This second phase creates the actual deployment project, that is, the components for a specific deployment project are selected and the project is built. After this is successfully terminated, the files and instructions required for the remote installation are published, that is, they are made available to the target devices.

1. Create and configure project
2. Select image
3. Select required drivers
4. Select disk configuration
5. Define targets
6. Schedule project build
7. Build project
8. Publish project files and instructions

The execution phase

This third phase can be added to verify the situation on the network after the remote installation has taken place and ensure that all the target devices are properly installed, up and running.

1. Remote installation on target device
2. Verify installation

Considerations when upgrading OSD to version 12.1 and later

BMC recommends following considerations before upgrading OSD to version 12.1 and later:

- Upgrade process
- Consolidating to one OSD Manager
- Driver by model upgrade side-effects
- Delta versus project transfer
- Related topics

Upgrade process

> **Note:**
>
> The Windows ADK must be installed on all OSD Managers for a successful upgrade to version 12.1 and later, either before or after the upgrade procedure.

As usual there are two possible upgrade mechanisms:

- **Automatic agent upgrade:**
  If this option is activated, all your OSD agents are also automatically upgraded to version 12.1 and later. All your projects are still functional, you only need to rebuild them to make them available for deployment again.
- **Manual agent upgrade:**
  If the automatic option is not activated, and you are rolling out the upgrade manually to your agents, all your OSD agents are still on version 12.0 after your master upgrade, and they are no longer functional. All your current projects are still fully functional and might even run, if so defined. However, it is impossible to make changes to them, or to view any of their data, including the progress of any running installations. If a deployment was in progress when the upgrade started, it failed. This is shown in the status of the device, once the respective OSD agent is upgrade, and in the deployment log.
  BMC strongly recommends to take all your projects offline before starting the upgrade process of the master and subsequently the agents.

> **Note:**
>
> As usual, the OSD upgrade mechanism removes all generated files for a clean start. All OSD objects are kept in the database, but all projects require a rebuild.

Consolidating to one OSD Manager

With version 12.1 a number of architectural changes were introduced to the operating system deployment:

- In version 12.0 and earlier many OSD Managers could be defined. Version 12.1 and later favors an architecture with only one OSD Manager and any number of image repositories.
- The OSD proxies that were used alongside the OSD Managers disappear and are automatically converted into *Network Boot Listeners* that are taking over the proxy's role.

For more information on the new architecture see OSD architecture and components .

Client Management versions prior to 12.1 used an architecture with more than one OSD Manager. When upgrading to version 12.1 or later, you can still keep all your OSD Managers, but you might want to analyze the advantages of the new architecture before deciding to stay with your existing architecture or move to the new one. Following are two examples, one where a move appears advantageous, and a second, where it is probably preferable to stay with the existing architecture:

> **Note:**
>
> All OSD Managers are automatically assigned the roles of *Image Repository* and *Network Boot Listener* during the upgrade.

1. An implementation uses the same projects and images throughout the entire infrastructure. This situation might arise when a company has a limited set of OS images for a limited set of hardware.
   There are 50 OSD Managers spread all over the globe on the different physical sites, and on them are copies of these projects. In this case, it would seem preferable to move to the new architecture and to one OSD Manager. This OSD Manager would then handle all the delta updates, instead of using an external tool to propagate the changes made to the OS images. When deleting all OSD Managers but one, all projects and images located on these other managers are lost. However, this is not a problem, because they are all duplicates of the same data that is still located on the *main* OSD Manager. All previously existing OSD Managers, which were deleted, can then be added as image repositories and can synchronize the same projects.
2. For an environment that has multiple OSD Managers storing many different projects and images, a migration to the new architecture might not be recommendable. These projects are different for a reason, or are under the supervision of different administrators, and therefore cannot be easily unified. However, the export and import of single projects might make it feasible to reduce the number of OSD Managers and condense the local architectures on individual sites.

Limitations

Windows versions before Windows Vista (XP, XP 64-bit, 2003, 2003 R2, and so on) are no longer supported as OSD Managers due to Windows ADK restrictions, as the Windows ADK cannot be installed on these operating systems. In the new architecture these devices can only have the role of image repository. Former OSD Managers on these operating systems are still shown in the console as OSD Managers, but they are not usable any more. Projects existing on these devices can be exported via the **File > Export** menu of the console and be imported to other OSD Managers.

Driver by model upgrade side-effects

Sometimes, for recent hardware, not all drivers could be automatically detected by the WinPE WMI script. A workaround was created, which involves determining the model ID of the computer, creating a folder with that name on a Samba share, dumping the drivers in it. After the OSD WIM install is run, the model ID of the machine is compared to this folder and its content is copied to the OSD destination folder on the installed system. On the next boot, Windows installs its components using the local OSD driver folder.

This process is now integrated in the OSD functionality and automated to some extent. However, the workaround does not work anymore, you need to execute the following procedure to make it work again:

> ⚠ **Note:**

This method only works for Windows Vista and later, as only those systems support recursive driver folders.
Samba shares for the model driver folder are not supported, the driver folders must be located in a local path of the OSD Manager.
The name of the models for existing folders is already in the correct format, Client Management uses the same system call as the workaround to find it.
The method is activated by default, therefore the projects using the workaround do not need to be updated, they are fully functional again, after they are rebuilt.

1. Copy or move all your driver folders from the Samba share to the new dedicated location on the OSD Manager: **<driver cache root>\bymodel\<model name>. You can do so directly under the Drivers by Model** node.

   Note:

   The driver cache folder can be changed by the user to another location in the OSD configuration interface in the console, but the content is not moved to the new location, this is a manual operation.

2. Rebuild the projects, concerned by the modified driver folders.

Example:

The previous path was **\\10.5.159.46\drivers\Optiplex GX280** . It must be copied manually to the default driver cache folder and becomes **C:\Program Files\BMC Software\Client\data\OsDeployment\drivers\bymodel\Optiplex GX280**.

Delta versus project transfer

Client Management now uses a stream database module to transfer as little data as possible across networks. This might be especially advantageous in networks with low bandwidth parts.

This new module allows the OSD agent to decide, if it is more advantageous, to transfer the complete new updated version of an object, or if the delta between the last version, currently stored on the transfer target, and the new version is smaller, and thus should be transferred instead. In this case, several deltas might be transferred instead of the complete new version.

Related topics

- Upgrading to Windows ADK and installing Windows ADK
- Upgrading OSD to v12.1 and later by consolidating to one OSD Manager
- Partially upgrading the OSD architecture to version 12.1 and later

Upgrading to Windows ADK and installing Windows ADK

Upgrading to Windows ADK

Due to the new UEFI compatibility in OSD, the previously used Windows AIK cannot be used anymore and must be replaced by the Windows ADK. The following scenarios are possible:

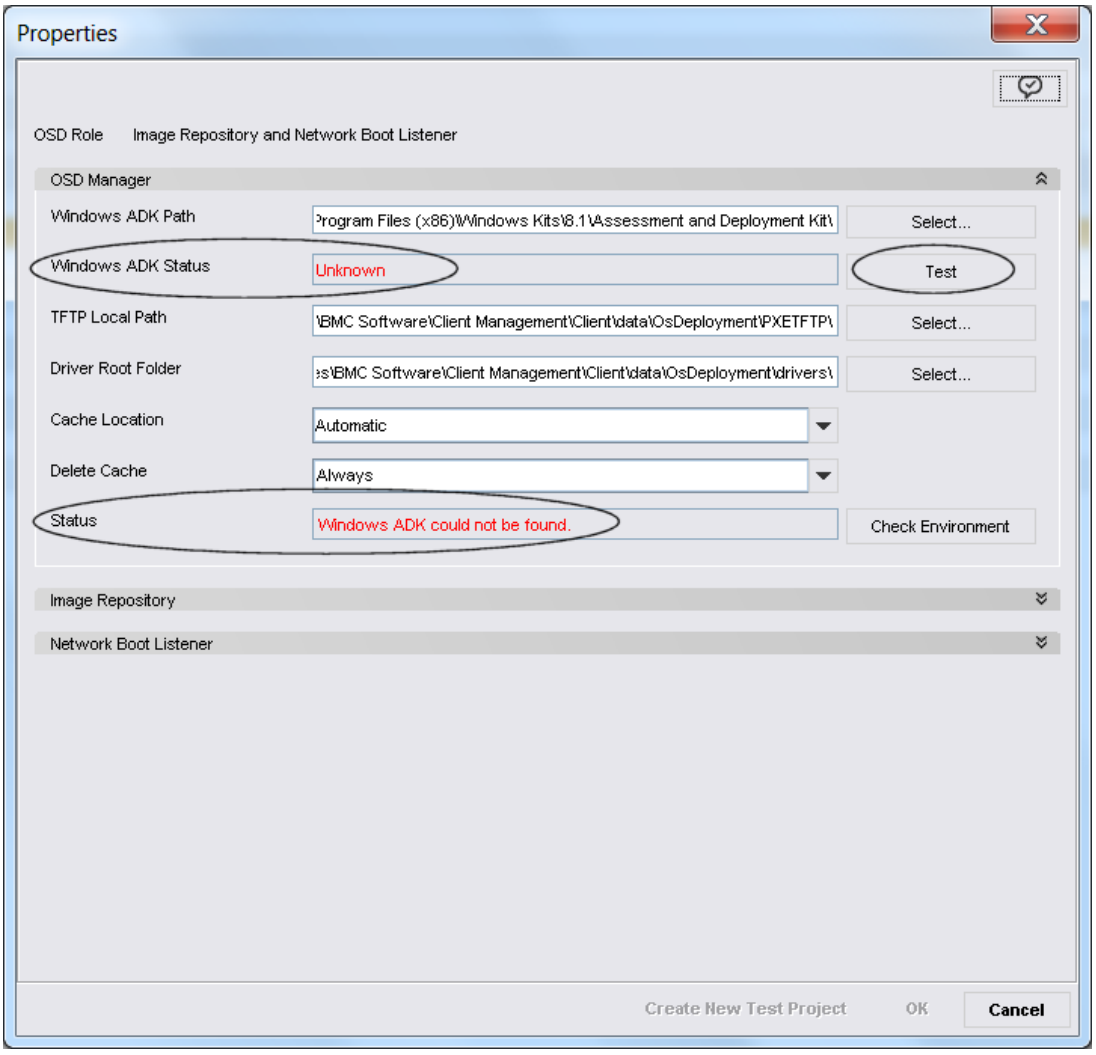
- Internet connection is available on the OSD Manager
  The OSD Manager configuration window has a button that allows the user to download and start the installation of the Windows ADK.
- No Internet connection or proxy on the OSD Manager
  The Windows ADK must be installed manually, using cached files from a computer with Internet connection and a specific command line to download the cache.

Upgrading to WADK with internet

This procedure guides you through the steps to install the Windows ADK (WADK) via the CM console. This procedure requires a working Internet connection on the OSD Manager device.

1. Select the **OS Deployment> Your OSD Manager** node.
2. Select the **Configuration** subnode.
3. Click **Properties** .The **Properties** window appears on the screen. If you have already upgraded the agent to version 12.1 the former Windows AIK path was replaced with the default WADK installation path. The **Windows ADK Status** box displays the **Unknown** message and the overall **Status** box shows **Windows ADK could not be found.** .

> **Note:**
>
> If the Windows AIK path was located on another drive letter, the new WADK path will also be put on this drive letter.

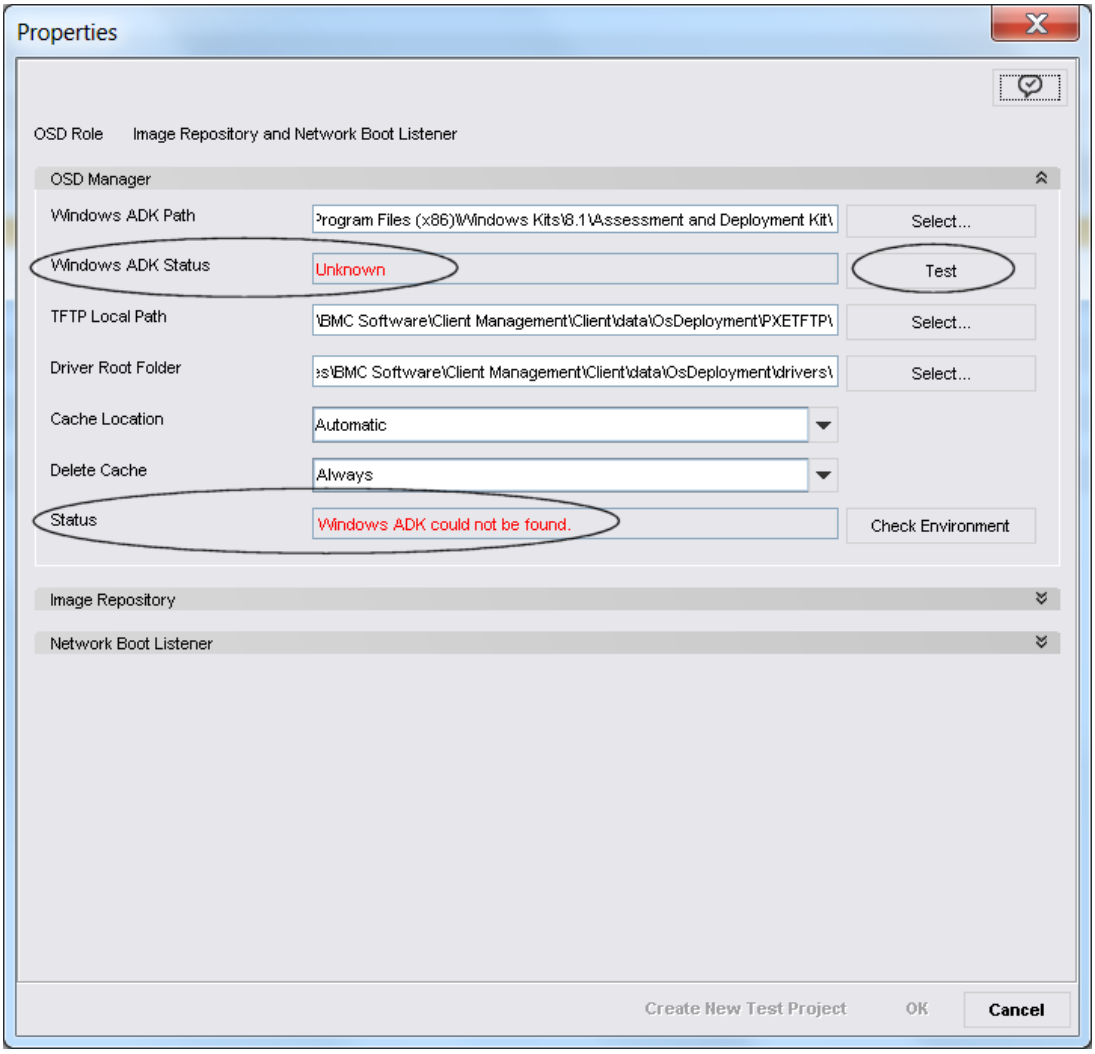


4. *(Optional)* If you want to install the WADK not in its default location, modify the path in the **Windows ADK Path** box.
5. Click **Test** next to the **Windows ADK Status** box.
   The CM agent now verifies if the OSD Manager has a working Internet connection and displays the result in the **Windows ADK Status** box. If the OSD Manager does not have a working Internet connection, see Installing the Windows ADK manually for instructions on how to install the WADK manually. If the status **Internet installation available** is displayed the label of the button changes to **Install Windows ADK** .
6. Click the **Install Windows ADK** button.

> The download and installation process may take quite a while, it is not necessary to keep this window open, to complete the installation. You can reopen it later to verify the progress and result.

The CM agent starts the download of the WADK installation package now and runs the installation. You can follow the progress via the different status values displayed in the **Windows ADK Status** box. The final status is **Windows ADK installed** . If the installation fails, see Installing the Windows ADK manually for instructions on how to install the WADK manually.

7. When the final status is displayed click the **Check Environment** button at the bottom next to the overall **Status** box to verify your environment.If the WADK installation is correct and all your other parameters are still valid the status OK is displayed.



Your OSD Manager is now updated and correctly configured; it is ready for creating and deploying operating systems in your network.

> **Note:**
>
> The previously used Windows AIK is not removed by the installation process, you need to do so manually, if you do not need it for any other operations.

The following topics provide more information about installing the Windows ADK:

Installing the Windows ADK manually

If your OSD Manager does not have an Internet connection, you must download the Windows ADK (WADK) via another computer with Internet connection.

1. On a computer with Internet access go to http://www.microsoft.com/en-US/download/details.aspx?id=39982 .
2. Download the **adksetup.exe** and save it locally.

3. Run in a terminal window as administrator the following command:

```
adksetup /layout <path>
```

whereby **<path>** is the location where the downloaded files are to be stored.

4. Copy the complete download with all directories and files to the OSD Manager.
5. Open a terminal window on the OSD Manager as administrator.
6. Go to the location of the downloaded cache.

7. Run the following command:

```
adksetup /quiet /installpath <path> /features
OptionId.WindowsPreinstallationEnvironment OptionId.DeploymentTools /log <path>
```

whereby

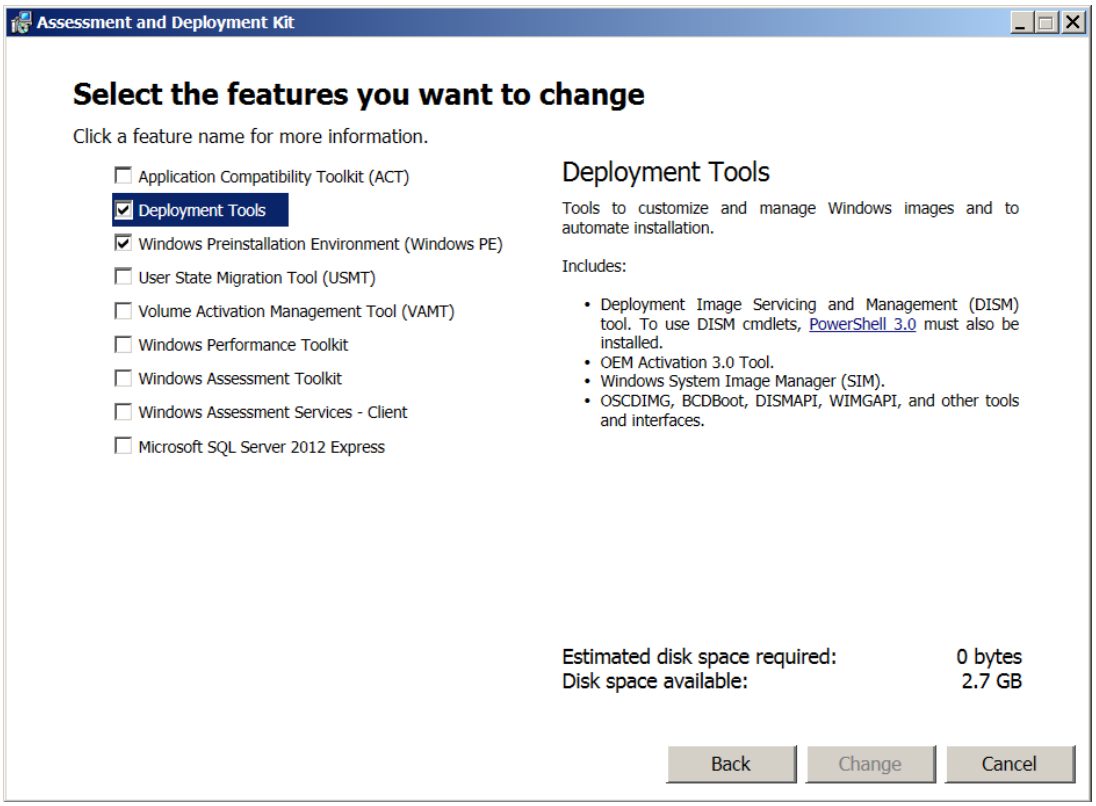
- **installpath <path>** is the full path to the installation directory of the Windows ADK.
- **log <path>** is the full path, where the WADK installation log is to be stored.

> The installation is silent, all necessary parameters are in the command line. Be aware that the installation can take a while.
> If the installation fails the first time, try again without the **installpath <path>** parameter. If a computer already has components of the Windows kit installed this may cause the installation to fail.

Installing the Windows ADK manually with Internet connection

It is also possible to manually install the Windows ADK on the OSD Manager with an Internet connection.

1. Go to http://www.microsoft.com/en-US/download/details.aspx?id=39982 .
2. Download the **adksetup.exe** and save it locally.
3. Launch the **adksetup.exe**.
   The installation wizard appears on the screen.



4. Select at least the **Deployment Tools** and **Windows Preinstallation Tools (Windows PE)** components, these are required for OSD to properly function.
5. Follow the installation instructions as explained by Microsoft: https://msdn.microsoft.com/en-us/library/hh825494.aspx .

Upgrading OSD to v12.1 and later by consolidating to one OSD Manager

This upgrade process is *only* for implementations that use the same projects and images throughout their entire infrastructure.

Upgrading to the new architecture with only one OSD Manager involves several steps.

> **Note:**
>
> Make sure you have read the upgrade considerations before you start this process.

1. Go to the **OS Deployment** node.
2. Define which of your many OSD Managers is going to be your unique OSD Manager.
3. Select all other OSD Mangers in the right window pane.
4. Click **Remove OSD Manager** .
   All spare OSD Managers are removed from the list, only the future OSD Manager remains.
5. Select your OSD Manager in the left tree and select its **Members** tab in the right pane.

6. Click **Add Image Repository/Network Boot Listener** .
7. Select the former OSD Manager devices in the **Add an Image Repository or a Network Boot Listener** window.
8. Check the **Image Repository** box.
9. *(Optional)* If the agent is not to be a network boot listener, clear the **Network Boot Listener** box.
10. Click **OK** .
    Your former OSD Managers were now all added as image repositories directly under the remaining OSD Manager.
11. Install the Windows ADK on the OSD Manager device.
12. After the Windows ADK installation, select the **Configuration** node of the OSD Manager.
13. Click **Properties** .
14. In the **Properties** window verify that the **Windows ADK Path** is correct.
15. *(Optional)* If this is not the case click **Select** next to the text box. A pop-up menu appears with the directory structure of the device where you can directly select the installation directory. Click **OK** to confirm and close the window.
16. Click **Test** next to the **Windows ADK Status** box, to test if the Windows ADK is correctly installed.
    If the OSD agent can find the Windows ADK in the indicated directory and it is fully functional the status is updated to **Windows ADK installed**. For any other status value review your installation and installation directory and repeat the test until the **Windows ADK installed** status is displayed.
17. Click **Check Environment** to verify that all your OSD Manager parameters are still properly set and working.
18. Select the **Storage** tab of your OSD Manager.
19. Click the **Synchronize** button in the top panel of the **Storage** tab.
20. In the appearing **Select Image Repositories** window select all image repositories.

    This operation transfers all OSD objects from the OSD Manager's image repository to all your former OSD Managers and makes them available to the targets.

21. Click **OK** .
    The **Operation Status** window appears, displaying the list of all image repositories and the synchronization status of all objects on each.

Note:

Be aware, that this status only shows, if the synchronization order was sent to the respective target, it does not indicate that the target received the order or that the objects were synchronized on it.

The order to synchronize the objects on the image repositories is launched. To verify if the image repositories are synchronized, you must check the **Storage** tab of each target.

Once the synchronization is completed your situation should be as it was before the upgrade, but with the new architecture.

> **Note:**
>
> This upgrade procedure purged most OSD folders of generated data on the former OSD Managers. The driver cache folder must be manually removed as well as the Windows AIK, which is no longer required on these devices.

Partially upgrading the OSD architecture to version 12.1 and later

If your architecture doesn't permit you to use only one OSD Manager, but there are still some areas of your network where you can consolidate the system, here's a procedure how to partially move to the new OSD architecture.

> **Note:**
>
> Make sure you have read the upgrade considerations before you start this process.

1. Uninstall the Windows AIK and install the Windows ADK on all devices that remain OSD Managers in your new architecture.
2. After the Windows ADK installation, select the **Configuration** node of the OSD Manager.
3. Click **Properties** .
4. In the **Properties** window verify that the **Windows ADK Path** is correct.
5. *(Optional)* If this is not the case, click **Select** next to the text box. A pop-up menu appears with the directory structure of the device where you can directly select the installation directory. Click **OK** to confirm and close the window.
6. Click **Test** next to the **Windows ADK Status** box, to test if the Windows ADK is correctly installed.
   If the OSD agent can find the Windows ADK in the indicated directory and it is fully functional the status is updated to **Windows ADK installed**. For any other status value, review your installation and installation directory and repeat the test until the **Windows ADK installed** status is displayed.
7. Click **Check Environment** to verify that all your OSD Manager parameters are still properly set and working.
8. Repeat the following procedure on all obsolete OSD Managers that are going to be removed:
   a. Select the projects you want to move to the new parent OSD Managers under the respective **Projects** node.

b. Click **Edit > Export** .
c. In the **Export the Current Node** dialog box enter the file path for the export directly into the **File Path** box or click the button next to it to call a list of all available drives and directories of your client.

> The path entered here must be a full path, it cannot be a relative path. Besides, you must enter a name for your export file with an extension.

d. Click **OK** .

> If the content of your exported objects are not in a location accessible by the new OSD Manager, you must also copy all the object content, that is the drivers, the image, and so on, to a location accessible by the new OSD Manager. The directory structure as it is defined in the object must be exactly the same on the target as it was on the source, otherwise the project build on the new OSD Manager will fail.

9. On the new parent OSD Manager go to the **Projects** node.
10. Click **Edit > Import** .
11. In the **Import a Node** dialog box select the file containing the data to import.
12. Click **OK**.
13. When the import is completed, go to the object properties and make sure everything still works, that is, if you are importing a project, click the test buttons and rebuild it.
    Go to the **Storage** tab to follow as the newly build projects come online again and are synchronized with the OSD Manager's image repository and thus become available to all children.

> **Note:**
>
> If a project appears in the list, but the connected image is not added, an error occurred during the build.

14. Select the **OS Deployment** node.
15. Select all obsolete OSD Mangers, from which you have recovered all still needed objects in the right window pane.
16. Click **Remove OSD Manager** .
    All obsolete OSD Managers are removed from the list.
17. Select your new parent OSD Manager in the left tree and select its **Members** tab in the right pane.

18. Click **Add Image Repository/Network Boot Listener** .
19. Select the obsolete OSD Manager devices from under this new parent in the **Add an Image Repository or a Network Boot Listener** window.
20. Check the **Image Repository** box.
21. *(Optional)* If the agent is not to be a network boot listener, clear the **Network Boot Listener** box.
22. Click **OK**.
    Your obsolete OSD Managers are now all added as image repositories directly under the new parent OSD Manager.
23. Select the **Storage** tab of your OSD Manager.
24. Select the objects that you moved from your obsolete OSD Manager to the new one in the right window pane.
25. Click **Edit > Synchronize** button.
26. In the appearing **Select Image Repositories** window select your obsolete OSD Manager, that is now an image repository.

    This operation transfers the selected OSD objects from the OSD Manager's image repository to your obsolete OSD Managers and makes them available to the targets.

27. Click **OK** .
    The **Operation Status** window appears, displaying the list of all image repositories and the synchronization status of the objects on each.

    Note:

    Be aware, that this status only shows, if the synchronization order was sent to the respective target, it does not indicate that the target received the order or that the objects were synchronized on it.

The order to synchronize the objects on the image repositories is launched. To verify if the image repositories are synchronized, you must check the **Storage** tab of each target.

Once the synchronization is completed your situation should be as it was before the upgrade, but with the new architecture.

Note:

This upgrade procedure purged most OSD folders of generated data on the former OSD Managers. The driver cache folder must be manually removed as well as the Windows AIK, which is no longer required on these devices.

Performing advanced OSD tasks

This section introduces you to further operating system deployment modes and options to leverage the complete functionality of the CM 's BMC Client Management - Operating System Deployment .

It provides the following examples:

- Creating an Image Capture
- Creating a SysPrep WIM image capture
- Creating a target in static IP mode
- Creating a target via a PXE subnet (setup mode)
- Creating a target via PXE subnet (non-setup mode)
- Deploying a Custom Image
- Deploying a Sysprep WIM image
- Deploying by multicast setup mode
- Deploying a WIM Image with PXE menu
- Creating a USB device to deploy operating systems

Creating an Image Capture

As the next example we will create a new master WIM image of the legacy device on which we just installed the *Windows 2008* 64-bit operating systems via the setup mode via the **Capture by WIM Image** option of the wizard. This mode makes a snapshot of an existing system on the active disk, usually C and creates a WIM image of it, which can then be used to be deployed to new devices as we will do in the next example. This procedure will also be executed via the **OS Deployment Wizard** , however, before you launch the wizard ensure that the device of which the image will be created is up and running.

1. To launch the **OS Deployment Wizard** select the **Wizards> OS Deployment** menu item. The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. Select the **Capture by WIM Image** option.
5. Click **Next** to continue.
6. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) Image Capture.
Architecture	Select the 64 Bit option for the 64-bit Windows 2008 image capture.

Parameter	Description
Supported BIOS Type	Select Legacy Only.
Target Drive	Select from this list box the drive letter on which the operating system is installed, in our example this should be the C drive, therefore select C from this list box.
Operation after Installation	Select from this list the Shutdown option.

7. Click **Next** to continue.
8. Leave the preselected value and click **Next** to continue.
   In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name box, for example Windows 2008 (64 bit) Image Capture.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Type	Select the Windows Vista / 7 / 8 / 10 Setup option.
Location	Enter into this text box network path including the name to the image folder, where the image to create is to be stored, for example, \\192.168.196.13\Build\Windows2008-64bit.wim. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager.

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right. The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window. The account will be added in the wizard window boxes.

9. To verify click **Check Image** to the right of the **Status** box.
   CM will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status**`Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
10. After the **Status**`Done` is returned click **Next** to go to the following wizard page.
11. The option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
12. Enter for example the name *Windows 2008 (64 bit) Image Capture* into the **Name** box.

13. This deployment will, of course, only have one target device and we will add it as a new target. For this select **Create Target** on top of the empty list box.
    The **Create a New Target** window appears.
14. Enter the following information into the respective boxes:

Parameter	Description
Name	Enter into this text box the short name of the target device exactly as you entered it for the setup, for example, scotty.
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes, preferably the MAC Address. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

15. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.
16. Click **Next** to continue.
17. Leave the preselected disk configuration and click **Next** .

> This configuration does not touch the disk. Make sure not to select any configuration that erases the disk and reformats it.

18. In the **Deployment Drivers** window mark the check boxes for all necessary WinPE drivers. This indicates that they are to be used.
19. Click **Next** to continue.
20. Leave all values as they are and click **Next** to continue.
21. As we want to activate and execute this image capture right away leave all values as they are and click **Finish** to launch the deployment.

The project will now be build, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on You can follow the progress of the project in its console node, because the focus of the console will automatically be moved to this object when the wizard is finished. In this view you can follow the different stages of the build. If any other than the final status `Build completed successfully.` displays the build failed and you need to review the parameters of the project and maybe the source files.

After the build is successfully completed the snapshot of the target device is started. You can follow the progress of the image creation process by selecting the **Assigned Objects > Target List > Your Target List** node in the left window pane. The right pane displays the target list member with its status information.

Creating a SysPrep WIM image capture

As the next example we will create a UEFI sysprep WIM image. This procedure will also be executed via the **OS Deployment Wizard** , however, before you launch the wizard ensure that the device of which the image will be created is up and running.

1. To launch the **OS Deployment Wizard** select the **Wizards > OS Deployment** menu item. The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. Select the **Capture by WIM Image** option.
5. Click **Next** to continue.
6. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) Sysprep Image Capture.
Architecture	Select the 64 Bit option for the 64-bit Windows 2008 image capture.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Target Drive	Select from this list box the drive letter on which the operating system is installed, in our example this should be the C drive, therefore select C from this list box.
Operation after Installation	Select from this list the Shutdown option.

7. Click **Next** to continue.
8. Leave the preselected value and click **Next** to continue.
9. In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name box, for example Windows 2008 (64 bit) Sysprep Image Capture.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Type	Select the Windows Vista / 7 / 8 / 10 Sysprep WIM Image option.
Location	Enter into this text box network path including the name to the image folder, where the image to create is to be stored, for example, `\\192.168.196.13\Build\Windows2008-64bit-sysprep.wim.`. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager.

Parameter	Description

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right.
	The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window.
	The account is added in the wizard window boxes.

10. To verify click **Check Image** to the right of the **Status** box.
    CM will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status** `Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
11. After the **Status** `Done` is returned click **Next** to go to the following wizard page.
12. *(Optional)* In the **OS Drivers** select the necessary operating system drivers and click **Next** .
13. *(Optional)* In the **OS Drivers**) select the necessary drivers by model and click **Next** .
14. The option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
15. Enter for example the name *Windows 2008 (64 bit) Sysprep Image Capture* into the **Name** box.
16. This deployment will, of course, only have one target device and we will add it as a new target. For this select **Create Target** on top of the empty list box.
    The **Create a New Target** window appears.
17. Enter the following information into the respective boxes:

Parameter	Description
Name	Enter into this text box the short name of the target device exactly as you entered it for the setup, for example, scotty.
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes, preferably the MAC Address. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

18. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.
19. Click **Next** to continue.
20. *(Optional)* In the **MBR Disk Configuration** select the desired disk configuration for legacy installations and click **Next** .
21. *(Optional)* In the **GPT Disk Configuration**) select the desired disk configuration for UEFI installations and click **Next** .
22. Leave the preselected disk configuration and click **Next** .

> This configuration does not touch the disk. Make sure not to select any configuration that erases the disk and reformats it.

23. In the **Deployment Drivers** window mark the check boxes for all necessary WinPE drivers. This indicates that they are to be used.
24. Click **Next** to continue.
25. Leave all values as they are and click **Next** to continue.
26. As we want to activate and execute this image capture right away leave all values as they are and click **Finish** to launch the deployment.
    The project will now be build, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on.

> **Note:**
>
> If any other than the final status `Build completed successfully.` displays the build failed and you need to review the parameters of the project and maybe the source files.

27. After the wizard has finished building the image the provided batch file `//Selecting the OSD Manager-O/PXETFTP/SYSPREP/RUNSYSPREP.BAT` , that will sysprep the target and finally reboot it, must be launched.

> The file must be executed as a privileged user (admin). If the file cannot be found in this location the project is not activated or not set as a Sysprep image type.

> The **Sysprep** batch script ensures that the BCM agent GUID is reset in the captured OS image. It ensures that duplicate GUIDs are not generated when deploying the OS image.

After the batch file is launched the snapshot of the target device is started. You can follow the progress of the image creation process by selecting the **Assigned Objects > Target List > Your Target List** node in the left window pane. The right pane displays the target list member with its status information.

Creating a target in static IP mode

Target devices can also be created in static mode. To do so, proceed as follows:

1. Select **Create Target** .
   The **Create a New Target** window opens on the screen with its three tabs, **General Information**, **Parameters** and **Unattended Information**.

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, `scotty`. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: `A-Z, a-z, 0-9`, the underscore (_) and a dash (n/a).
Target	Leave this radio button selected to attribute static IP addresses.

2. Select the **Parameters** tab and fill in the boxes for the target operating system information.

Parameter	Description
Edition	Select from the drop-down box the Windows edition that is being installed, for example Windows Vista Enterprise. The listed editions were automatically detected from the installation CD/DVD.
Language	Select from the drop-down box the language. This language setting will be applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages were automatically detected from the installation CD/DVD.
Product Key	Enter into this text box the OS product key (for example, `ABCDE-FGHIJ-KLMNO-PQRST-UVWXY`).
Static IP	Select this radio button to statically assign the IP addresses to the devices. The following text boxes must be defined for static IP addressing:
Host IP Address	Enter into this text box the IP address which is to be attributed to the target device. This text box is mandatory.
Subnet Mask	Enter into this text box the subnet mask for the target device. This text box is mandatory.
Gateway	Enter into this text box the IP address of the gateway of the target device. This text box is mandatory.
Preferred DNS Server	Enter into this text box the IP address of the preferred DNS server of the target device. This text box is mandatory.
Alternate DNS Server	Enter into this text box the IP address of the alternate DNS server of the target device. This text box is optional.

Click **Default Values** below these boxes to preenter the **Subnet Mask** , **Gateway** and **Preferred DNS Server** boxes with the default values.

3. Select the **Unattended Information** tab and fill in the boxes for your organization.
4. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.

Creating a target via a PXE subnet (setup mode)

You can also create new target devices by specifying a subnet in which they will be located. When creating new targets in this way, it is added to the OS Deployment database specifically for this deployment. To do so, proceed as follows:

1. Select **Create Target** .
   The **Create a New Target** window opens on the screen with its three tabs, **General Information**, **Parameters** and **Unattended Information**.
2.

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, `scotty`. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: `A-Z, a-z, 0-9`, the underscore (_) and a dash .
PXE Subnet Filter	Select this radio button. A new text box next to the preceding Name text box appears in the window. You can enter into this text box the way the device names within a subnetwork are automatically incremented. The default value here is 001, that is, the name with the suffix 001, 002, and so on, for example, HQ001, HQ002, ... HQ099.
PXE Subnet Filter	Enter into this text box the IP address in its dotted notation for the subnet which is to contain the target devices. The address can be entered with the wildcard character asterisks (*): 192.168.1.**,** 192.168..* or 192..*.

3. Select the **Parameters** tab and fill in the boxes for the target operating system information.

Parameter	Description
Edition	Select from the drop-down box the Windows edition that is being installed, for example Windows Vista Enterprise. The listed editions were automatically detected from the installation CD/DVD.
Language	Select from the drop-down box the language. This language setting will be applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages were automatically detected from the installation CD/DVD.
Product Key	Enter into this text box the OS product key (for example, `ABCDE-FGHIJ-KLMNO-PQRST-UVWXY`).
TCP/IP Parameters	The boxes in this box provide you the possibility to define the parameters for static or dynamic IP address management:
Dynamic IP	Select this radio button to dynamically assign the IP addresses for the devices. This option is only applicable to Setup projects. This is the default value.
Static IP	Select this radio button if the IP addresses are statically assigned to the devices. The following text boxes must be defined for static IP addressing:
Host IP Address	Enter into this text box the IP address which is to be attributed to the target device. This text box is mandatory.
	Enter into this text box the subnet mask for the target device. This text box is mandatory.

Parameter	Description
Subnet Mask	
Gateway	Enter into this text box the IP address of the gateway of the target device. This text box is mandatory.
Preferred DNS Server	Enter into this text box the IP address of the preferred DNS server of the target device. This text box is mandatory.
Alternate DNS Server	Enter into this text box the IP address of the alternate DNS server of the target device. This text box is optional.

Click **Default Values** below to preenter the **Subnet Mask** , **Gateway** and **Preferred DNS Server** boxes with the default values.

4. Select the **Unattended Information** tab and fill in the boxes for your organization.
5. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.

Creating a target via PXE subnet (non-setup mode)

You can also create new target devices by specifying a subnet in which they will be located. When creating new targets in this way, it is added to the OS Deployment database specifically for this deployment. To do so, proceed as follows:

1. Select **Create Target** .
   The **Create a New Target** window opens on the screen with its three tabs, **General Information**, **Parameters** and **Unattended Information**.

Note:

As we are now creating a target for the non-setup modes you can ignore the **Parameters** and **Unattended Information** tabs, because these are only applicable to the setup mode.

2. Fill in the boxes for the following parameters:

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, `scotty`. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: `A-Z, a-z, 0-9`, the underscore (_) and a dash .
PXE Menu	

Parameter	Description
	Select this radio button to define the targets via a PXE menu. A new text box next to the preceding Name text box appears in the window. You can enter into this text box the way the device names within a subnetwork are automatically incremented. The default value here is 001, that is, the name with the suffix 001, 002, and so on, for example, HQ001, HQ002, ... HQ099.

3. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.

Deploying a Custom Image

To execute this example you need an already prepared custom image ready and available, such as for example a ghost image.

1. To launch the **OS Deployment Wizard** select the **Wizards > OS Deployment** menu item. The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. In the **Deployment Type** windows select the **Custom Mode** option and click **Next** to continue.
5. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) Custom Deployment.
Architecture	This list box indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. Select the 64 Bit option for the 64-bit Windows 2008 setup deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Target Drive	Select from this list box the drive letter on which the operating system is to be installed, in our example we will use the C drive, therefore select C from this list box.

6. Click **Next** to go to the following wizard page.
7. The option to create a new image (**Create a new OS image or setup**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the parameters of the new image.
8. In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name box, for example Windows 2008 (64 bit) Custom Deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Location	

Parameter	Description
	Enter into this text box network path to the folder, where the custom image and the program is located, for example, `\\192.168.196.13\ghosts64`. This is the folder which contains the ghost executable file for the deployment and the ghost image. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager and the target devices.

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right. The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window. The account will be added in the wizard window boxes.

Custom Image Command Line	This text box contains the command required to deploy the image, for example, ghost32.exe -clone, mode=restore,src=W:/XP32.GHO,dst=1:0 -SURE for a ghost image, whereby W: is the mounted share of the UNC OS location in the WinPE. An example when using imagex would be: imagex /apply "W:/MyImageFile.wim" 1 C:.
By Disk	If the option is selected the script does not do anything partition or disk related after running the custom command.

After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** `Done` , the wizard cannot continue.

9. To verify click **Check Image** to the right of the **Status** box.
   CM will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status** `Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
10. After the **Status** `Done` is returned, click **Next** to go to the following wizard page.
11. *(Optional)* In the **OS Drivers** select the necessary operating system drivers and click **Next** .
12. *(Optional)* In the **OS Drivers**) select the necessary drivers by model and click **Next** .
13. In the target list window the option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
14. Enter for example the name *Windows 2008 (64 bit) Custom Deployment* into the **Name** box.
15. This deployment will only have one target device and we will add it as a new target. For this click **Create Target** on top of the empty list box.
    The **Create a New Target** window appears.
16. Enter the following information into the respective boxes of the **General Information** tab for the new device:

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, scotty. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: A-Z, a-z, 0-9, the underscore (_) and a dash .
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device. This is the most precise information to identify the device and should be preferred to the other two following identification options. The MAC address can be entered in one of the following formats: xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

17. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.
18. Click **Next** to go to the following wizard page, **Disk Configuration** .
19. *(Optional)* In the **MBR Disk Configuration** select the desired disk configuration for legacy installations and click **Next** .
20. *(Optional)* In the **GPT Disk Configuration**) select the desired disk configuration for UEFI installations and click **Next** .
21. Leave the preselected disk configuration and click **Next** to continue.
22. In the **Deployment Drivers** window mark the check boxes for all required WinPE drivers, that is, at least one network and possibly a SATA driver.

> If you have not yet defined the necessary drivers you can do so also in this wizard window. For this see topics Scanning a Directory for Drivers and Defining Deployment Drivers which describe the different processes.

23. Click **Next** to continue.
24. In the **PXE Menu Parameters** window leave all values as they are and click **Next** to continue.
25. As we want to activate and execute this first deployment right away leave all values as they are and click **Finish** to launch the deployment.

The project will now be build, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on You can follow the progress of the project in its console node, because the focus of the console will automatically be moved to this object when the

wizard is finished. In this view you can follow the different stages of the build. If any other than the final status `Build completed successfully.` displays the build failed and you need to review the parameters of the project and maybe the source files.

After the build is successfully completed the files are put at the required location on the OSD Manager for deployment. To now start the actual operating system deployment to the target device you must switch on the device. It will boot on the PXE boot section and the operating system installation is executed.

> **Note:**
>
> Do not start the target devices before the project is finished and ready to launch the installation. If the target devices are already running before the PXE boot will not find the files for the installation and the deployment and installation of the new OS on the target devices will not take place.

You can follow the progress of the installation process of the ghost by selecting the **Assigned Objects > Target List > Your Target List** node in the left window pane. The right pane displays the target list member with its status information.

Deploying a Sysprep WIM image

In this example we will install a new device via the **WIM Image Mode** using the WIM image we captured in the preceding example. The **WIM Image Mode** uses a snapshot of an operating system taken of an installed device to install the same operating system on the target device or a sysprepped OS, able to be deployed on various hardware types. The snapshot or image file contains all information required to install the new device.

1. To launch the **OS Deployment Wizard** select the **Wizards > OS Deployment** menu item. The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. In the **Deployment Type** window select the **WIM Image Mode** option and click **Next** to continue.
5. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) Syprep WIM Image Deployment.
Architecture	This list box indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. Select the 64 Bit option for the 64-bit Windows 2008 WIM image deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.

Parameter	Description
Target Drive	Select from this list box the drive letter on which the operating system is to be installed, in our example we will use the C drive, therefore select C from this list box.

6. Click **Next** to go to the following wizard page.
7. The option to create a new image (**Create a new OS image or setup**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the parameters of the new image.
8. In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name box, for example Windows 2008 (64 bit) Syprep WIM Image Deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Type	From the list select the Windows Vista / 7 / 8 / 10 Sysprep WIM Image option.
Location	Enter into this text box network path to the folder, where you stored the image file that we created in our previous example including the name of the image, for example, `\\192.168.196.13\Build\Windows2008-64bit-sysprep.wim`. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager and the target devices, that is, it is therefore recommended to put it on a device within the subnet.

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right. The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window. The account will be added in the wizard window boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** `Done` , the wizard cannot continue.

9. To verify click **Check Image** to the right of the **Status** box.
   CM will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status** `Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.

10. After the **Status** `Done` is returned click **Next** to go to the following wizard page.
    The **OS Drivers** appears.

> **Note:**
>
> For a sysprep installation, an extra wizard window will be displayed in which other drivers required by the SysPrep installation must be defined. This is the equivalent for manually inserting the drivers floppy during the installation process. Here you can define all drivers that might be needed by the deployment operating system to properly run.

11. Select the drivers that are needed by the operating system, that is, any other required video, audio, modem drivers, and so on, by checking their respective boxes.

> If you have not yet defined the necessary drivers you can do so also in this wizard window. For this see topics Scanning a Directory for Drivers and Defining OS Drivers which describe the different processes.

12. Click **Next** to go to the following wizard page, **Target List Configuration** .
13. *(Optional)* In the **OS Drivers** select the necessary operating system drivers and click **Next** .
14. *(Optional)* In the **OS Drivers**) select the necessary drivers by model and click **Next** .
15. The option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
16. Enter for example the name *Windows 2008 (64 bit) Setup Deployment* into the **Name** box.
17. Select the template of the unattended file that is to be used for the deployment.

> You can either use the template which is provided by BMC , leave the text box empty, or you can use you own custom defined file. For this example we will use the BMC default file, therefore do not modify the entry. If you use your own customized `Unattend.xml` file make sure it is in UTF-16 encoding.

> If the unattended file template box is empty, the OSD Manager will use the default unattended file template corresponding to the image type.

18. This deployment will only have one target device and we will add it as a new target. For this select **Create Target** on top of the empty list box.
    The **Create a New Target** window appears with its three tabs, **General Information** , **Parameters** and **Unattended Information** .
19. Enter the following information into the respective text boxes of the **General Information** tab for the new device:

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, scotty. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: A-Z, a-z, 0-9, the underscore (_) and a dash .
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device. This is the most precise information to identify the device and should be preferred to the other two following identification options. The MAC address can be entered in one of the following formats: xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

20. Select the **Parameters** tab and fill in the boxes for the target operating system information.

Parameter	Description
Edition	Select from the drop-down box the Windows edition that is being installed, for example Windows Vista Enterprise. The listed editions were automatically detected from the installation CD/DVD.
Language	Select from the drop-down box the language. This language setting will be applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages were automatically detected from the installation CD/DVD.
Product Key	Enter into this text box the OS product key (for example, ABCDE-FGHIJ-KLMNO-PQRST-UVWXY).

21. Select the **Unattended Information** tab and fill in the boxes for your organization.
22. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.
23. Click **Next** to continue.
24. *(Optional)* In the **MBR Disk Configuration** select the desired disk configuration for legacy installations and click **Next** .
25. *(Optional)* In the **GPT Disk Configuration**) select the desired disk configuration for UEFI installations and click **Next** .
26. In the list of available disk configurations select the **Disk with two partitions** option.

> This configuration will create two partitions on the hard disk, the first, the boot or active partition with 30 GB and the second with the remaining space.

27. Click **Next** to go to the following wizard page.
28. In the **Deployment Drivers** window mark the check boxes for all required WinPE drivers, that is, at least one network and possibly a SATA driver.
29. Click **Next** to continue.
30. Leave all values as they are and click **Next** to continue.
31. As we want to activate and execute this deployment right away leave all values as they are and click **Finish** to launch the deployment.

The project will now be build, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on You can follow the progress of the project in its console node, because the focus of the console will automatically be moved to this object when the wizard is finished. In this view you can follow the different stages of the build. If any other than the final status `Build completed successfully.` displays the build failed and you need to review the parameters of the project and maybe the source files.

After the build is successfully completed the files are put at the required location on the OSD Manager for deployment. To now start the actual operating system deployment to the target device you must switch on the device. It will boot on the PXE boot section and the operating system installation is executed.

> **Note:**
>
> Do not start the target devices before the project is finished and ready to launch the installation. If the target devices are already running before the PXE boot will not find the files for the installation and the deployment and installation of the new OS on the target devices will not take place.

> The **Sysprep** batch script ensures that the BCM agent GUID is reset in the captured OS image. It ensures that duplicate GUIDs are not generated when deploying the OS image.

You can follow the progress of the image creation process by selecting the **Assigned Objects > Target List > Your Target List** node in the left window pane. The right pane displays the target list member with its status information.

Deploying by multicast setup mode

This example creates a setup deployment, applicable to both UEFI and legacy computes, which is distributed by multicast.

To be able to execute this example you need to prepare two computers, preferably one with UEFI and one with legacy BIOS, to use for the multicast deployment.

1. To launch the **OS Deployment Wizard** select the **Wizards> OS Deployment** menu item. The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. Do not modify anything in this window and click **Next** to go to the following wizard page.
5. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) Setup Deployment.
Architecture	This list box indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. Select the 64 Bit option for the 64-bit Windows 2008 setup deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time. Make sure the Legacy and UEFI value is selected.
Target Drive	Select from this list box the drive letter on which the operating system is to be installed, in our example we will use the C drive, therefore select C from this list box.
Use Model Drivers	Uncheck this box, this example does not used model drivers.

6. Check the **Deployment by Multicast** box.
7. Click **Next** to continue.
8. In the **Edit Multicast Options** window clear the **After (Min.)** option of the **Automatic Start Conditions** parameter.
9. Click the drop-down-list to the right of the **Registered Targets** option and enter_2_ instead of the prepopulated value.
10. Click **Next** to continue.
11. The option to create a new image (**Create a new OS image or setup**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the parameters of the new image.
    In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name box, for example Windows 2008 (64 bit) Setup Deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Type	This parameter defines the image type being used for the deployment. This list is already pre-filtered and only provides image types applicable to the selected deployment mode. For our example select the Windows Vista / 7 / 8 / 10 Setup option.

Parameter	Description
Location	Enter into this text box the network path to the image or setup folder, where you copied the image files required for the installation, for example, `\\192.168.196.13\Windows2008-64bit`. This is the folder which contains the setup.exe file for the deployment. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager.

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right. The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window. The account will be added in the wizard window boxes.

After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** `Done` , the wizard cannot continue.

12. To verify click **Check Image** to the right of the **Status** box.
    CM will now verify all entries of this page, that is, the directory and the access rights to it.
    If all values are correct the **Status**`Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
13. After the **Status**`Done` is returned click **Next** to go to the following wizard page.
14. Select the drivers that are needed by the operating system, that is, any other required video, audio, modem drivers, and so on, by checking their respective boxes.

If you have not yet defined the necessary drivers you can do so also in this wizard window. For this see topics Scanning a Directory for Drivers and Defining OS Drivers which describe the different processes.

15. Click **Next** to go to the following wizard page, **Target List Configuration** .
16. *(Optional)* In the **OS Drivers** select the necessary operating system drivers and click **Next** .
17. *(Optional)* In the **OS Drivers**) select the necessary drivers by model and click **Next** .
18. The option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
19. Enter for example the name *Windows 2008 (64 bit) Setup Deployment* into the **Name** box.
20. Select the template of the unattended file that is to be used for the deployment.

> You can either use the template which is provided by BMC , leave the text box empty, or you can use you own custom defined file. For this example we will use the BMC default file, therefore do not modify the entry. If you use your own customized `Unattend.xml` file make sure it is in UTF-16 encoding.

> If the unattended file template box is empty, the OSD Manager will use the default unattended file template corresponding to the image type.

21. This deployment will only have two target devices and we will add them as a new targets. For this select **Create Target** on top of the empty list box.
    The **Create a New Target** window appears with its three tabs, **General Information** , **Parameters** and **Unattended Information** .
22. Enter the following information into the respective boxes of the **General Information** tab for the new device:

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, scotty. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: A-Z, a-z, 0-9, the underscore (_) and a dash .
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device. This is the most precise information to identify the device and should be preferred to the other two following identification options. The MAC address can be entered in one of the following formats: xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

23. Select the **Parameters** tab and fill in the boxes for the target operating system information.

Parameter	Description
Edition	Select from the drop-down box the Windows edition that is being installed, for example Windows Vista Enterprise. The listed editions were automatically detected from the installation CD/DVD.
Language	Select from the drop-down box the language. This language setting will be applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages were automatically detected from the installation CD/DVD.

Parameter	Description
Product Key	Enter into this text box the OS product key (for example, ABCDE-FGHIJ-KLMNO-PQRST-UVWXY).
TCP/IP Parameters	Leave the preselected option Dynamic IP in this box, this will automatically assign the target device its new IP address via DHCP.

24. Select the **Unattended Information** tab and fill in the boxes for your organization.
25. Click **OK** at the bottom of the window to confirm the data for the new target device and add it to the target list.
26. Repeat the preceding steps to add the second device.
27. Click **Next** to go to the following wizard page and the **Disk Configuration** .
28. *(Optional)* In the **MBR Disk Configuration** select the desired disk configuration for legacy installations and click **Next** .
29. *(Optional)* In the **GPT Disk Configuration**) select the desired disk configuration for UEFI installations and click **Next** .
30. In the list of available disk configurations select the **Disk with two partitions** option.

> This configuration will create two partitions on the hard disk, the first, the boot or active partition with 30 GB and the second with the remaining space.

31. Click **Next** to go to the following wizard page.
32. In the **Deployment Drivers** window mark the check boxes for all required WinPE drivers, that is, at least one network and possibly a SATA driver.
33. Click **Next** to go to the last wizard page.
34. As we want to activate and execute this first deployment right away leave all values as they are and click **Finish** to launch the deployment.
    The project is now built, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on. You can follow the progress of the project in its console node, because the focus of the console is automatically moved to this object when the wizard is finished. In this view you can follow the different stages of the build. If any other than the final status `Build completed successfully.` is displayed, the build failed and you need to review the parameters of the project and maybe the source files. The Multicast transfer is launched at once. Both targets are listed here and have the status `In Progress` .
35. Manually switch on the target devices.
    It will boot on the PXE boot section and the operating system installation is executed.

> **Note:**

Do not start the target devices before the project is finished and ready to launch the installation. If the target devices are already running the PXE boot will not find the files for the installation and the deployment and installation of the new OS on the target devices will not take place.

36. Select the **Multicast Sessions> Your Multicast Server> Your Multicast Session** subnode.
In this view you can follow the Multicast transfer.

> **Note:**
>
> The column **Sent (%)** indicates the advancement of the transfer for both devices. The transfer is terminated when the parameter **Server Status** displays `Done` .

37. You can follow the progress of the installation by selecting the **Assigned Objects> Target List > Your Target List** node in the left window pane.
The right pane displays the target list members with their status information. Find your target devices and follow the different stages in this view. At the same time you can see on the screen of the target device the advancement of the process.

Deploying a WIM Image with PXE menu

In this third example we will install a new device via the **WIM Image Mode** using the WIM image we captured in the preceding example. The **WIM Image Mode** uses a snapshot of an operating system taken of an installed device to install the same operating system on the target device or a sysprepped OS, able to be deployed on various hardware types. The snapshot or image file contains all information required to install the new device.

1. To launch the **OS Deployment Wizard** select the **Wizards > OS Deployment** menu item.
The wizard appears with its first window, **OSD Manager** .
2. Select *Your OSD Manager* .
3. Click **Next** to go to the following wizard page.
4. In the **Deployment Type** windows select the **WIM Image Mode** option and click **Next** to continue.
5. In the **Project Parameters** window define the following parameters:

Parameter	Description
Name	Enter a self-explanatory name for the project into this text box, for example Windows 2008 (64 bit) WIM Image Deployment.
Architecture	This list box indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. Select the 64 Bit option for the 64-bit Windows 2008 WIM image deployment.
Supported BIOS Type	

Parameter	Description
	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Target Drive	Select from this list box the drive letter on which the operating system is to be installed, in our example we will use the C drive, therefore select C from this list box.

6. Click **Next** to go to the following wizard page.
7. The option to create a new image (**Create a new OS image or setup**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the parameters of the new image.
8. In the **Image Parameters** window define the following parameters:

Parameter	Description
Name	Enter a descriptive name for the image in the Name text box, for example Windows 2008 (64 bit) WIM Image Deployment.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Location	Enter into this text box network path to the folder, where you stored the image file that we created in our previous example including the name of the image, for example, \\192.168.196.13\Build\Windows2008-64bit.wim. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager and the target devices, that is, it is therefore recommended to put it on a device within the subnet.

Connection Parameters	Enter the login and password to be used by the deploying device to access the network location in read and write mode.
	a. To enter the login information click **Edit** to the right. The **Properties** window appears.
	b. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation. The login name must have one of the following formats:
	`<domain name>\<user logon>`
	`<local host name>\<user logon>`
	Be aware that `.` is not a valid domain in this case.
	c. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
	d. To confirm the credentials click **OK** at the bottom of the window. The account will be added in the wizard window boxes.

After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** `Done` , the wizard cannot continue.

9. To verify click **Check Image** to the right of the **Status** box.
   CM will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status** `Done` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.

10. After the **Status** Done is returned click **Next** to go to the following wizard page.
11. *(Optional)* In the **OS Drivers** select the necessary operating system drivers and click **Next** .
12. *(Optional)* In the **OS Drivers**) select the necessary drivers by model and click **Next** .
13. The option to create a new target list (**Create a new target list**) is selected by default, therefore click **Next** to go directly to the following wizard page to define the members of the new target list.
14. This deployment will only have one target device and we will add it as a new target. For this select **Create Target** on top of the empty list box.
    The **Create a New Target** window appears with its three tabs, **General Information** , **Parameters** and **Unattended Information** .
15. Enter the following information into the respective text boxes of the **General Information** tab for the new device:

Parameter	Description
Name	Enter into this text box the short name that the new device is to have, for example, scotty. Be aware that the name of the new target can only have a maximum of 15 characters and can only contain the following characters: A-Z, a-z, 0-9, the underscore (_) and a dash .
Target	Leave the radio button selected as we are defining a single target and enter the information for at least one of the three following text boxes. If the device is already up and running the wizard will recover information about the MAC address, based on the provided IP address or DNS name.
MAC Address	Enter into this text box the current MAC address of the target device. This is the most precise information to identify the device and should be preferred to the other two following identification options. The MAC address can be entered in one of the following formats: xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
IP Address	Enter into this text box the current IP address of the target device in its dotted notation. This option can be used if the MAC address is unknown and device is already running. In this case the respective target device will try to find its MAC address and provide this information.
DNS	Enter into this text box the current DNS information of the target device. This option can be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device will try to find its IP address which in turn will then search for the MAC address and provide this information.

16. Click **Next** to continue.
17. *(Optional)* In the **MBR Disk Configuration** select the desired disk configuration for legacy installations and click **Next** .
18. *(Optional)* In the **GPT Disk Configuration**) select the desired disk configuration for UEFI installations and click **Next** .
19. In the list of available disk configurations select the **Disk with two partitions** option.

> This configuration will create two partitions on the hard disk, the first, the boot or active partition with 30 GB and the second with the remaining space.

20. Click **Next** to go to the following wizard page.

21. In the **Deployment Drivers** window mark the check boxes for all required WinPE drivers, that is, at least one network and possibly a SATA driver.
22. Click **Next** to continue.
23. In the **PXE Menu Parameters** window check the **Add the project to the PXE start menu** box.
24. Enter the item name under which the current project will appear in the menu, for example, *Windows 2008 (64 bit) WIM Image Deployment -Dell GX280* .
25. Select the menu to which to add it from the following list, in our case this will be the *Test Menu* menu, because it is already defined and its range includes our test device.
26. Click **Next** to continue.
27. As we want to activate and execute this deployment right away leave all values as they are and click **Finish** to launch the deployment.

The project will now be build, that is, all parameters are verified, the files are copied to the location required for the remote installation, and so on You can follow the progress of the project in its console node, because the focus of the console will automatically be moved to this object when the wizard is finished. In this view you can follow the different stages of the build. If any other than the final status `Build completed successfully.` displays the build failed and you need to review the parameters of the project and maybe the source files.

After the build is successfully completed the files are put at the required location on the OSD Manager for deployment. To now start the actual operating system deployment to the target device you must switch on the device. It will boot on the PXE boot section and the operating system installation is executed.

> **Note:**
>
> Do not start the target devices before the project is finished and ready to launch the installation. If the target devices are already running before the PXE boot will not find the files for the installation and the deployment and installation of the new OS on the target devices will not take place.

You can follow the progress of the image installation process by selecting the **Assigned Objects > Target List > Your Target List** node in the left window pane. The right pane displays the target list member with its status information.

Creating a USB device to deploy operating systems

The following example creates a completely self-sufficient USB device to deploy a WIM image on UEFI devices on the OSD Manager device. In this case self-sufficient means that the target device does not require an Internet connection for the deployment.

You need to have a WIM image for UEFI deployment ready and built to run this example.

Note

- A bootable USB device can only be created on the OSD Manager and the USB device must be physically connected to the OSD Manager device.
- Make sure your USB device is large enough to contain all the project data in addition to the WinPE if you create a USB device for offline mode. The estimated size is displayed in this view in the Total estimated size on the USB device: box.
- Any data that are stored on the selected USB device are irrevocably deleted before the bootable USB device is created.

1. Plug the USB device into the OSD Manager device.
2. Select the **USB Device** tab of the **OS Deployment > Your OSD Manager > Projects > Your Project Type > Your Project** node in the right window pane.
3. Select the **Offline Mode** radio button.
   The value of the Total estimated size on the USB device: below is updated to the estimated size that must be available on the USB device. This value represents the size of the project plus the connected image and the WinPE.
4. Select the drive into which you connected the USB device from the **Selected drive for USB device list**.

   This list only shows the drives on which a USB device is connected. It displays the drive letter together with the total size of the connected USB device. Be aware, that this is not the currently available space of the device, as the contents of it are erased before the USB device is created.

5. Leave the **NTFS** radio button selected.
6. Select the answer file from the **Which answer file would you like to use?** list. Leave the **Automatic** value, if you want the USB device to use the automatic mode.
7. Click **Start** to create the USB device.
   The USB device is cleaned of all existing data and the selected data are copied to the USB device. You can follow the progress of the USB creation in the progress bar at the bottom of the tab. Once the USB device is ready, you can plug it into the new device to deploy to and the USB device automatically launches the deployment process.

Managing OSD Managers

All operations about any deployments are directly done on the OSD Manager. It creates operating system images for deployment to individual devices or groups of devices, called targets or target lists.

The OSD Manager is responsible for creating the deployment projects for all targets in your environment and dispatching them to the respective image repositories and network boot listeners. It executes also the function of image repository and can be a network boot listener in addition.

The OSD Manager node has the following tabs:

- **Dashboard**
- **Members**
- **Graph**
- **USB Device**
- **Storage**

The OSD Manager node has the following subnodes:

- **Configuration**
- **Drivers**
- **Images**
- **Disk Configurations**
- **Target Lists**
- **Projects**
- **PXE Menus**
- **Multicast Sessions**
- One node for each defined **Image Repository**
- One node for each defined **Network Boot Listener**

The following topics provide more information about managing OSD managers:

- Adding and configuring the OSD Manager
- Operations on the OSD Manager
- OSD Manager Dashboard
- OSD Manager Members
- OSD Topology Graph
- Creating a self-sufficient USB device for OS deployment
- OSD Manager Storage

Adding and configuring the OSD Manager

The following topics provide more information about adding and configuring the OSD manager:

- Adding the OSD Manager
- Configuring a Device as OSD Manager under the OS Deployment Node
- Configuring a device as OSD Manager in the device's properties
- Configuring the OSD Manager

Adding the OSD Manager

The first step for any type of operating system deployment is the selection and configuration of the OSD Manager.

To add the OSD Manager you have two different possibilities:

- Add the OSD Manager under the main **OS Deployment** node
- Assign a device the OSD Manager role via the device's properties, either in the **Device Topology** or under the **Device Groups** node

Configuring a Device as OSD Manager under the OS Deployment Node

1. Select **OS Deployment** in the left window pane.
2. Select **Edit > Add Device**
   The **Add a new OSD Manager** pop-up menu appears displaying the list of all devices that can be OSD Managers due to their operating system.
3. Select the future OSD Manager from one of the list boxes.
4. Click **OK** to confirm and close the window.

The device is added to the table of **OSD Manager** and its configuration parameter is updated.

Configuring a device as OSD Manager in the device's properties

1. Select **Device Groups > Your Device Group > Your Device** or **Device Topology > Your Device** in the left window pane.
2. Click **Edit > Properties** .
   The **Properties** pop-up menu appears.
3. Check the **OSD Manager** box.

   > For devices, which do not have the required operating system, this option is not accessible.

4. Click **OK** to confirm and close the window.

The device is added to the table of **OSD Manager** and its configuration parameter is updated.

Configuring the OSD Manager

When configuring the OSD Manager, two or three different parts must be configured, depending on its assigned roles:

- The specific OSD Manager parameters
- The parameters for the image repository role
- If it is also assigned the network boot agent role, the parameters for the network boot agent

1. Go to the **OS Deployment> Your OSD Manager> Configuration** node in the left window pane.
2. Click **Properties** .
   The **Properties** window appears.
3. Define the following parameters for the OSD Manager role:

Parameter	Description
Windows ADK Path	Enter into this text box the path to the Windows ADK. If you do not enter any value, the default installation path is used. To directly select the path click **Select** next to the text box. A pop-up menu appears with the directory structure of the device where you can directly select the installation directory. Click **OK** to confirm and close the window.
Windows ADK Status	To test if the Windows ADK (WADK) is correctly installed, click Test next to the box. The agent verifies the WADK installation and updates the displayed status accordingly.
TFTP Local Path	Enter into this text box the local path to the shared TFTP server directory. To directly select the path click Select next to the text box. A pop-up menu appears with the directory structure of the device where you can directly select the path. Click **OK** to confirm and close the window.
Driver Root Folder	This text box contains the complete path to the directory where the drivers are copied to for later use. The default directory for this is `<InstallDir>/Master/data/OSDeployment/drivers/`. Do not modify this value, if you are following a standard deployment. To directly select the path click **Select** next to the text box. A pop-up menu appears with the directory structure of the device where you can directly select a different directory. Click **OK** to confirm and close the window.
Status	This field displays the overall progress of the WinPE initialization process which generates files based on the images of the WIM Windows ADK. These files are then used as the base for any OSD project in the BMC Client Management - Software Distribution. Here you can see the advancement of the initialization in percent values and any error messages should errors occur. Be aware, that this process might take several minutes to complete. During this process, which is required only once when defining the OSD Manager for the first time, the console can be used for any type of viewing but no writing operations. To start the process click **Check Environment**.

> The definition of the OSD Manager cannot be completed until the environment check completes without errors and the **Status** shows `OK - Initialization Complete` .

4. To verify click **Check Environment** to the right of the **Status** box.
   CM now verifies all entries of this page, that is, the directories and the access rights to them and the DHCP server address, if it is installed on another device. If all values are correct, the **Status**`OK` is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
5. Click the double arrow in the **Image Repository** line.
   For the image repository you need to define the following parameter:

Parameter	Description
Storage Path	

Parameter	Description
	Enter into this text box the relative path for the storage location for all necessary OSD data. The path is relative to the agent installation directory. Click **Browse** to select the path in the storage path selection window. Click **OK** to confirm and close the window. If this field is left empty, the default path (../data /OsDeployment/streams) is used.

6. If the OSD Manager is also a network boot listener, click the double arrow in the **Network Boot Listener** line to define the parameters of this role as well:

Parameter	Description
Internal DHCP	Check this box if you want to use the DHCP gateway of the OSD module instead of specifically configuring your own DHCP server. In this case a DHCP gateway is installed that is redirecting the computers to the OSD manager and get installed, instead of adding the necessary options to your existing DHCP server.If you do not use this option make sure you have a DHCP server on a different machine that is configured as explained in the configuration options of the Prerequisites topic, preferably with the 066/067 options. If you clear this box, the following two boxes become available.
DHCP Server Address	Enter the IP address or DNS name of the DHCP server which redirects the PXE requests to the local TFTP server. The DHCP server must have the protocol BOOTP activated.This option is only available, if the internal DHCP gateway is not used.
Skip DHCP Check	If the DHCP server is installed on the same device as the OSD Manager device, you must check this text box, because the DHCP server cannot be verified in this case. This test verifies, if the BOOTP protocol is activated on the DHCP server.This option is only available, if the internal DHCP gateway is not used.
Unicast Server Port (TCP)	This parameter determines on which port the unicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the unicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in TCP, typically 1613. Only modify this default value, if absolutely necessary.
Multicast Server Port (UDP)	This parameter determines on which port the multicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the multicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in UDP, typically 1610. Only modify this default value, if absolutely necessary.
Interfaces	For the Interfaces you need to define on which local interfaces the agent is to listen. You have the following options: • **All Interfaces:** Check this radio button, to listen on all local network interfaces. • **Custom Interfaces:** Check this radio button, to only listen on some local network interfaces. The box below displays the list of available interfaces. Check the boxes of all interfaces to listen to.

7. Click **OK** to finalize the OSD Manager definition.

> **Note:**
>
> Be aware that the first initialization might take several minutes.

Operations on the OSD Manager

You can execute the following operations on the OSD Manager:

- Changing the OSD role
- Adding image repositories and network boot listeners
- Removing an OSD Manager

Changing the OSD role

Changing the OSD role means that an existing OSD agent is either taking on another role or giving up one of its assigned roles, that is, being an image repository or network boot listener or both. You can assign the OSD Manager the additional role of network boot listener, but you cannot remove its image repository role, which it is assigned by default.

> **Note:**
>
> An image repository can only be modified to a network boot listener if it has no children.

1. Select **Edit > Change OSD Role** .
2. In the **Change the OSD Role** window either clear the role to remove or check the box for the role to add to the current OSD agent.
3. Click **OK** .

The roles of the OSD agent are updated immediately.

Adding image repositories and network boot listeners

Any device with any supported operating system in Client Management can be an image repository or network boot listeners or both. When a device is added to one or both of these roles, the OSD module is loaded on the device and it also becomes an *OSD agent* .

> **Note:**
>
> Be aware, that the selected device must be online at the time of selection. When the selection is confirmed, the master agent accesses the newly defined OSD agent via direct access to load the OSD module and to configure it. If the device is not reachable, an error occurs and the new role is not assigned.

1. Select **Edit > Add Image Repository/Network Boot Listener** .
2. Select the agent you want for the new role in the **Add an Image Repository or a Network Boot Listener** window.
3. *(Optional)* If the new role for the agent is to be an image repository, select the **Image Repository** box.

4. *(Optional)* If the agent is not to be a network boot listener, clear the **Network Boot Listener** box.
5. Click **OK**.

The OSD agent is added to the list of children with the defined roles.

Removing an OSD Manager

When you are removing an OSD Manager, you are only removing this role from the device, not deleting the device from the database.

> **Note:**
>
> All OSD related data stored on the image repository to be removed is deleted, no further deployments can be done from this device.
> OSD Managers that have children cannot be removed.
> Removing an OSD Manager might take a few moments, as the complete cache needs to be flushed and the console could block during this operation.

1. Select the **OS Deployment** node.
2. Select the OSD Manager to remove in the list.
3. Select **Edit > Remove OSD Manager** .

The selected OSD Manager is removed, and all its objects and other OSD related data are purged.

OSD Manager Dashboard

The **Dashboard** provides an overview over all projects that are connected to this **OSD Manager**. It provides the following information:

- Project Breakdown by Type (Active/Total)
- Image type used by active projects
- Project Information

Project Breakdown by Type (Active/Total)

The values in the left upper part of the view display the list of possible types of deployment and how many of each exist and are active on this **OSD Manager**.

Parameter	Description
Deployment by Installation	The number of deployments by installation that are currently active and how many exist in total, active and inactive.
Deployment by WIM Image	The number of deployments by WIM image that are currently active and how many exist in total, active and inactive.
Customized Deployment	The number of customized deployments that are currently active and how many exist in total, active and inactive.

Parameter	Description
Capture by WIM Image	The number of captures by WIM image that are currently active and how many exist in total, active and inactive.

Image type used by active projects

This pie chart displays the information of the following Project Information table in graphical format.

Project Information

This table displays the breakdown of image types by active projects.

Parameter	Description
Name	The name of the project.
Type	The type of deployment of the project.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Operating System	The operating system the project is to install.
Active Target Count	The number of targets assigned to the project that are currently active.
Target Count	The total number of targets that are assigned to the project.
Subnet Mask	The subnet that is assigned to this project. If the targets are assigned otherwise to the project this field remains empty.

OSD Manager Members

The **Members** provides the list of all image repositories and network boot listeners in your network. It provides the following information:

Parameter	Description
Name	The network name of the device.
OSD Role	The OSD role of the device, that is, if it is only an image repository or a network boot listener, or both.
IP Address	The IP address of the device.
Operating System	The name of the operating system, as discovered by the agent, for example, **Debian Linux 64-bit** .

Operations on OSD Manager members

You can execute the following operations on the members of an OSD agent:

- Adding image repositories and network boot listeners
- Removing OSD agents
- Changing the OSD role
- Changing the image respository

Adding image repositories and network boot listeners

Any device with any supported operating system in Client Management can be an image repository or network boot listeners or both. When a device is added to one or both of these roles, the OSD module is loaded on the device and it also becomes an *OSD agent*.

> **Note:**
>
> Be aware, that the selected device must be online at the time of selection. When the selection is confirmed, the master agent accesses the newly defined OSD agent via direct access to load the OSD module and to configure it. If the device is not reachable, an error occurs and the new role is not assigned.

1. Select **Edit > Add Image Repository/Network Boot Listener** .
2. Select the agent you want for the new role in the **Add an Image Repository or a Network Boot Listener** window.
3. *(Optional)* If the new role for the agent is to be an image repository, select the **Image Repository** box.
4. *(Optional)* If the agent is not to be a network boot listener, clear the **Network Boot Listener** box.
5. Click **OK** .

The OSD agent is added to the list of children with the defined roles.

Removing OSD agents

When you are removing an OSD agent, either an image repository or a network boot listener, you are only removing this role from the device, not deleting the device from the database.

> **Note:**
>
> Removing image repositories:
>
> All OSD related data stored on the image repository to be removed is deleted, no further deployments can be done from this device.
> Image repositories that have children cannot be removed.
> If you are removing an image repository this might take a few moments, as the complete cache needs to be flushed and the console could block during this operation.

1. Select the **Members** tab of the **OS Deployment > Your OSD Manager** node.
2. Select the OSD agents to remove in the list.
3. Select **Edit > Remove OSD Roles** .
   A **Confirmation** window appears.
4. Click **Yes** .

The selected OSD nodes are removed, their storage cache is emptied and all OSD related data purged.

Changing the OSD role

Changing the OSD role means, that an existing OSD agent is either taking on another role or giving up one of its assigned roles, that is, being an image repository or network boot listener or both. You can assign the OSD Manager the additional role of network boot listener, but you cannot remove its image repository role, which it is assigned by default.

> **Note:**
>
> An image repository can only be modified to a network boot listener if it has no children.

1. Select **Edit > Change OSD Role** .
2. In the **Change the OSD Role** window either clear the role to remove or check the box for the role to add to the current OSD agent.
3. Click **OK** .

The roles of the OSD agent are updated immediately.

Changing the image respository

Changing the image repository means, that you are changing the parent of the currently selected OSD agent.

1. Select **Edit > Change Image Repository** .
2. From the list in the window select the image repository you want to move your OSD agent to.
3. Click **OK** .

The selected OSD agent is moved immediately under the new parent.

OSD Topology Graph

The **Graph** provides a graphical overview over the hierarchical structure of all devices with an OSD role. The root node is the OSD Manager with its first level of image repositories and network boot listeners below. All network boot listeners are a final node without children. Image repositories can have one or several more levels of children. For more information on the graph tab and its possibilities, see The Graph tab .

Creating a self-sufficient USB device for OS deployment

Client Management allows you to create a self-sufficient USB device for operating system deployment. It provides you with the following two modes for this:

- **Offline Mode**
  This mode assumes that the target device does not have an Internet connection and no possible way to contact the OSD Manager. It stores all data that is necessary for a successful deployment, that is, the WinPE and the complete project data, setup or WIM image (including sysprep).
  Should the target device have access to a network and a network boot listener can be found by the device, the OS installation first tries to see if more recent data are available via the network before using the data stored on the USB device. If yes, the new data is downloaded and the installation effected with the most recent data, if not the installation is launched using the project data stored on the device.
- **Online Mode**
  This mode assumes that the target device does have an Internet connection and a connection with the OSD Manager. The data required to launch the deployment are stored on the USB device, and all other, further required data, such as the actual image to be installed, are then downloaded from the OSD Manager.

The default file system for the USB key to create is NTFS. However, specific tablets, such as Surface 2, and possibly other older UEFI hardware, cannot boot on an NTFS partition. The OSD functionality therefore provides you with both choices when creating the USB device:

- **NTFS**
  Most more recent device allow booting from an NTFS partition. This has the advantage that the full disk space of a USB device larger than 32 GB can be used and WIM images can also be stored on the device. Before selecting this option, make sure your targets support booting from NTFS.
- **FAT32**
  The FAT32 file system allows to boot every device, but it has a number of limitations and should therefore only be used if absolutely necessary; either when creating a USB device for offline mode, or when creating a USB device for on-line mode. The FAT32 system is limited 32 GB partitions and a maximum file size of 4 GB. The base image for a WIM image is approximately 3.5 GB for Windows 8.1 update 1, and easily passes the 4 GB size limit if the system was customized with large software, such as Microsoft Office, before the capture.

A USB device can be created on OSD Manager level or at project level, however, the USB device must be connected physically to the OSD Manager for both cases.

This section includes:

Creating a USB device on the OSD Manager

Note:

A bootable USB device can only be created on the OSD Manager and the USB device must be physically connected to the OSD Manager device.
Make sure your USB device is large enough to contain all the project data in addition to the WinPE if you create a USB device for offline mode. The estimated size is displayed in this view in the **Total estimated size on the USB device:** box.
Any data that are stored on the selected USB device are irrevocably deleted before the bootable USB device is created.

1. Plug the USB device into the OSD Manager device.
2. Select the **USB Device** tab of the **OS Deployment> Your OSD Manager** node in the right window pane.
3. Select if you want to create an online or offline device by clicking the respective radio button.
4. Select the project to copy for the USB device from the **Which project would you like to use?** list.
   The value of the **Total estimated size on the USB device:** below is now updated to show the estimated size that must be available on the USB device. This value represents the size of the project plus the connected image and the WinPE.
5. Select the drive into which you connected the USB device from the **Which drive would you like to use?** list.

   This list only shows the drives on which a USB device is connected. It displays the drive letter together with the total size of the connected USB device. Be aware, that this is not the currently available space of the device, as the contents of it are erased before the USB device is created.

6. If your target does only boot from a FAT32 partition, select the **FAT32** radio button.
7. Select the answer file from the **Which answer file would you like to use?** list. Leave the **Automatic** value, if you want the USB device to use the automatic mode.
8. Click **Start** to create the USB device.

The USB device is cleaned of all existing data and the selected data are copied to the USB device. You can follow the progress of the USB creation in the progress bar at the bottom of the tab.

OSD Manager Storage

The **Storage** tab represents the image repository role of the OSD Manager. Same as for all other image repositories it is divided into the following parts:

- The top part provides information on the disk space of the OSD Manager.
- The four buttons provide specific operations that are executed on all the available data on selected image repositories.
- The bottom part displays the list of all available OSD objects.

Disk space information

The disk space information is provided by several different parameters as well as a pie chart that displays the overall situation on the disk.

Parameter	Description
Local Path	Displays the full path to the location where the OSD data are stored.
Used Space by OSD	The size in GB, that all stored OSD data currently use on the disk.
Used Space (without OSD)	The amount of disk space in GB that is used otherwise, that is, for all other data, apart from OSD.
Available Space	The amount of disk space in GB that is currently available on the disk.

Available OSD objects

This part displays the list of OSD objects on the device. On the OSD Manager, only one version of a specific object is ever available.

> **Note:**
>
> The content of this view cannot be managed in it. Whenever a new object is created, it is automatically added to the cache of the image repository on the OSD Manager, and it appears in this list. To remove an object from this list, you must delete it from its location on the OSD Manager, that is, a project must be deleted under the **Projects** node, an image under the **Images** node, and so on.

Parameter	Description
Name	This column displays the hierarchy and the name of the respective OSD object. Click the arrow to the left to open or close the hierarchy on every level.
Status	This column provides the synchronization status of the projects between the image repository and the OSD Manager. The possible values are: • `Synchronized`  The object size equals the cache size. • `Not Synchronized`  The cache size is 0. • `Synchronizing`  The cache size does not yet equal the object size, but the download is still progressing. • `Synchronization failed`  The cache size is larger than 0 but does not match the object size and no download is in progress.
Size	The total size of the stream in MB on the OSD Manager.

Parameter	Description
Cache Size	The size in MB of the object in the local cache of the OSD agent, once it is synchronized. On the master this is always 0 MB.
Create Time	The date and time at which the object was originally created or the project was last built after modifications.

This section includes:

- Operations on all objects of the image repository storage of the OSD Manager
- Operations on specific objects of the image repository storage of the OSD Manager

Operations on all objects of the image repository storage of the OSD Manager

You can execute the following image repository storage operations on the OSD Manager:

- Synchronizing all OSD objects on specific image repositories
- Stopping the synchronization of all OSD objects on specific image repositories
- Exporting all OSD objects from the OSD Manager
- Completely clearing the cache of selected image repositories

Synchronizing all OSD objects on specific image repositories

This operation allows the administrator to synchronize all OSD objects that are defined on the OSD Manager immediately for selected image repositories.

This can be very useful in situations, for example, where complete departments were equipped with new computers and these need to be installed over a weekend.

1. Click the **Synchronize** button in the top panel of the **Storage** tab.
2. In the appearing **Select Image Repositories** window select the image repositories to synchronize.
3. Click **OK** .
   The **Operation Status** window appears, displaying the list of all selected image repositories and the synchronization status of the selected objects on each.

   > **Note:**
   >
   > Be aware, that this status only shows, if the synchronization order was sent to the respective target, it does not indicate that the target received the order or that the objects were synchronized on it.

4. Click **Close** to close the window.

The order to synchronize the objects on the image repositories is launched. To verify if the image repositories are synchronized, you must check the **Storage** tab of each target.

Stopping the synchronization of all OSD objects on specific image repositories

This operation stops all currently running synchronizations on specific image repositories. The already transferred data remains in the cache on the image repositories, and the next time a target requests the data, the image repository starts downloading again. The remaining data, not downloaded during the aborted synchronization, is downloaded into the cache of the repository.

> **Note:**
>
> If a deployment of a project is currently in progress on a target, when the synchronization is aborted, the deployment fails.

1. Click the **Stop Synchronization** button in the top panel of the **Storage** tab.
2. In the appearing **Select Image Repositories** window, select the image repositories on which to stop the synchronization.
3. Click **OK** .

All synchronizations are stopped on the selected image repositories. On the image repositories, the cache size is updated to the amount already downloaded.

Exporting all OSD objects from the OSD Manager

This menu item allows you to export the complete cache of all OSD objects defined on the OSD Manager to a USB storage medium and then import it on an image repository. This might be a useful operation, if your network is very slow and the data to transfer is very large.

> **Note:**
>
> Existing content on the USB medium is irrevocably deleted before exporting the cache.

1. Click the **Export Cache** button in the top panel of the **Storage** tab.
2. In the appearing **Export Cache** window select the drive to which the USB medium is connected.
3. Click **OK** .
4. In the appearing **Confirmation** appears, click **Yes** to continue.

Any data that are currently stored on the USB medium is deleted and then all OSD objects are copied to it. When the copy operation is completed, the USB medium is ready to be transported and connected to an image repository for import.

Completely clearing the cache of selected image repositories

This operation completely clears the cache on selected image repositories, that is, it removes all downloaded and stored OSD data on these devices. This operation is irreversible and all deleted data are irrevocably lost. You should therefore use this operation with caution.

> **Note:**
>
> This might take a few moments and the console could block during this operation.

1. Click the **Clear Cache** button in the top panel of the **Storage** tab.
2. In the appearing **Select Image Repositories** window select the image repositories on which you want to completely clear the cache.
3. Click **OK** .
4. Click **Yes** in the appearing **Confirmation** window.

The OSD cache of the selected image repositories is completely emptied and all data are deleted.

Operations on specific objects of the image repository storage of the OSD Manager

You can execute the following image repository storage operations on the OSD Manager:

- Clearing specific OSD objects from the cache on selected image repositories
- Synchronizing specific OSD objects on image repositories
- Stopping the synchronization of specific OSD objects on image repositories
- Exporting specific OSD objects from the OSD Manager
- Importing OSD objects on image repositories

Clearing specific OSD objects from the cache on selected image repositories

This operation allows you to clear specific OSD objects from the cache on selected image repositories.

> **Note:**
>
> This might take a few moments and the console could block during this operation.

1. Select the OSD objects to clear in the right window pane.
2. Select **Edit > Clear Cache** .
3. In the appearing **Select Image Repositories** window select the image repositories on which you want to clear the selected objects from the cache.
4. Click **OK**.
5. Click **Yes** in the appearing **Confirmation** window.

The cache of the selected OSD objects is cleared and all their data are deleted.

Synchronizing specific OSD objects on image repositories

This operation allows the administrator to synchronize specific OSD objects immediately for selected image repositories.

This can be very useful when an operating system is to be deployed time critically, such as, starting the operation on Friday evening before you leave the office to make sure by Monday morning everything is in place.

1. Select the objects to synchronize in the right pane.
2. Click the **Synchronize** button in the top panel of the **Storage** tab.
3. In the appearing **Select Image Repositories** window select the image repositories to synchronize.
4. Click **OK**.
   The **Operation Status** window appears, displaying the list of all selected image repositories and the synchronization status of the selected objects on each.

   > **Note:**
   >
   > Be aware, that this status only shows, if the synchronization order was sent to the respective target, it does not indicate that the target received the order or that the objects were synchronized on it.

5. Click **Close** to close the window.

The order to synchronize the selected objects on the image repositories is launched. To verify if the image repositories are synchronized, you must check the **Storage** tab of each target.

Stopping the synchronization of specific OSD objects on image repositories

This operation stops specific OSD object synchronizations on selected image repositories. The already transferred data remains in the cache on the image repositories, and the next time a target requests the data, the image repository starts downloading again. The remaining data, not downloaded during the aborted synchronization, is downloaded into the cache of the repository.

1. Select the objects whose synchronizations you want to stop in the right pane.
2. Click **Edit > Stop Synchronization** .
3. In the appearing **Select Image Repositories** window select the image repositories on which to stop the synchronizations.
4. Click **OK.**

The selected synchronizations are stopped on the selected image repositories. On the image repositories, the cache size is updated to the amount already downloaded.

Exporting specific OSD objects from the OSD Manager

This menu item allows you to export specific OSD objects from the OSD Manager to a USB storage medium and then import it on an image repository. This might be a useful operation, if your network is very slow and the data to transfer is very large.

Note:

Existing content on the USB storage medium is irrevocably deleted before exporting the cache.

1. Select the objects to export in the right bottom window pane.
2. Click **Edit > Export Cache** .
3. In the appearing **Export Cache** window select the drive of the USB medium.
4. Click **OK**.
5. In the appearing **Confirmation** appears, click **Yes** to continue.

Any data that is currently stored on the USB medium is deleted and then the selected OSD objects are copied to it. When the copy operation is completed, the USB medium is ready to be transported and connected to an image repository for import.

Importing OSD objects on image repositories

This menu item allows you to import OSD objects from a USB storage medium exported from another image repository or the OSD Manager.

This might be a useful operation, if your network is very slow and the data to transfer is very large.

1. Select **Edit > Import Cache** .
2. In the appearing **Import Cache** window select the drive to which you have connected the USB medium.
3. Click **OK**.
   A result window appears to inform you of the success or failure of the import.

Managing Image Repository

The image repository is the bridge between the OSD Manager and the deployment target. Contrary to the OSD Manager it is platform independent and thus can be any device with a CM agent . It does not build any deployment projects, it stores projects it is assigned by the OSD Manager, thus it requires a large amount of hard disk space to store the cached data. The image repository communicates very regularly with the OSD Manager to ensure its cached files are still valid.

In a perfect architecture you would have one image repository per physical site, which would then have one network boot listener per subnet as children. An image repository can be a network boot listener at the same time, but it can only have another image repository or the OSD Manager as a parent. It can have other image repositories and network boot listeners as children.

An image repository has the following tabs and subnodes:

- **Members**
- **Storage**
- **Configuration**

- One node for each defined **Image Repository**
- One node for each defined **Network Boot Listener**

Sizing requirements

The image repository needs to store the project data, which tend to be quite large. You need to preview the following storage space on the hard disk of the image repository:

- size of the image file
- each project, activated or not, takes approximately an additional 250MB without drivers
- size of the attached drivers

This section includes:

- Managing image repository members
- Managing image repository storage
- Managing image repository configuration

Managing image repository members

The **Members** provides the list of all image repositories in your network. It provides the following information:

Parameter	Description
Name	The network name of the device.
OSD Role	The OSD role of the device, that is, if it is only an image repository or as well a network boot listener.
IP Address	The IP address of the device.
Operating System	The name of the operating system, as discovered by the agent, for example, **Debian Linux 64-bit** .

Operations on image repository members

You can execute the following operations on the members of an OSD agent:

- Adding image repositories and network boot listeners
- Removing OSD agents
- Changing the OSD role
- Changing the image repository

Adding image repositories and network boot listeners

Any device with any supported operating system in Client Management can be an image repository or network boot listeners or both. When a device is added to one or both of these roles, the OSD module is loaded on the device and it also becomes an *OSD agent* .

> **Note:**

Be aware, that the selected device must be online at the time of selection. When the selection is confirmed, the master agent accesses the newly defined OSD agent via direct access to load the OSD module and to configure it. If the device is not reachable, an error occurs and the new role is not assigned.

1. Select **Edit > Add Image Repository/Network Boot Listener** .
2. Select the agent you want for the new role in the **Add an Image Repository or a Network Boot Listener** window.
3. *(Optional)* If the new role for the agent is to be an image repository, select the **Image Repository** box.
4. *(Optional)* If the agent is not to be a network boot listener, clear the **Network Boot Listener** box.
5. Click **OK** .

The OSD agent is added to the list of children with the defined roles.

Removing OSD agents

When you are removing an OSD agent, either an image repository or a network boot listener, you are only removing this role from the device, not deleting the device from the database.

Note:

Removing image repositories:

All OSD related data stored on the image repository to be removed is deleted, no further deployments can be done from this device.
Image repositories that have children cannot be removed.
If you are removing an image repository this might take a few moments, as the complete cache needs to be flushed and the console could block during this operation.

1. Select the **Members** tab of the **OS Deployment > Your OSD Manager** node.
2. Select the OSD agents to remove in the list.
3. Select **Edit > Remove OSD Roles** .
   A **Confirmation** window appears.
4. Click **Yes**.

The selected OSD nodes are removed, their storage cache is emptied and all OSD related data purged.

Changing the OSD role

Changing the OSD role means, that an existing OSD agent is either taking on another role or giving up one of its assigned roles, that is, being an image repository or network boot listener or both. You can assign the OSD Manager the additional role of network boot listener, but you cannot remove its image repository role, which it is assigned by default.

> **Note:**
>
> An image repository can only be modified to a network boot listener if it has no children.

1. Select **Edit > Change OSD Role** .
2. In the **Change the OSD Role** window either clear the role to remove or check the box for the role to add to the current OSD agent.
3. Click **OK** .

The roles of the OSD agent are updated immediately.

Changing the image repository

Changing the image repository means, that you are changing the parent of the currently selected OSD agent.

1. Select **Edit > Change Image Repository** .
2. From the list in the window select the image repository you want to move your OSD agent to.
3. Click **OK**.

The selected OSD agent is moved immediately under the new parent.

Managing image repository storage

The **Storage** is divided into two parts:

- The top part provides information on the disk space of the selected OSD agent.
- The bottom part displays the list of OSD streams, that is, images, projects and drivers, available on the OSD manager and their status on the image repository.

Disk space information

The disk space information is provided by several different parameters as well as a pie chart that displays the overall situation of the disk.

Parameter	Description
Local Path	Displays the full path to the location where the OSD data are stored.
Used Space by OSD	The size in GB, that all stored OSD data currently use on the disk.

Parameter	Description
Used Space (without OSD)	The amount of disk space in GB that is used otherwise, that is, for all other data, apart from OSD.
Available Space	The amount of disk space in GB that is currently available on the disk.

OSD objects in the image repository cache

This part displays the list of OSD streams, that is the images, projects and drivers, available on the master and their status on the OSD agent. Each of these object streams can have more than one version and several deltas. The table displays the following information for each:

Parameter	Description
Name	This column displays the hierarchy and the name of the respective OSD object. Click the arrow to the left to open or close the hierarchy on every level.
Status	This column provides the synchronization status of the projects between the image repository and the OSD Manager. The possible values are: • `Synchronized`  The object size equals the cache size. • `Not Synchronized`  The cache size is 0. • `Synchronizing`  The cache size does not yet equal the object size, but the download is still progressing. • `Synchronization failed`  The cache size is larger than 0 but does not match the object size and no download is in progress.
Size	The total size of the stream in MB on the OSD Manager.
Cache Size	The size in MB of the object in the local cache of the OSD agent, once it is synchronized. On the master this is always 0 MB.
Size to be downloaded	This field shows the size (GB) of what remains to be synchronized. This can be either the full object size, or a partial remaining value, if the synchronization was interrupted.
Create Time	The date and time at which the object was originally created or the project was last built after modifications.

This section includes:

- Operations on all objects of the image repository storage
- Operations on specific objects of the image repository storage

Operations on all objects of the image repository storage

You can execute the following operations on all cached objects of image repositories:

- Synchronizing all OSD objects
- Stopping the synchronization of all OSD objects
- Exporting all OSD objects from image repositories

- Completely clearing the image repository cache

Synchronizing all OSD objects

This operation allows the administrator to synchronize the image repository with all OSD objects that are defined on the OSD Manager immediately.

> **Note:**
>
> The newest version can be downloaded either as a complete new version or as a delta, depending on which is smaller.

1. Click the **Synchronize** button in the top panel of the **Storage** tab.
   The synchronization is launched immediately.

In this window you call follow the progress of the synchronization as the synchronized objects appear one after the other in the right pane, if it is the first synchronization, or as the **Cache Size** for each object is updated.

Stopping the synchronization of all OSD objects

This operation stops all currently running synchronizations on the image repository. The already transferred data remains in the cache, and the next time a target requests the data, the download starts again. The remaining data, not downloaded during the aborted synchronization, is downloaded into the cache of the repository.

> **Note:**
>
> If a deployment of a project is currently in progress on a target, when the synchronization is aborted, the deployment fails.

1. Click the **Stop Synchronization** button in the top panel of the **Storage** tab.
   The synchronization currently in progress is immediately stopped.

In this view you can see which of the objects were already synchronized via their new versions or deltas and in the updated cache size, and for which the synchronization was aborted, due to unchanged values.

Exporting all OSD objects from image repositories

This menu item allows you to export all OSD objects currently stored in the cache of the image repository to a USB storage medium and then import it on another image repository. This might be a useful operation, if your network is very slow and the data to transfer is very large.

> **Note:**

Existing content on the USB medium is irrevocably deleted before exporting the cache.

1. Click the **Export Cache** button in the top panel of the **Storage** tab.
2. In the appearing **Export Cache** window select the drive to which the USB medium is connected.
3. Click **OK** .
4. In the appearing **Confirmation** appears, click **Yes** to continue.

Any data that is currently stored on the USB medium is deleted and then all OSD objects are copied to it. When the copy operation is completed, the USB medium is ready to be transported and connected to another image repository for import.

Completely clearing the image repository cache

This operation completely clears the cache of an image repository. This operation is irreversible and all deleted data are lost. You should therefore use this operation with caution. To recover all or part of the data you need to resynchronize with the OSD Manager image repository. If there are currently deployments running, they fail.

Note:

This might take a few moments and the console could block during this operation.

1. Click the **Clear Cache** button in the top panel of the **Storage** tab.
2. Click **Yes** in the appearing **Confirmation** window.

The OSD cache of the image repository is completely emptied and all data are deleted.

Operations on specific objects of the image repository storage

You can execute the following operations on selected cached objects of image repositories:

- Clearing the cache on an image repository of specific OSD objects
- Synchronizing specific OSD objects
- Stopping the synchronization of specific OSD objects
- Exporting specific OSD objects from image repositories
- Importing OSD objects on image repositories

Clearing the cache on an image repository of specific OSD objects

This operation allows you to clear the cache of specific OSD objects. If there are currently deployments running that are using this data, they fail.

Note:

This might take a few moments and the console could block during this operation.

1. Select the OSD objects to clear in the right window pane.
2. Select **Edit > Clear Cache** .
3. Click **Yes** in the appearing **Confirmation** window.

The cache of the selected OSD objects is cleared and all their data are deleted.

Synchronizing specific OSD objects

This operation allows the administrator to synchronize specific OSD objects immediately with the newest versions available on the OSD Manager.

> **Note:**
>
> The newest version can be downloaded either as a complete new version or as a delta, depending on which is smaller.

1. Select the objects to synchronize in the right pane.
2. Select **Edit > Synchronize** .
   The synchronization is launched immediately.

In this window you call follow the progress of the synchronization as the the **Cache Size** for each object is updated and new versions or deltas are added to the list of cached objects.

Stopping the synchronization of specific OSD objects

This operation stops specific OSD object synchronizations. The already transferred data remains in the cache, and the next time a target requests the data, the image repository starts downloading again. The remaining data, not downloaded during the aborted synchronization, is downloaded into the cache of the repository.

1. Select the objects for which the synchronization is to stop in the right pane.
2. Click **Edit > Stop Synchronization** .

The selected synchronizations are stopped. In this view you can see which of the objects had already terminated their synchronizations via their new versions or deltas and in the updated cache size, and for which the synchronization was aborted, due to unchanged values.

Exporting specific OSD objects from image repositories

This menu item allows you to export specific OSD objects currently stored in the cache of an image repository to a USB storage medium and then import it on another image repository. This might be a useful operation, if your network is very slow and the data to transfer is very large.

> **Note:**

Existing content on the USB storage medium is irrevocably deleted before exporting the cache.

1. Select the objects to export in the right bottom window pane.
2. Select **Edit > Export Cache** .
3. In the appearing **Export Cache** window select the drive of the USB medium.
4. Click **OK** .
5. In the appearing **Confirmation** appears, click **Yes** to continue.

Any data that is currently stored on the USB medium is deleted and then the selected OSD objects are copied to it. When the copy operation is completed, the USB medium is ready to be transported and connected to another image repository for import.

Importing OSD objects on image repositories

This menu item allows you to import OSD objects from a USB storage medium exported from another image repository or the OSD Manager.

This might be a useful operation, if your network is very slow and the data to transfer is very large.

1. Select **Edit > Import Cache** .
2. In the appearing **Import Cache** window select the drive to which you have connected the USB medium.
3. Click **OK** .
   A result window appears to inform you of the success or failure of the import.

Managing image repository configuration

The **Configuration** node allows you to configure specific aspects of the image repository. The following parameters are available:

Parameter	Description
OSD Role	The type of OSD role the device is assigned to. This may be either **Image Repository** , **Network Boot Listener** or **Image Repository and Network Boot Listener** , if the OSD agent executes both roles.
Storage Path	Enter the name of the environment variable for which the value is to be recovered, for example, *CLASSPATH* .
Network Interfaces	Defines on which local interfaces the agent listens. This can be either all interfaces or some specific ones.

This topic includes:

Configuring image repositories

To configure or modify the configuration of an image repository proceed as follows:

1. Select the **Configuration** node of the image repository to modify in the left window pane.

2. Select **Edit > Properties** .
   The **Properties** window appears.
3. Make the desired changes:

Parameter	Description
Storage Path	Enter into this text box the relative path for the storage location for all necessary OSD data. The path is relative to the agent installation directory. Click Browse to select the path in the storage path selection window. Click OK to confirm and close the window. If this field is left empty the default path (../data /OsDeployment/streams) is used.
Automatic Cache Clean-up	To modify the displayed synchronization schedule, click Edit to call the Scheduler window. Make the desired changes to the schedule in this window, then click OK to confirm your modifications.

4. *(Optional)* Click **Create New Test Project** to test your new settings via a test deployment.
5. Click **OK** to confirm the changes and close the window.

Any changes made are saved and applied to the selected image repository.

Configuring Network Boot Listener

The **OS Deployment** node is the central entry point for the deployment of operating systems to the devices within your network. With this functionality you can install completely new devices with an empty hard disk, you can reinstall existing devices with new operating systems or repair existing systems.

A network boot listener node has only Configuration subnode. The following topic guides you through the network boot listener configurations:

- Configuration node of network boot listener
- Configuring or modifying Network Boot Listeners

Configuration node of network boot listener

The **Configuration** node allows you to configure specific aspects of the network boot listener. The following parameters are available:

Parameter	Description
OSD Role	The type of OSD role the device is assigned to. This may be either **Image Repository** , **Network Boot Listener** or **Image Repository and Network Boot Listener** , if the OSD agent executes both roles.
Internal DHCP	Check this box if you want to use the DHCP gateway of the OSD module instead of specifically configuring your own DHCP server. In this case a DHCP gateway is installed that is redirecting the computers to the OSD manager and get installed, instead of adding the necessary options to your existing DHCP server. If you do not use this option make sure you have a DHCP server on a different machine that is configured as explained in the configuration options of the **Prerequisites** topic, preferably with the 066/067 options.
DHCP Server Address	The IP address or DNS name of the DHCP server which redirects the PXE requests to the local TFTP server. The DHCP server must have the protocol BOOTP activated.

Parameter	Description
Skip DHCP Check	If the DHCP server is installed on the same device as the OSD Manager device you must check this box, as the DHCP server cannot be verified in this case. This test verifies if the BOOTP protocol is activated on the DHCP server.
Unicast Server Port (TCP)	This parameter determines on which port the unicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the unicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in TCP, typically 1613.
Multicast Server Port (UDP)	This parameter determines on which port the multicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the multicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in UDP, typically 1610.
Network Interfaces	Defines on which local interfaces the agent listens. This can be either all interfaces or some specific ones.

Configuring or modifying Network Boot Listeners

To configure or modify the configuration of a network boot listener proceed as follows:

1. Select the **Configuration** node of the network boot listener to modify in the left window pane.
2. Select **Edit> Properties** .
   The **Properties** window appears.
3. Make the desired changes in the respective boxes:

Parameter	Description
Internal DHCP	Check this box if you want to use the DHCP gateway of the OSD module instead of specifically configuring your own DHCP server. In this case a DHCP gateway is installed that is redirecting the computers to the OSD manager and get installed, instead of adding the necessary options to your existing DHCP server.If you do not use this option make sure you have a DHCP server on a different machine that is configured as explained in the configuration options of the Prerequisites topic, preferably with the 066/067 options. If you clear this box, the following two boxes become available.
DHCP Server Address	Enter the IP address or DNS name of the DHCP server which redirects the PXE requests to the local TFTP server. The DHCP server must have the protocol BOOTP activated.This option is only available if the internal DHCP gateway is not used.
Skip DHCP Check	If the DHCP server is installed on the same device as the OSD Manager device you must check this text box, because the DHCP server cannot be verified in this case. This test verifies if the BOOTP protocol is activated on the DHCP server.This option is only available if the internal DHCP gateway is not used.
Unicast Server Port (TCP)	This parameter determines on which port the unicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the unicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in TCP, typically 1613. Only modify this default value if absolutely necessary.
Multicast Server Port (UDP)	

Parameter	Description
	This parameter determines on which port the multicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the multicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in UDP, typically 1610. Only modify this default value if absolutely necessary.
Interfaces	For the Interfaces you need to define on which local interfaces the agent is to listen. You have the following options: All Interfaces: Check this radio button to listen on all local network interfaces. Custom Interfaces: CCheck this radio button to only listen on some local network interfaces. The box below displays the list of available interfaces. Check the boxes of all interfaces to listen to.

4. *(Optional)* Click **Create New Test Project** to test your new settings via a test deployment.
5. Click **OK** to confirm the changes and close the window.

Any changes made were saved and applied to the selected network boot listener.

Managing OSD Drivers

The **Drivers** node provides access to all drivers which are defined for the operating system deployment. From this view you can also access the **Driver Tags** . These provide you the possibility to classify your drivers according to your requirements.

The following different types or classes of drivers can be defined:

- **Deployment Drivers**
  Deployment drivers are the drivers that are required by the WinPE for installation
- **OS Drivers**
  Operating system drivers are drivers that may be required by the operating systems for its regular functioning once it is installed on the target devices, such as the keyboard or mouse drivers, video and audio drivers, modem drivers, and so on.
- **Driver Tags**
  Driver tags are used to classify drivers according to their targets to make their selection easier when assigning them to specific projects.
- **Drivers by Model**
  Drivers by model are folders that contain all drivers that are pertinent to a specific hardware model. This should be your preferred driver management method for more recent hardware, but it can also be used for older models.

This section includes following topics:

Deployment Drivers

Deployment drivers are the drivers that are required by the WinPE for installation, that is, network drivers, applicable to the different network cards in your infrastructure and the SATA drivers, if devices in your network have a SATA disk. All these drivers must be Windows 7 compliant drivers, because they are used by the WinPE.

Deployment drivers are limited to network and hard disk drivers as they are absolutely required by WinPE to perform its tasks.

In the tree structure in the left window pane below the **Deployment Drivers** node you can see a subnode for each **Driver Class** for which at least one driver is defined.

OS Drivers

Operating system drivers are drivers that may be required by the operating systems for its regular functioning once it is installed on the target devices, such as the keyboard or mouse drivers, video and audio drivers, modem drivers, and so on.

In the tree structure in the left window pane below the **OS Drivers** node you can see a subnode for each **Driver Class** for which at least one driver is defined.

Managing Driver Families

The nodes for the different driver classes are automatically created when the first driver of the respective type is created. All newly created drivers will automatically be added in their driver class.

The **Driver Family** node provides a list of all existing drivers with the following information:

Column	Description
Name	This column lists the names of all drivers that were created under the main **Drivers** node.
Architecture	This column indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program for which the driver is required. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.
Type	This column identifies the type of the driver, that is, if it is a WinPE driver, or if it is a network or a SATA disk driver, a video or a modem driver, a keyboard driver, and so on, required for the execution of the operating system.
Import Date	The date and time at which the driver was imported into the CM database.

This section includes the following topics:

- Creating a new driver
- Scanning a directory for drivers
- Modifying a driver
- Deleting a driver

Creating a new driver

To create a new driver proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Drivers** in the left window pane.
2. Select **Edit > Create Driver**
   The **Properties** window appears.
3. Select a drivers .inf file:
   a. Click **Select** next to the **Driver .inf File** field.
      The **Driver File** from *Your OSD Manager* window appears, providing the directory structure of the currently selected OSD Manager.
   b. Browse to the correct file and select it.
   c. Click **OK** to confirm and to close the window.
      After the agent has located the file most of the following text boxes will be filled in automatically and most of them are not editable to ensure data integrity.
4. Enter a name for the new driver.
5. If the driver is required for a specific installation you can add a tag to classify it.
6. If desired, add a note to the new driver.
7. Click **OK** at the bottom of the window to confirm the data for the new driver.

The new driver will be automatically created under the driver class node to which it belongs, for example, all network card drivers will be created under the **Network Cards** node. If the folder for this class does not yet exist it is created.

Scanning a directory for drivers

New computers tend to come with their own driver CD/DVD on which the driver files are organized in a tree, where the branches are the device type and then supported operating systems. To simplify the import of all these drivers Client Management provides you with the option of scanning this directory and automatically importing all drivers found by the scan.

To scan a directory for drivers proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Drivers** in the left window pane.
2. Select **Edit > Scan Directory** .
   The **Scan Directory** dialog box appears on the screen.
3. Select the directory which contains the driver hierarchy.
4. Click **OK** to confirm.
   The agent will now scan the indicated directory and all its subdirectories. After the scan is finished the **Scan Directory** window appears, displaying the list of drivers found.
5. If you want to classify the drivers that you are importing enter a descriptive name into the **Tag** field.
6. Click **OK** to launch the driver import for all found drivers.

The drivers are being imported. The generated driver entries are named after the available driver information, such as the internal name, the supported architecture and operating system.

The new drivers will be automatically created under the driver class node to which they belongs, for example, all graphic card drivers will be created under the **Video** node of the **OS Drivers** node and all network card drivers will be created under the **Network Cards** under the **Deployment Drivers** node. If the folder for this class does not yet exist it is created.

Modifying a driver

1. Select **OS Deployment > Your OSD Manager > Drivers** in the left window pane.
2. Select the desired driver in the left window pane.
3. Select **Edit > Properties** .
   The **Properties** window appears.
4. Make the desired modifications in the respective boxes.
5. Click **Check Driver** to the right of the **Status** box.
6. If the **Status** box displays:
   a. **OK** , click **OK** at the bottom of the window to confirm the modifications.
   b. Anything other than **OK** , reverify your modifications for errors and repeat steps 5 and 6.

Your modifications were saved and applied to the selected driver.

Deleting a driver

> **Note:**
>
> This operation will delete the driver and all its relations to the other objects. It is instantaneous as the driver is no longer included in the images, it is now associated, and therefore does not disrupt the use of the image, because these do not need to be rebuilt.

To delete a driver proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Drivers** in the left window pane.
2. Select the driver to delete in the right window pane.
3. Select **Edit > Delete**

The selected object will be deleted immediately.

Managing Drivers by model

For recent hardware, the WinPE WMI script cannot always automatically detect all drivers. This option allows you to create a directory in which all drivers pertinent to a specific hardware model are copied and to be used by OSD projects for this model type.

Following are some examples how you can find the hardware model name:

- You can use a test project: A single active test project run on the representative set of hardware devices automatically creates the model name folders on the OSD Manager (**<driver cache root>/bymodel/<model name>/**) and it displays the model name in the test project success window.
- You can use a standalone VB script: You can find a **.vbs** script in the < CM agent >\data\OsDeployment\modelname\modelname.vbs location to run. It results in a popup stating the model name to create the folder manually with.
- You can use the hardware inventory of Client Management : You can find the model name in the hardware inventory section under **Computer System > Model** and use it to create the folder manually.

The **Drivers by Model** node provides a list of all existing driver model name folders with the following information:

Column	Description
File Name	This column lists the names of all files and directories that are located in the selected driver directory.
Size	This column displays the size of the respective file. The field is empty for directories.
Access	This column displays the access types defined for the file or directory in the standard notation of **r** , **w** , **x** and **-** .
Last Modification Time	The date and time at which the driver file or directory was copied into this folder.

Operations on drivers by model

You can execute the following operations on the drivers by model and their content:

- Creating new directories for model drivers
- Transferring the driver files to the model directories
- Scanning model drivers for changes

Creating new directories for model drivers

You can manually add directories to the file structure for the model drivers. To do so, proceed as follows:

1. In the left pane select **Drivers by Model** node or a subdirectory under which the new directory is to be placed.
2. Click **Edit > Create Directory** .
   The **Create a New Directory** pop-up dialog box opens.
3. Enter a name for the new directory then click **OK** to confirm your addition, otherwise click **Cancel** .

Transferring the driver files to the model directories

You can directly transfer the driver files from their original location to the model driver directory on the OSD Manager from the respective directory.

1. Go to the driver directory under the **Drivers by Model** node.
2. Select **File Transfer** .
   The **File Transfer** window opens on the screen. This window allows you to copy files from another device to the OSD Manager.
3. Find the driver files to be copied in the tree hierarchy of the remote device and select it.
4. Select the target directory, that is, **<driver cache root>/bymodel/<model name>/** on the OSD Manager.
5. Click the arrow between the two boxes to start the transfer.

   > The transfer can be stopped and thus the file copy being canceled by clicking **Cancel the current transfer** .

6. Select **Close** at the bottom of the window when all required files were transferred.

Scanning model drivers for changes

If changes were made to the model drivers, the directories need to be scanned to make the projects aware of these changes. This is done either automatically, when the OSD module is started, or whenever any project is (re-)built. However, to make sure you can also manually scan the model drivers for any changes as follows:

1. In the left pane select **Drivers by Model** node or a subdirectory under which the new directory is to be placed.
2. Click **Edit > Scan Drivers by Model** .
3. Click **Yes** in the **Confirmation** dialog box.
   The scan of all existing directories is directly started.

The view of a selected Driver

The view of a driver provides access to the information of the selected driver via its two tabs:

- **Driver Information**
- **Supported Hardware**

The following sections provide more information about Driver Information and Supported Hardware:

Driver Information

The WinPE requires specific drivers for the OS deployment, that is, the driver for the network card installed on the target device and, if the target has a SATA disk, the SATA driver as well. Also the installation of the operating system might require specific drivers, such as video or keyboard drivers. In this view all options about the defined drivers can be viewed and modified.

The table of the driver's node displays the following information about the selected driver:

Parameter	Description
Name	This field displays the name of the currently selected driver.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are 32-bit for x86 and 64-bit for amd64 Windows installations.
Catalog File	The name of the Microsoft catalog file.
Tags	The list of tags to which the driver is assigned to.
Class Family	The family (type) of the driver, for example, *audio driver, video driver, mouse driver, NIC driver* and so on.
Class GUID	The unique identifier of the class (Microsoft specific).
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Driver Description	A brief description of the driver by the manufacturer.
Supported OS	The list of operating systems supported by the driver.
Driver Version	The release date and version of the driver.
Driver File List	The list of files required by the driver for installation.
Import Date	The date and time at which the import of the driver terminated.
Inf File Name	The name of the principal driver file (*.inf).
Manufacturer	The name of the component manufacturer.
Signature	The signature of the driver, which in most cases should be *$WINDOWS NT$* .
Provider	The name of the driver manufacturer.
Type	This field identifies the type of the driver, that is, if it is a WinPE driver, a network or a SATA disk driver, a video or a modem driver, a keyboard driver, and so on, required for the execution of the operating system.
Driver .inf File	The name of the *.inf* file of the driver and the path to it, for example, <code>D:/Drivers/TEXTORM/chipset/Vista32/Ethernet/nvfd6032.inf</code>.
Creation Date	The date and time that the currently selected driver was created for the first time.
Last Modification Date	Displays the date and time at which the selected object was modified for the last time; for folders this field remains empty.
Notes	This free text field can contain additional information concerning the selected object.

Supported Hardware

This tab displays the list of hardware equipments that the currently selected driver supports.

The table displays the following information about the hardware:

Parameter	Description
Description	This field displays the name of the driver hardware, such as the name of the network, the audio or the modem card.
Component	This column displays the list of corresponding components.

Driver Tags

Driver tags are used to classify drivers according to their targets to make their selection easier when assigning them to specific projects. A tag is like a folder, that can be assigned to a group of drivers that are required for example for a specific type of computer, for example, Dell GX280 contains all drivers that are required when installing a computer of this type.

This section also includes following topics:

View of a Driver Tag

Next to the **General** tab, the **Driver Tags** node has a **Drivers** tab, listing all drivers that the selected tag is assigned to.

Parameter	Description
Name	This column lists the name of the driver.
Architecture	This column indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program for which the driver is required. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.
Type	This column identifies the type of the driver, that is, if it is a WinPE driver, or if it is a network or a SATA disk driver, a video or a modem driver, a keyboard driver, and so on, required for the execution of the operating system.
Import Date	The date and time at which the driver was imported into CM .
Notes	This free text field can contain more information about the selected object.

Creating a new Tag

To create a new driver tag proceed as follows:

1. Click **Create Driver Tag**  .
   The **Create a Driver Tag** window appears.
2. Enter an explicative name into the **Name** field, for example, the type of computer for which the drivers are required, *Dell GX280* .
3. Click **OK** to confirm.

The new tag is added to the list of tags.

Managing OSD Images

The **Images** node provides access to all images which are defined for the operating system deployment.

Images must be created for all different types of deployment, that is, one is required as well when capturing a WIM image. Images are the objects that contain all the base information required to access the setup files or the WIM/custom image to install on the target device, that is, the directory where to find it and the access credentials.

Images are the objects that contain all the base information required by the target devices for the remote operating system installation, such as the location where to find the files to install, how to access the location, of which type the installation is, and all the installation instructions required by the target device to execute the deployment.

Images do not include the necessary drivers, these are added apart, the same images can be used in different sub-networks within the organization using different sets of drivers.

In the tree structure in the left window pane, the **Images** node has one subnode for each **Image Type** for which at least one image is defined.

The following topics are provided:

Image types

The nodes for the different image types are automatically created when the first image of the respective type is created. All newly created images will automatically be added in their image type:

Mode	Image Types
Setup Mode	• Windows Vista / 7 / 8 / 10 Setup • Windows XP/Server 2003 Setup
WIM Image Mode	• Standard WIM Image • Windows XP/Server 2003 Sysprep WIM Image • Windows Vista / 7 / 8 / 10 Sysprep WIM Image
Custom Mode	• WIM Image Capture • Customized Image

The **Image Type** node provides a list of all existing images with the following information:

Parameter	Description
Name	This column lists the names of all images that were created under the **Images** node.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.

Parameter	Description
Type	This parameter defines the image type being used for the deployment. This list is already pre-filtered and only provides image types applicable to the selected deployment mode.

In the tree structure in the left window pane, the **Images** node has one subnode for or each defined image.

Related topics

- Operations on OSD Images
- View of an image

Operations on OSD Images

Following operations can be performed on OSD Images:

Creating a new OS Image

To create a new OS image proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Images** in the left window pane.
2. Select **Edit > Create Image** .
   The **Properties** window appears.
3. Enter the desired data into the respective boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** OK, the image cannot be created.

4. Click **Check Image** to the right of the **Status** field to verify.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directory and the access rights to it. If all values are correct the **Status** OK is returned, otherwise an error message displays in the **Status** field indicating where the parameter value is not correct.
5. Click **OK** once the **Status** OK is returned, to confirm the new image.

A new OS image was created.

Duplicating an OS Image

To duplicate an existing image and all its assignments proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Images** in the left window pane.
2. Select the image to duplicate from the list in the right window pane.
3. Select **Edit > Duplicate** .
   The **Properties** window appears.

4. Enter a new name for the new image.

> In CM two images with the same name cannot co-exist.

5. Make any other desired changes to the new image.
6. Click **OK** to confirm the data for the new image.

The new image will be created under the main **Image** node with the same assigned objects as the original.

Deleting an OS Image

To delete an OS image proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Images** in the left window pane.
2. Select the image to delete in the table to the right.
3. Select **Edit > Delete** .

The selected OS image was deleted immediately.

View of an image

The table of an **Image** node displays the following information about the currently selected image:

Parameter	Description	
Name	This field displays the name of the selected image.	
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.	
Architecture	This field indicates the type of architecture the image is to be applicable to. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.	
Type	This parameter defines the image type being used for the deployment. This list is already pre-filtered and only provides image types applicable to the selected deployment mode. This parameter defines the image type being used for the deployment. The possible values are **Windows Vista / 7 / 8 / 10 Setup** and **Windows XP/Server 2003 Setup** for the **Setup Mode** , **Standard WIM Image** , **Windows XP/Server 2003 Sysprep WIM Image** and **Windows Vista / 7 / 8 / 10 Sysprep WIM Image** for the **WIM Image Mode** deployment and **WIM Image Capture** and **Customized Image** for the **Custom Mode** .	
Location	This field displays the network path to the image or setup folder, where the image files are located. This directory can be located on any device in your network, as long as it can be accessed by the OSD Manager. Depending on the mode selected for the image this can be, for example:	
	Setup Mode	`\\192.168.196.13\Vista32` , to indicate the folder which contains the setup.exe file for the deployment.

Parameter	Description	
		The path for this mode does not include the name of the executable file. `\\192.168.196.13\XP32` , to indicate the folder which contains the `i386\winnt32.exe` directory and file for the deployment.
WIM Image Mode	`\\192.168.196.13\Vista32\vista32.wim` , to indicate the folder which contains the image file for the deployment. Be aware that for this mode the name of the image file (`.wim`) is part of the path. The WIM image file must already exist.	
Custom Mode	`\\192.168.196.13\ghosts32` , indicating where the custom image executable file is located. This image itself can either be located in the same directory or in one of the specified directory's subdirectories. Be aware that for this mode the name of the file is not part of the path, the name will be specified via the command line parameter.	
WIM Image Capture	`\\192.168.196.13\Vista32\images\vista32_test.wim` , indicating the location where the operating system WIM image to be created is to be stored. Be aware that for this mode the name of the image file (`.wim`) is part of the path. If a WIM image of this name already exists, it is overwritten without forewarning.	
Login (read access)	The login to be used by the deploying device to access the network location in the required mode, that is, read and write mode for WIM Capture, read and execute for all other modes.	
Custom Image Command Line	This field contains the command required to deploy the image, for example, `ghost32.exe -clone,mode=restore,src=W:/XP32.GHO,dst=1:0 -SURE` for a ghost image, whereby `W:` is the mounted share of the UNC OS location in the WinPE. An example when using imagex would be: `imagex /apply "W:/MyImageFile.wim" 1 C:` . It is only filled in if the image is to be used for a custom mode deployment via a ghost image.	
By Disk	If the option is selected the script does not do anything partition or disk related after running the custom command.	
Last Check Status	This field displays the status returned by the last verification of the image.	
Last Check Time	This field displays the date and time of the last image verification.	
Detected Languages List	The language of the target operating system as detected by the system.	
Sysprep Tools Path	The full path to the directory in which the files necessary for a sysprep deployment are located. This is defined by CM and cannot be modified.	
Creation Date	The date and time the currently selected image was created for the first time.	
Last Modification Date	The date and time in the user specified format at which the last modification occurred to the selected object.	

Parameter	Description	
Notes	This free text field can contain more information the selected object.	

In addition this node provides access to the object which are linked with the currently selected image:

- All projects to which the image is assigned to
- All operating system drivers that are included in the image

Operations on View of OSD Image

The following topic provides more information about modifying an OS image:

Modifying an OS Image

To modify the parameters of an existing OS image proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Images > Your OS Image** in the left window pane.
2. Select **Edit > Properties**
   The **Properties** window appears.
3. Make the desired changes in the respective boxes.
4. Click **Check Image** to the right of the **Status** box.

> If the **Status** box appears any other value than OK you need to reverify the changes for errors before you can continue.

5. Click **OK** once the **Status** OK is returned, to confirm the modification of the selected image.

Your changes were saved and applied to the selected OS image.

The following topic provides more information about **Project** node:

Projects

The **Projects** node displays the list of individual projects assigned to the selected object. Projects can be assigned to:

- any number of WinPE compatible drivers (the node is not available for non-WinPE drivers)
- any number of images
- only one target list

The table shows the following information about the projects assigned to the currently selected object:

Parameter	Description
Name	This field displays the name of the currently selected project.

Parameter	Description
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.
Type	This field displays the deployment type which the project contains, possible values are Windows Vista/Server 2008 Setup, Windows XP/Server 2003 Setup, Deployment by Installation, Customised Deployment, Deployment by WIM Image and Capture by WIM Image.
Online	This value indicates if the project was build and the files required to install and reboot the device are available, that is, the image files, the boot file, the PXE files, the unattended files, etc. Possible values are Yes, the build process finished successfully and the necessary files were published and No, the necessary files are not yet published and available. Only one project can be online at a time.

Managing OSD Disk Configurations

The **Disk Configurations** node provides access to all hard disk configurations which are defined for the operating system deployment.

BMC Client Management - Software Distribution comes with a number of predefined hard disk configurations which are directly available under this node. This node also allows you to create your own hard disk configurations with partition definition for specific requirements in your infrastructure.

The **Disk Configurations** node provides a list of all existing hard disk configurations with the following information:

Parameter	Description
Name	This column lists the names of all hard disk configurations that were created under the main **Disk Configurations** node.
Partition Table	xxxx.
Size	This value displays the total size of the respective hard disk in MB.
Partition	This field indicates the number of partitions defined for the respective hard disk.

In the tree structure in the left window pane below the **Disk Configurations** top node you can see one subnode for each defined **Disk Configuration**.

For more information on managing OSD Disk Configurations, see the following topics:

- Disk configuration operations
- View of a disk configuration
- View of a partition
- Partition operations

Disk configuration operations

You can execute following operations on OSD disk configurations:

Creating a disk configuration

To create a new disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration** in the left window pane.
2. Select **Edit > Create Disk Configuration** .
3. Enter the necessary data for the parameters in the **Create a New Disk** window:

Parameters	Description
Name	A descriptive name of the object.
Description	This is a free text field into which you can enter any type of description and information that is pertinent to the new disk configuration.
Size (GB)	The size of the disk. It is only used to estimate if the partitions overall size is sensible. It has no impact on the real disk.
Delete Disk Partitions	Defines if any partitions that already exist on the target device are deleted. This option should be used with caution, as any data on the disk is lost irretrievably if selected.
Partition Type	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, etc.
Status	Before the disk configuration can be created it must be verified that all entered data is correct. To execute a check on the disk click **Test** next to the non-editable Status box. Be aware that the disk creation cannot be confirmed until the disk verification succeeded, that is, the status value OK is displayed.
Notes	This free text field can contain additional information concerning the selected object.

4. Click **OK** to confirm the data for the new disk configuration.

The new disk configuration with the specified data is created.

Duplicating a disk configuration

To duplicate an existing disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select **Edit > Duplicate** .
   The **Edit Disk** window appears.
3. Enter a name for the new disk configuration.

> In CM two disk configurations with the same name cannot co-exist.

4. Make any other required changes to the new disk configuration.
5. Click **OK** to confirm the new disk configuration.

The new disk configuration was created under the main **Disk Configurations** node with the same assigned objects as the original.

Deleting a disk configuration

To delete a disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select **Edit > Delete** .

The selected object will be deleted immediately.

Modifying a disk configuration

To modify the parameters of a defined disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select **Edit > Properties** .
3. Modify the necessary parameters in the **Properties** window:

Parameters	Description
Name	This column lists the name of the selected hard disk configuration.
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Size (GB)	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Delete Disk Partitions	This parameter defines if any partitions that already exist on the target device are deleted, possible values are Yes and No. This option should be used with caution, because any data on the disk will be lost irretrievably if selected.
Partition Type	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, etc.
Status	Before the disk configuration can be modified it must be verified that all entered data is correct. To execute a check on the disk click **Test** next to the non-editable Status box. Be aware that the disk modification cannot be confirmed until the disk verification succeeded, that is, the status value OK is displayed.
Notes	This free text field can contain more information about the selected object.

4. Click **OK** to confirm the modifications.

Your modifications of the parameters are saved and applied to the selected disk configuration.

View of a disk configuration

A hard disk configuration provides the OS deployment with all the necessary information about how to deal with the hard disk of the target devices, that is, should it be reformatted or used as it is, if it is reformatted, how many partitions of which size are to be created, and which of the partitions is the boot partition.

The disk configuration pane (to the right) has the following tabs containing information about the selected hard disk configuration:

The Disk Setup tab

The **Disk Setup** tab specifies the basic information of the new hard disk configuration to be created on the target device during installation.

The table of the **Disk Setup** tab displays the following information:

Parameter	Description
Name	This column lists the name of the selected hard disk configuration.
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, and so on.
Size (GB)	This value displays the total size of the respective hard disk in GB.
Partition Table	The format of the partition table, that is, if it supports legacy or UEFI installations.
Delete Disk Partitions	This parameter defines if any partitions that already exist on the target device are deleted, possible values are **Yes** and **No** . This option should be used with caution, because any data on the disk will be lost irretrievably if selected.
Creation Date	The date and time the currently selected disk configuration was created for the first time.
Last Modification Date	The date and time in the user specified format at which the last modification occurred to the selected object.
Notes	This free text field can contain more information about the selected object.

The Partition Setup tab

The **Partition Setup** tab provides access to the parameters of the hard disc configuration about its basic partition information.

These partitions are created during the installation process on the remote target device.

The table of the **Partition Setup** tab displays the following information on the defined partitions:

Parameter	Description
Order	This parameter specifies the order in which the partitions will be modified, if there is more than one partition, 1 indicating the first partition, and so on.

Parameter	Description
Name	This column lists the names of the defined partitions.
Size (GB)	This value displays the total size of the respective disk partition in GB. **FAT-32** disks cannot be larger than 32 GB. The specified size is adjusted to the cylinder snap and can therefore be somewhat smaller or larger than the defined value.
Format	This parameter indicates the format of the partition, possible values being **NTFS** , **FAT-32** or **Do Not Format** , if the disk is not to be formatted but to use the current configuration, such as to keep another partition type for Linux or to keep partitions with existing data.
Extend	This parameter is of interest if the defined disk partitions do not completely use up the available disk space. Possible values are **Yes** , extend partition, in this case the size fixed for the disk will be ignored and the remaining disk space will be added to the respective partition. If you select **No** , do not extend the partition, the remaining disk space cannot be used. Only one partition per disk can be extended. As **FAT-32** disks cannot be larger than 32 GB, extending it over this limit will generate an error.

View of a partition

The node for the individual partitions provides access to all its parameters and values.

The table of a partition displays the following information on the selected object:

Parameter	Description
Name	The name of the defined partition.
Partition Number	The unique physical partition number on the disk the currently selected entry belongs to, 1 is the first partition, 2 the second, and so on.
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Extend	This parameter is of interest if the defined disk partitions do not completely use up the available disk space. Possible values are **Yes** , extend partition, in this case the size fixed for the disk will be ignored and the remaining disk space will be added to the respective partition. If you select **No** , do not extend the partition, the remaining disk space cannot be used. Only one partition per disk can be extended. As **FAT-32** disks cannot be larger than 32 GB, extending it over this limit will generate an error.
Format	This parameter indicates the format of the partition, possible values being **NTFS** , **FAT-32** or **Do Not Format** , if the disk is not to be formatted but to use the current configuration, such as to keep another partition type for Linux or to keep partitions with existing data.
Label	The unique name of the partition, for example, *SYSTEM, DATA* or *BACKUP*).
Drive Letter	The logical drive letter from C to Z assigned to the drive, each letter can only be assigned once.
Size (GB)	This value displays the total size of the respective disk partition in GB. **FAT-32** disks cannot be larger than 32 GB. The specified size is adjusted to the cylinder snap and can therefore be somewhat smaller or larger than the defined value.
Active Partition	This parameter defines if a partition is active, that is, if it is potentially bootable. This partition must be used to install the operating system on, which is to be booted. Only one partition can be active per disk.
Type	This parameter defines the type of the partition, that is, if it is a primary, extended or logical partition.
Order	This parameter specifies the order in which the partitions will be modified, if there is more than one partition, 1 indicating the first partition, and so on.

Parameter	Description
Creation Date	The date and time the currently selected partition was created for the first time.
Last Modification Date	The date and time in the user specified format at which the last modification occurred to the selected object.
Notes	This free text field can contain more information about the selected object.

For more information about operations on partitions, see Partition operations.

Partition operations

You can execute the following operations on the partitions of a disk:

- Creating a new partition
- Duplicating a Partition
- Modifying a Partition
- Moving a Partition Up or Down
- Deleting a Partition

Creating a new partition

To create a new partition proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select the **Partition Setup** tab in the right window pane.
3. Select **Edit > Create Partition** 
4. Enter the necessary data for the parameters in the **Create a new partition** window:

Parameters	Description
Name	The name of the defined partition.
Partition Number	The unique physical partition number on the disk the currently selected entry belongs to, 1 is the first partition, 2 the second, and so on.
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Extend	This parameter is of interest if the defined disk partitions do not completely use up the available disk space. Possible values are **Yes,** extend partition, in this case the size fixed for the disk will be ignored and the remaining disk space will be added to the respective partition. If you select **No,** do not extend the partition, the remaining disk space cannot be used. Only one partition per disk can be extended. As **FAT-32** disks cannot be larger than 32 GB, extending it over this limit will generate an error.
Format	This parameter indicates the format of the partition, possible values being **NTFS, FAT-32** or **Do Not Format**, if the disk is not to be formatted but to use the current configuration, such as to keep another partition type for Linux or to keep partitions with existing data.
Label	The unique name of the partition, for example, *SYSTEM, DATA or BACKUP*).
Drive Letter	The logical drive letter from C to Z assigned to the drive, each letter can only be assigned once.

Parameters	Description
Size (GB)	This value displays the total size of the respective disk partition in GB. **FAT-32** disks cannot be larger than 32 GB. The specified size is adjusted to the cylinder snap and can therefore be somewhat smaller or larger than the defined value.
Active Partition	This parameter defines if a partition is active, that is, if it is potentially bootable. This partition must be used to install the operating system on, which is to be booted. Only one partition can be active per disk.
Type	This parameter defines the type of the partition, that is, if it is a primary, extended or logical partition.
Order	This parameter specifies the order in which the partitions will be modified, if there is more than one partition, 1 indicating the first partition, and so on.
Creation Date	The date and time the currently selected partition was created for the first time.
Last Modification Date	The date and time in the user specified format at which the last modification occurred to the selected object.
Notes	This free text field can contain more information about the selected object.

WinPE has a number of limitations as described on the Microsoft website (http://technet.microsoft.com/en-us/library/cc507857.aspx) such as the fact that drive letter assignments are *not* persistent between sessions. This means that no matter which drive you assigned specific drive letter in the disk configuration of an OS deployment, the drive letter assignments will be in the default order after WinPE is restarted.

5. Click **OK** to confirm the data for the new partition.

A new partition with the specified data is created.

Duplicating a Partition

To duplicate an existing partition proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select the **Partition Setup** tab in the right window pane.
3. Select the partition to be duplicated in the right window pane.
4. Select **Edit > Duplicate** .
   The **Edit Disk** window appears.
5. Enter a name for the new partition.

In CM two partitions with the same name cannot co-exist.

6. Make any other required changes to the new partition.
7. Click **OK** to confirm the new partition.

The new partition will be created under the node of the selected disk configuration with the same assigned objects as the original.

Modifying a Partition

To modify the parameters of a partition proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk > Your Partition** in the left window pane.
2. Select **Edit > Properties**
3. Modify the necessary parameters in the **Properties** window:

Parameters	Description
Name	The name of the defined partition.
Partition Number	The unique physical partition number on the disk the currently selected entry belongs to, 1 is the first partition, 2 the second, and so on.
Description	This field is a free text field and can contain some descriptive text or necessary information about the object.
Extend	This parameter is of interest if the defined disk partitions do not completely use up the available disk space. Possible values are **Yes,** extend partition, in this case the size fixed for the disk will be ignored and the remaining disk space will be added to the respective partition. If you select **No,** do not extend the partition, the remaining disk space cannot be used. Only one partition per disk can be extended. As **FAT-32** disks cannot be larger than 32 GB, extending it over this limit will generate an error.
Format	This parameter indicates the format of the partition, possible values being **NTFS, FAT-32** or **Do Not Format**, if the disk is not to be formatted but to use the current configuration, such as to keep another partition type for Linux or to keep partitions with existing data.
Label	The unique name of the partition, for example, *SYSTEM, DATA or BACKUP*).
Drive Letter	The logical drive letter from C to Z assigned to the drive, each letter can only be assigned once.
Size (GB)	This value displays the total size of the respective disk partition in GB. **FAT-32** disks cannot be larger than 32 GB. The specified size is adjusted to the cylinder snap and can therefore be somewhat smaller or larger than the defined value.
Active Partition	This parameter defines if a partition is active, that is, if it is potentially bootable. This partition must be used to install the operating system on, which is to be booted. Only one partition can be active per disk.
Type	This parameter defines the type of the partition, that is, if it is a primary, extended or logical partition.
Order	This parameter specifies the order in which the partitions will be modified, if there is more than one partition, 1 indicating the first partition, and so on.
Creation Date	The date and time the currently selected partition was created for the first time.
Last Modification Date	The date and time in the user specified format at which the last modification occurred to the selected object.
Notes	This free text field can contain more information about the selected object.

4. Click **OK** to confirm the modifications.

Your modifications of the parameters were saved and applied to the selected partition.

Moving a Partition Up or Down

To move a partition up or down in the list proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select the **Partition Setup** tab in the right window pane.
3. Select the partition to be moved in the right window pane.
4. Select **Edit > Move Up** or **Move Down**

The selected partition was moved up or down in the list of partitions.

Repeat step 4 until the partition is at the desired position.

Deleting a Partition

To delete a partition proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration > Your Disk** in the left window pane.
2. Select the **Partition Setup** tab in the right window pane.
3. Select the partition to be deleted in the right window pane.
4. Select **Edit > Delete**

The selected object will be deleted immediately.

Managing OSD target lists

As the targets of an OS deployment can be any device in the infrastructure, that is, also a device on which no CM agent is installed, these targets must be grouped, using target lists.

The target lists can contain individual devices with or without a CM agent installed and all the members of already existing device groups.

The **Target Lists** node provides a list of all existing target lists with the following information:

Parameter	Description
Name	This column lists the names of all target lists that were created under the main **Target Lists** node.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are 32 Bit for x86 and 64 Bit for amd64 Windows installations.

In the tree structure in the left window pane below the **Target Lists** top node you can see a subnode for each defined target list.

Operations on target lists

You can execute following operations on the target lists:

- Creating a target list
- Duplicating a target list
- Deleting a target list
- Modifying a target list

Creating a target list

To create a new target list proceed as follows:

1. Select **OS Deployment> Your OSD Manager> Target Lists** in the left window pane.
2. Select **Edit> Create Target List** .
   The **Properties** window appears.
3. Enter the desired data into the respective boxes.

> The unattended Windows Setup answer file, typically called `Unattend.xml` , is the answer file for Windows Setup that is created by using Windows System Image Manager (Windows SIM). The answer file enables the configuration of default Windows settings, as well as the addition of drivers, software updates, and other applications. The answer file enables OEMs and corporations to customize Windows Setup tasks, for example, specifying disk configuration, changing the default values for Internet Explorer, and installing further drivers. If you create your own customized `Unattend.xml` file make sure it is in UTF-16 encoding.

4. Add target devices to the target list:

> There are three ways of adding targets to the target list
> - **Add new targets**
> - **Add existing devices to the target list**
> - **Create a new target**

Method	Description / Steps
Add new targets	Refer to the task Adding a new target to a target list.
Add existing devices to the target list	Refer to the task Adding an existing target to a target list.
Create a new target	Refer to the task Creating a target.

5. Click **OK** to confirm the data for the new target list.

6. The new target list was created under the main **Target Lists** node, containing the selected target devices.

Duplicating a target list

To duplicate an existing target list proceed as follows:

1. Select **OS Deployment> Your OSD Manager> Target Lists** in the left window pane.
2. Select the target list to be duplicated in the right window pane.
3. Select **Edit> Duplicate** .
   The **Properties** window appears.
4. Enter a name for the new target list.

> In CM two target lists with the same name cannot co-exist.

5. Make any other required changes to the new target list.
6. Click **OK** to confirm the target list.
7. The new target list will be created under the main **Target Lists** node with the same assigned objects as the original.

Deleting a target list

To delete a target list proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists** in the left window pane.
2. Select the target list to be deleted in the right window pane.
3. Select **Edit > Delete** .

The selected object will be deleted immediately.

Modifying a target list

To modify the parameters of a target list proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists** in the left window pane.
2. Select the target list to be modified in the right window pane.
3. Select **Edit > Properties** .
   The **Properties** window appears.
4. Make the desired modifications in the respective boxes.
5. Click **OK** to confirm the modifications.

Your modifications of the parameters were saved and applied to the selected target list.

For more information on managing target list, see Managing targets.

Managing targets

A target list contains all the devices to which the deployment is to be assigned. This node provides access to the members of the selected list and their respective information. If the target list is defined by a subnet mask, this list will be filled in dynamically and the devices will add themselves once they are booted. By default this list is updated every 4 minutes.

The table of the target list's node displays the following information:

Parameter	Description
Name	This column lists the names of all targets.
MAC Address	The MAC, that is, the hardware address of the device.
Type	This field indicates if the device was added to the target list as an individual device (Target) or if it is part of a subnet mask (PXE Mask).
Status	This field displays the current status of the selected device with regards to the operating system deployment.
Activation Status	This field displays the status of the target device with regards to their OS installation. The possible values are **Inactive Target** illustrated also with a blue flag  , if the installation process was launched with success and **Active Target** illustrated also with a green flag  , if the device is still waiting to launch its OS installation or an error occurred.
DHCP Activated	Indicates if the internal DHCP server is enabled.
Static IP Address	The IP address which is to be attributed to the target device.

A target list also provides access to all of its members via their own subnode.

The following sections provide information about managing Targets:

- Creating a target
- Adding a new target to a target list
- Adding an existing target to a target list
- Duplicating a target
- Deleting a target
- View of a target

Creating a target

You can also create target devices by individually specifying their data or by specifying a subnet. Only one subnet per target list can be defined. When creating a new target in this way, it is added to the OS Deployment database specifically for this deployment.

To create a new target proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. **Edit > Create Target**
   The **Create a New Target** window appears with its three tabs, **General Information** , **Parameters** and **Unattended Information**.
3. Enter the desired information into the respective boxes.

   > Select the PXE Menu radio button, if the project is to be assigned to a PXE menu. In this case you cannot define a subnet, the PXE menu will take care of this.

4. Click **OK** to add the target device and close the window.

A new target for the selected target list was created.

Adding a new target to a target list

Devices can be added to the list of targets through a number of different ways. One is through different types of lists.

To add a target to a target list proceed as follows:

1. Select **OS Deployment> Your OSD Manager> Target Lists> Your Target List** in the left window pane.
2. Click **Edit> Add Targets** .
   The **Select Devices from the List** window appears providing you with different methods to select the targets.

Select a method to add a target:

Method	Description / Steps
AutoDisc Object	The AutoDiscovery module provides a list of all devices of any type found in the network, such as printers or devices with and without the agent installed. However, the list displayed in this case will only show all clients of type device and only those with a status of Verified or Learned, which means that all devices in this list were verified for existence either by the local client or a neighbor client and exist on the network. To add a device from the list of all autodiscovered devices known to the database proceed as follows: 1. a. Select the **AutoDisc Object tab** in the left window bar. > The **Available Devices** box appears the list of all available devices. You will find more information about the list of autodiscovered devices in the main manual. b. Select the device/devices to be added as targets from the list. c. Click **Add** to move the selected devices to the list of Selected Devices. d. Click the **OK** to confirm the selections and close the window.

Method	Description / Steps
AutoDisc Device	The tab AutoDisc Device allows you to select your target devices from a list of autodiscovered devices by one specific network device. Proceed as follows: 1. a. Select the **AutoDisc Device** tab in the left window bar. The **Select a Device** window appears. b. Select the device of which the autodiscovered list is to be used from one of the tabs of the **Select a Device** dialog box. c. Click **OK** to confirm the selection and close the window. The **Select Devices from the List** dialog box now only displays the devices that were discovered by the selected network device. d. Select the device/devices to be added as targets from this list. e. Click **Add** to move the selected devices to the list of **Selected Devices**. f. Click the **OK** to confirm the selections and close the window.
Network	You can add a device from the list of your Microsoft network neighborhood. To do so, proceed as follows: 1. a. Select the **Network** tab in the left window bar. The box **OK** displays the **Microsoft Windows Network Neighborhood** structure on the screen. b. Select the device/devices to be added to the list from one of its groups. c. Click the **OK** to confirm the selections and close the window.
CSV List	To add a device to the deployment from an existing .csv file proceed as follows: 1. a. Select the **CSV List** tab in the left window bar. The **Open** window appears, in which you need to select the file containing the device list. b. Navigate to the desired .csv file and click **Open** at the bottom of the window. The box **Available Devices** displays now the list of all devices contained in the selected CSV list. c. Check the **Header** box, if your CSV file has a title line which is to be removed. d. Select the device to be added to the deployment from the list in the window. You can also select all devices in the list by using **Select All**. e. Click the OK to confirm the selections and close the window.

The selected target device(s) will be added to the selected target list.

Adding an existing target to a target list

This is the easiest way to add a device to the target list if you deploy only to devices that are already known to the CM database. Devices without agents are not available in this window, that is, devices that have not yet been scanned and added as unconnected devices.

To add an existing target to a target list, proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. Select **Edit > Add Device** .
   The **Select a Device** window appears.
3. Select the device to be added from one of the tabs in the window's sidebar.
4. Click **OK** to confirm.

The selected device was added to the target list.

Duplicating a target

To duplicate an existing target proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. Select the target to be duplicated in the right window pane.
3. Select **Edit > Duplicate** .
   The **Edit Target** window appears.
4. Enter a name for the new target.

   > In CM two targets with the same name cannot co-exist.

5. Make any other required changes to the new target.
6. Click **OK** to confirm the target.

The new target will be created under the selected target list with the same assigned objects as the original.

Deleting a target

To delete a target proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. Select the target to be deleted in the right window pane.
3. Select **Edit > Delete** .

The selected object will be deleted immediately.

View of a target

A target is the individual device on which an operating system is to be remotely installed via the OS deployment. A target can be any device of your infrastructure, independent of the fact if a BCM agent is installed on it. It can be a new device, completely empty, a device on which another operating system is already installed and is to be upgraded or a device of which the operating system must be repaired.

Next to the **General** tab, this node has a **Agent Log File** tab, displaying the contents of the log file for the deployment of the selected target device.

The section includes following topics:

- The Target List General tab
- Agent Log File
- Modifying targets

The Target List General tab

The following table describes parameters of Target List General tab:

Parameter	Description
Name	The user access name. It is simply used as a display name, but it must be unique anyway.
Start Suffix	Displays the suffix which is used to automatically increment the device names within a subnetwork. This field is only displayed for devices with Target Mode PXE Subnet Mask.
Installed Device Count	This field is only displayed for devices with Target Mode PXE Subnet Mask.
Description	Optional free text field in which you may enter additional information regarding the object.
Architecture	Select the type of architecture the target list is to be applicable to.
Operating System	Displays the name of the operating system which is installed on the device. If none is installed yet the field remains empty.
Language	Select from the drop-down box the language. This language setting is applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages have been automatically detected from the installation CD/DVD.
Mac Address	Displays the current MAC address of the target device. This field remains empty if the target is added via a PXE Subnet Filter or a PXE Menu.
IP Address	Displays the current IP address of the target device in its dotted notation. This field remains empty if the target is added via a PXE Subnet Filter or a PXE Menu.
DNS	Displays the current DNS information of the target device. This field remains empty if the target is added via a PXE Subnet Filter or a PXE Menu.
PXE Subnet Filter	Displays the IP address in its dotted notation for the subnet which is to contain the target devices. This field remains empty if the target is added manually or via a PXE Menu.
Target Mode	Indicates the way the target was added to the project, that is, if it was added directly as a Target or via a PXE Subnet Mask or a PXE Menu.
Organization	Defines the name of your organization, for example, *BMC Software* .

Parameter	Description
Workgroup	The network workgroup of the target devices, for example, *WORKGROUP* . If you enter a value here and as well into the **Domain** field later on, this value is ignored.
Administrator Login	Enter into this field the login name to which is to be created for the newly installed OS with the full administrator rights accorded on the new device. For Vista and later versions this field is ignored, as the login name is predefined by Microsoft and can not be modified.
User Login	Enter into this field the login name with which the user is to log on to his device which provides him with the required user rights. This parameter is only applicable to Vista and later.
Domain	Enter into this field the name of the domain the new device should belong to, for example, *TESTLAB* . If you entered a name for the workgroup above the domain value prevails.
Domain Administrator Name	Enter into this field the login name of the domain administrator with which he may access the new device without the domain prefix. for example, *Administrator* and not *TESTLABAdministrator* or *.Administrator* .
DHCP Activated	Indicates if the internal DHCP server is enabled.
Static IP Address	The IP address which is to be attributed to the target device.
Subnet Mask	The subnet mask for the target device.
Default Gateway	The IP address of the gateway of the target device.
Primary DNS Server	The IP address of the preferred DNS server of the target device.
Auxiliary DNS Server	The IP address of the alternate DNS server of the target device.
Product Key	Defines the preformatted input for the OS product key (for example: *ABCDE-FGHIJ-KLMNO-PQRST-UVWXY*). Replace the standard key already entered in this field with the key provided by Microsoft on your installation DVD.
Color Depth	Defines the color depth in bits per pixel of the target screen.
Resolution (DPI)	Defines the resolution in dpi that is to be used for the fonts displayed on the screen of the device to be installed.
Refresh Rate (hz)	Defines the refresh rate in Hertz of the target screen (for example: *85* for CRT, *60* for LCD).
Screen Resolution	Defines the resolution in pixels of the target screen. The value in parenthesis behind the value indicates for which screen size the respective resolution is generally used.
Time Zone	The timezone in which the target device is located.
First Login Command	Defines the commands to be executed on the first login, this may be a path to a batch file to execute, for example, *E:Apps.bat* or *cmd /c REGEDIT /S E:Appspatch.reg* . This parameter is both applicable to Windows setup as well as sysprep.
Activation Status	This field displays the status of the target device with regards to their OS installation. The possible values are **Inactive Target** illustrated also with a blue flag , if the installation process was launched with success and **Active Target** illustrated also with a green flag , if the device is still waiting to launch its OS installation or an error occurred.

Parameter	Description
Status	This field displays the current status of the selected device with regards to the operating system deployment.
Creation Date	The date and time at which the target was created for the deployment.
Last Modification Date	Displays the date and time at which the selected object was modified for the last time; for folders this field remains empty.
Notes	This free text field can contain additional information concerning the selected object.

Agent Log File

This tab displays the contents of the log file of the multicast session.

Modifying targets

To modify the parameters of one or multiple target proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. Select the target to be modified in the right window pane.

> It is possible to edit the parameters of several targets at the same time. In this case all boxes in the **Properties** window will be blank by default. If you enter or select a value for a box this value will become applicable to all selected devices. All other values remain as they are. When selecting multiple targets all boxes which cannot be duplicated, such as the MAC address, are not accessible. This option is specifically useful for operations such as activating or deactivating a number of targets at the same time.
> To select multiple targets, select one, press and hold the CTRL key and select further targets.

3. Select **Edit> Properties**  .
   The **Edit Target** / **Edit Targets** window appears.
4. Make the desired modifications in the respective boxes.
5. Click **OK** to confirm the modifications.
6. Your modifications of the parameters were saved and applied to the selected target(s).

Managing OSD Projects

Projects are the central point which collect all different elements which compose the OS deployment.

Via these elements it receives all the information which is then compiled during the project build process. After this process has terminated with success the project becomes active and publishes all required information and files, that is, all required information is made available to the target devices for installation.

In the tree structure in the left window pane below the **Projects** node you can see one subnode for each project type for which at least one project is defined.

The following topics are provided:

- Project types
- Related topics

Project types

The nodes for the different project types are automatically created when the first project of the respective type is created. All newly created projects will automatically be added in their project type.

The node of a **Project Type** provides a list of all existing projects of its type with the following information:

Parameter	Description
Name	This column lists the names of all projects that were created under the respective **Project Type** node.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are **32-bit** for x86 and **64-bit** for amd64 Windows installations.
Type	This field displays the deployment type which the project contains, possible values are **Windows Vista/Server 2008 Setup, Windows XP/Server 2003 Setup, Deployment by Installation, Customized Deployment, Deployment by WIM Image** and **Capture by WIM Image** .
Online	This value indicates if the project was a build and the files required to install and reboot the device are available, that is, the image files, the boot file, the PXE files, the unattended files, and so on. Possible values are **Yes** , the build process finished successfully and the necessary files were published, and **No** , the necessary files are not yet published and available. Only one project can be online at a time.

In the tree structure in the left window pane below a project type's node you can see one subnode for each defined Project.

Related topics

- Managing projects
- Managing multicast sessions

Managing projects

The node of a project provides access to the project's dashboard and to its parameters and their values and its log file via the following tabs:

- The project's dashboard

- General settings of a project
- Deployment log file of an OSD project
- Creating a USB device for an OSD project

The project's dashboard

The values in the upper part of the view display the main parameters and their values of this project.

Parameter	Description
Name	This field shows the name of the selected project.
Build Status	This field displays the current status of the build. If any other status than **OK** appears in this field, the current project can not be deployed to the targets for installation.
Re-build required	This field displays if a full or partial re-build of the project is required before it can go online. This might be the case after modifications such as the addition of drivers to the project have occurred.
Last Build Date	This field displays the date and time at which the last build of the currently selected project finished.
Scheduled Date	This field displays the date and time that defines when the project build operation is to be launched.
Description	A summarized description of the functionality of the service, such as Provides software installation services such as Assign, Publish, and Remove.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are **32-bit** for x86 and **64-bit** for amd64 Windows installations.
Capture or Deployment Disk	This field displays the drive letter on which the new operating system is installed on the target devices or on which it is installed if a capture of an existing system is to be done by the selected project.
Online	This value indicates if the project was a build and the files required to install and reboot the device are available, that is, the image files, the boot file, the PXE files, the unattended files, and so on. Possible values are **Yes** , the build process finished successfully and the necessary files were published, and **No** , the necessary files are not yet published and available. Only one project can be online at a time.
Operation after Installation	This field provides the list of possible actions which can be executed after the installation of the operating system has finished on the target. The possible values are **Reboot, Shutdown** and **None** . This option is not applicable to the Setup mode.

The lower part of the view provides the table for all devices that are included in the project and general information about the advancement of the deployment.

Parameter	Description
Name	The name of the device as it is known in the network.
MAC Address	The physical address of the device.
Type	Indicates the way the target was added to the project, that is, if it was added directly as a **Target** or via a **PXE Subnet Mask** or a **PXE Menu** .
Status	This field displays the current status of the listed device with regards to the operating system deployment.

Parameter	Description
Activation Status	This field displays the status of the listed target device with regards to their OS installation. The possible values are **Inactive Target** illustrated also with a blue flag , if the installation process was launched with success and **Active Target** illustrated also with a green flag , if the device is still waiting to launch its OS installation or an error occurred.
DHCP Activated	Indicates if the internal DHCP server is enabled.
Static IP Address	The IP address which is to be attributed to the target device.

Creating a USB device for an OSD project

BMC Client Management allows you to create a self-sufficient USB device for operating system deployment. It provides you with the following two modes for this:

- **Offline Mode**
  This mode assumes that the target device does not have an Internet connection and no possible way to contact the OSD Manager. It stores all data that is necessary for a successful deployment, that is, the WinPE and the complete project data, setup or WIM image (including sysprep).
  Should the target device have access to a network and a network boot listener can be found by the device, the OS installation first tries to see if more recent data are available via the network before using the data stored on the USB device. If yes, the new data is downloaded and the installation effected with the most recent data, if not the installation is launched using the project data stored on the device.
- **Online Mode**
  This mode assumes that the target device does have an Internet connection and a connection with the OSD Manager. The data required to launch the deployment are stored on the USB device, and all other, further required data, such as the actual image to be installed, are then downloaded from the OSD Manager.

The default file system for the USB key to create is NTFS. However, specific tablets, such as Surface 2, and possibly other older UEFI hardware, cannot boot on an NTFS partition. The OSD functionality therefore provides you with both choices when creating the USB device:

- **NTFS**
  Most more recent device allow booting from an NTFS partition. This has the advantage that the full disk space of a USB device larger than 32 GB can be used and WIM images can also be stored on the device. Before selecting this option, make sure your targets support booting from NTFS.
- **FAT32**
  The FAT32 file system allows to boot every device, but it has a number of limitations and should therefore only be used if absolutely necessary; either when creating a USB device for offline mode, or when creating a USB device for on-line mode. The FAT32 system is limited 32 GB partitions and a maximum file size of 4 GB. The base image for a WIM image

is approximately 3.5 GB for Windows 8.1 update 1, and easily passes the 4 GB size limit if the system was customized with large software, such as Microsoft Office, before the capture.

A USB device can be created on OSD Manager level or at project level, however, the USB device must be connected physically to the OSD Manager for both cases.

This section also includes:

Creating the USB device

Note:

A bootable USB device can only be created on the OSD Manager and the USB device must be physically connected to the OSD Manager device.
Make sure your USB device is large enough to contain all the project data in addition to the WinPE if you create a USB device for offline mode. The estimated size is displayed in this view in the **Total estimated size on the USB device:** box.
Any data that are stored on the selected USB device are irrevocably deleted before the bootable USB device is created.

1. Plug the USB device into the OSD Manager device.
2. Select the **USB Device** tab of the **OS Deployment> Your OSD Manager> Projects> Your Project Type> Your Project** node in the right window pane.
3. Select if you want to create an online or offline device by clicking the respective radio button. The value of the **Total estimated size on the USB device:** below is updated depending on your selection and shows the estimated size that must be available on the USB device. This value represents the size of the project plus the connected image and the WinPE for an offline project or only the necessary boot data for online mode.
4. Select the drive into which you connected the USB device from the **Which drive would you like to use?** list.

   This list only shows the drives on which a USB device is connected. It displays the drive letter together with the total size of the connected USB device. Be aware, that this is not the currently available space of the device, as the contents of it are erased before the USB device is created.

5. If your target does only boot from a FAT32 partition, select the **FAT32** radio button.
6. Select the answer file from the **Which answer file would you like to use?** list. Leave the **Automatic** value, if you want the USB device to use the automatic mode.
7. Click **Start** to create the USB device.

The USB device is cleaned of all existing data and the selected data are copied to the USB device. You can follow the progress of the USB creation in the progress bar at the bottom of the tab.

General settings of a project

This tab provides access to the general parameters and settings of the selected project. Some of these parameters can be modified. Be aware that modifying a parameters might require a partial or full rebuild of the project.

Parameter	Description
Name	This field shows the name of the selected project.
Supported BIOS Type	The type of BIOS mode supported by the project, that is, if it supports legacy as well as UEFI deployments or only one of them. Only the setup mode supports projects valid for legacy and UEFI at the same time.
Re-build required	This field displays if a full or partial re-build of the project is required before it can go online. This might be the case after modifications such as the addition of drivers to the project have occurred.
Build Status	This field displays the current status of the build. If any other status than **OK** appears in this field, the current project can not be deployed to the targets for installation.
Last Build Date	This field displays the date and time at which the last build of the currently selected project finished.
Cache Location	This parameter allows the user to manually select the partition where the cache is downloaded, or specify a path. It may be a driver letter, or **System** or **Automatic** . The default value is **Automatic**, which selects the partition with the largest - and writeable - free space available.
Type	This field displays the deployment type which the project contains, possible values are **Windows Vista/Server 2008 Setup, Windows XP/Server 2003 Setup, Deployment by Installation, Customized Deployment, Deployment by WIM Image** and **Capture by WIM Image** .
Delete Cache	Defines if and when the downloaded material is deleted on the client. The following values are available: • **Never** : The downloaded cache is never deleted and thus always available to the user if the deployment succeeds. This may be used for local system recovery, especially if using a setup installation. • **On Success** : The downloaded cache is only deleted if the deployment is successful, to reclaim the disk space. In case of a deployment failure the cache is not deleted and the user may access it for debugging purposes, especially if using the **do not reboot** option in the project parameters and perform manual operations. • **Always** : The downloaded cache is always deleted, on success and on failure of any type.
Description	This is a free text field that contains any type of description and information that is pertinent to the project
Use Model Drivers	The OSD Manager automatically selects and copies the relevant driver folder based on the machine model name during the installation (Setup as well as Sysprep).
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are **32-bit** for x86 and **64-bit** for amd64 Windows installations.
Capture or Deployment Disk	This field displays the drive letter on which the new operating system is installed on the target devices or on which it is installed if a capture of an existing system is to be done by the selected project.

Parameter	Description
Online	This value indicates if the project was a build and the files required to install and reboot the device are available, that is, the image files, the boot file, the PXE files, the unattended files, and so on. Possible values are **Yes**, the build process finished successfully and the necessary files were published, and **No**, the necessary files are not yet published and available. Only one project can be online at a time.
Operation after Installation	This field provides the list of possible actions which can be executed after the installation of the operating system has finished on the target. The possible values are **Reboot, Shutdown** and **None**. This option is not applicable to the Setup mode.
Scheduled Date	This field displays the date and time that defines when the project build operation is to be launched.
Disable Automated Driver Detection	If selected, the automatic driver detection is NOT performed during the project deployment.
Creation Date	The date and time the currently selected project was created for the first time.
Last Modification Date	The date and time in the user-specified format at which the last modification occurred to the selected object.
Notes	This free text field can contain additional information concerning the selected object.

Project operations

You can execute the following operations on or for a project:

- Creating a project
- Duplicating a project
- Modifying a project
- Building a project
- Deleting a project
- Viewing deployment logs

Creating a project

To create a new project proceed as follows:

1. Select **OS Deployment> Your OSD Manager> Projects** in the left window pane.
2. Select **Edit> Create Project**
   The **OS Deployment Wizard** window appears displaying the dialog box about the project.
3. Select the **Deployment Type** :

Type	Description
OS Deployment: Setup Mode	Using the setup mode allows you to execute a regular installation of the operating system on the remote devices or targets via the operating system's setup executable file. The use of an unattended file makes the installation silent and automatic.

Type	Description
OS Deployment: WIM Image Mode	The WIM mode allows you to deploy the new operating systems or images of other non-booting disks to the targets via a WIM image, that is either delivered on the operating system disk or via a custom created WIM image. This mode may only be used if the target hardware is compatible to the hardware of the source device.
OS Deployment: Custom Mode	This mode allows you to use other applications with which snapshots of existing installations may be created and then be 'duplicated' on other devices, such as for example ghost images.
WIM Image Capture	The WIM capture mode allows you to create your own WIM images to be deployed via the WIM mode within your network. You may also use this mode create images of other, non-booting disks, such as drives that contain only applications or data and deploy these via the WIM mode to other devices within your infrastructure.

4. Click **Next** to go the next window.
5. Define the project specific parameters in their respective boxes.
6. Click **Next** to go the next window.
7. To add the new project to a PXE boot menu check the **Add** box. If the project is not to be part of a PXE menu continue directly with the next step.
   - Enter a name for the project under which it displays in the boot menu into the **Caption** field.
   - Enter a description if required.
   - Select the menu to add to from the following list. If no menu exists yet, create one by clicking **Create Menu**  above the table.
8. Click **Finish** to confirm the data for the new project.

The new project will be automatically created under the project type node to which it belongs, that is, all projects of type WIM Capture will be created under the **Capture by WIM Image** project type node. If the folder for this type does not yet exist it is created.

Duplicating a project

To duplicate an existing project proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Projects > Your Project Type** in the left window pane.
2. Select the project to be duplicated in the right window pane.
3. Select **Edit > Duplicate**  .
   The **Properties** window appears.
4. Enter a name for the new project.

> In CM two projects with the same name cannot co-exist.

5. Make any other required changes to the new project.
6. Click **OK** to confirm the new project.

The new project will be created under the same project type node and with the same assigned objects as the original.

Modifying a project

To modify the parameters of a defined project proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Projects > Your Project Type** in the left window pane.
2. Select the project to be modified in the right window pane.
3. Select the project's **General** tab.
4. Select **Edit > Properties** .
5. Make the desired modifications in the respective boxes of the **Properties** window:

Parameters	Description
Number	The project number that is automatically assigned to each new project. This value cannot be modified.
Name	This field shows the name of the selected project.
Description	This is a free text field into which you can enter any type of description and information that is pertinent to the project.
Architecture	This field indicates the type of architecture for the OS deployment, that is, the architecture of the WinPE image launching the setup program. The possible options are 32-bit for x86 and 64-bit for amd64 Windows installations.This value cannot be modified.
BIOS Type	Select the type of BIOS mode supported by the project, that is, if it is to support UEFI or legacy deployments or both.
Operation after Installation	This field provides the list of possible actions which can be executed after the installation of the operating system has finished on the target. The possible values are Reboot, Shutdown and None. This option is not applicable to the Setup mode.
Target Drive	Select from this field the drive letter for/of the operating system. If the project is for a Vista setup, the selected target drive must exist in the disk configuration selected for the project.
Disable Automated Driver Detection	If selected, the automatic driver detection is NOT performed during the project deployment.
Use Model Drivers	The OSD Manager automatically selects and copies the relevant driver folder based on the machine model name during the installation (Setup as well as Sysprep).
Deployment by Multicast	Check this box if the operating system deployment to the targets is to be effected via Multicast.
Cache Location	This parameter allows the user to manually select the partition where the cache is downloaded, or specify a path. It may be a driver letter, or System or Automatic. The default value is Automatic, which selects the partition with the largest - and writeable - free space available.
Delete Cache	Defines if and when the downloaded material is deleted on the client. The following values are available: Never: The downloaded cache is never deleted and thus always available to the user if the deployment succeeds. This may be used for local system recovery, especially if using a setup installation.On Success: The downloaded cache is only deleted if the deployment is successful, to reclaim the disk space. In case of a deployment failure the cache is not deleted and the user may access it for debugging purposes, especially if using the do not reboot option in the project parameters and perform manual operations.Always: The downloaded cache is always deleted, on success and on failure of any type.

Parameters	Description
Notes	This free text field can contain additional information concerning the selected object.

6. Click **OK** to confirm the modifications.

Your modifications of the parameters were saved and applied to the selected project.

Building a project

In case of a Sysprep WIM Capture distribution, the target **must** be running before the project becomes active! Also, you must manually launch the provided batch file `//<;OSD Manager>/PXETFTP/SYSPREP/RUNSYSPREP.BAT` that will sysprep the target and finally reboot it. The file must be executed as a privileged user (admin). If the file cannot be found in this location the project is not activated or not set as a Sysprep image type.

Whenever modifications are made to a project it must be rebuilt to verify all modifications and parameters, before it can be used again.

To (re)build a project proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Projects > Your Project Type > Your Project** in the left window pane.
2. Select **Edit > Build Project**  .
   The **Build a Project** window appears.
3. Define the time at which the build process is to be executed by selecting either:
   - The **Immediately** radio button
   - The **Deferred to** radio button and entering the desired date and time values in the respective boxes.
4. If the project does not require a full build you have the choice to:
   - either only generate an incremental build, that is, to rebuild only the elements that require rebuilding by leaving the **Incremental Build (generate only changed elements, faster)** option selected,
   - or you can also force a complete build, that is, rebuild the whole project with all modifications by selecting the **Full Build (generate all elements, longer)** option.

   > **Note:**
   >
   > Be aware that this process is time and resource consuming.

5. If desired, check the **Active** box.

> When the **Active** box is checked, the project files are published and made available for the target devices after a successful build.

6. Click **OK** to confirm.

The selected project will now be (re)built.

Deleting a project

To delete a project proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Projects > Your Project Type** in the left window pane.
2. Select the project to be deleted in the right window pane.
3. Select **Edit > Delete** .

The selected object will be deleted immediately.

Viewing deployment logs

The log file tab displays the complete log of the deployment to all targets of the currently selected project.

Managing multicast sessions

The multicast sessions node provides access to all active and pending sessions of the currently selected project and the parameters defined for these sessions. It is only available for project that support multicast, such as deployments by setup and WIM images, sysprep or not. Custom deployments and captures are not supported. However, it is available even if the project is unicast, because the administrator can switch between unicast and multicast mode at any time from within the multicast options view.

Its details are shown via the following tabs:

- [The Session's Dashboard|Session Dashboard#id122NA0T0730]
- [The Session's Options|Session Options#id122NA0T00RO]
- [The Session's History|Session History#id122NA0U05E9]

Furthermore you can see a subnode for each defined Multicast Server that executes sessions for this project.

The following topics provide more information about managing multicast sessions:

- Session dashboard
- Session options
- The multicast server node of a project

Session dashboard

The **Dashboard** provides an overview in graphical as well as tabular format over all multicast sessions of the selected project:

Parameter	Description
Multicast Session Breakdown	This table displays information relative to the multicast session status situation.
Projects	The number of project sessions that are either planned, executing or finished their execution within this project.
Running	The number of currently executing sessions.
Pending	The number of currently pending sessions. Pending in this case means that the session starts as soon as the current session finishes if it is the next session in the queue.
Waiting	The number of sessions currently waiting for devices to connect or the timer to finish. Once it is manually started by the user or the automatic threshold(s) are reached its status becomes Pending.
Status Breakdown	This pie chart displays the overall and final status of the project, that is the number of deployments that succeeded or failed.

The following table provides the following information about the sessions and all their targets:

Parameter	Description
Proxy	The name of the Multicast Server on which sessions are executed for this project.
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running* .

This section also include following topics:

Putting a project online

Projects that were prepared for deployment but never activated can be put online directly in this view:

1. Click **Put the project online** in the upper right corner of the panel.
   A confirmation window appears.

2. Click **Yes** to confirm the operation.
   The project will be put online immediately, that is, it is now available for its targets and the deployment can start whenever the targets are ready.

Taking a project offline

Projects that have successfully executed and have no need to remain online any longer can be put offline directly in this view:

1. Click **Take the project offline** in the upper right corner of the panel.
   A confirmation window appears.
2. Click **Yes** to confirm the operation.
   The project will be put offline immediately, that is, it is no longer available to its targets.

Session options

The **Options** tab provides access to the Multicast settings specific to the project. A number of these settings can be modified, but be aware that some of them then require a full rebuild of the project. Also, modifying these settings will only affect sessions related to this particular project.

Parameter	Description
Cache Location	This parameter allows the user to manually select the partition where the cache is downloaded, or specify a path. It may be a driver letter, or **System** or **Automatic** . The default value is **Automatic** , which selects the partition with the largest - and writeable - free space available.
Client Timeout (ms)	The time in milliseconds for each multicast client to wait any packet from the server before declaring the server offline and terminating with an error.
Delete Cache	Defines if and when the downloaded material is deleted on the client. The following values are available: • **Never**: The downloaded cache is never deleted and thus always available to the user if the deployment succeeds. This may be used for local system recovery, especially if using a setup installation. • **On Success**: The downloaded cache is only deleted if the deployment is successful, to reclaim the disk space. In case of a deployment failure the cache is not deleted and the user may access it for debugging purposes, especially if using the **do not reboot** option in the project parameters and perform manual operations. • **Always**: The downloaded cache is always deleted, on success and on failure of any type.
Multicast Enabled	Indicates if the project data is transferred to the targets via multicast.
Mode	Defines which mode, *Multicast* or *Broadcast* , is to be used for the deployment. The default selection is *Multicast* . *Broadcast* is the easier mode as the user is not required to modify his infrastructure switch configuration. However, this option may slow down the network if it is used in a production environment instead of a dedicated subnet.
Packet Size (KB)	Defines the payload the multicast server is to send to the clients for each packet. The allowed values are between *0* and *64* KB, with a default of *64* KB. You can decrease the packet size for cases where its network reliability is low. This way the default performs at the maximum speed for most of the users with a standard network.

Parameter	Description
Proxy Access	Specifies if an internal tunnel should be used when using an OSD proxy. The OSD proxy may not have direct access to the share on which the WIM image is stored. This setting allows the OSD manager to stream the image to the proxy which in turn multicasts the file to the clients. To activate this option check the **Use Tunnel** box.
Read Ahead size (MB)	The number of chunks of data the multicast server collects in advance from the source file to be multicasted. The values are between 10 and 50, the default being 10. The higher the number, the more memory is used to cache these chunks.
Retry Count	Defines the number of consecutive retries the multicast server should attempt to communicate with a particular client after unsuccessful attempts before declaring it as failed and ignore it for the rest of the session. The default value is 50.
Retry Timeout (ms)	Defines the time in milliseconds for the multicast server to wait for an acknowledgement before the client failure counter is incremented. The possible value must be between 100 and 10000, the default being 200.
Packets to Send Ahead	Defines the number of packets to send in advance before waiting for the feedback on the first packet, which vastly increases the transfer efficiency on reliable networks. The available values range from 1 to 500. The better the network, the higher the number should be. The default value is set to 5 to work for the majority of cases. This represents a maximum value to reach; if the network is fast the value is not exceeded. The multicast server has an auto-adjust feature to lower the send ahead and avoid failures.
Max Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Automatic Start Conditions	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)** : The transfer automatically starts after the defined number of minutes after the connection of the first target to the server. • **Registered Targets** : The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions** : The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Registered Targets	Check this box if the session is to be automatically started after a certain number of clients have connected. If the timer condition is also set the session starts when the first of the two set conditions is fulfilled.
After (Min.)	Check this box if the transfer is to be automatically started after a certain amount of time after the first client connected to the server. Clients connecting after the beginning of the transfer join an automatically created new session which starts once the current session is over. If the count condition is also set the session starts when the first of the two set conditions is fulfilled.

The multicast server node of a project

A node exists for each OSD Server that executes multicast sessions of the project. It provides the following information in its dashboard:

Parameter	Description
Multicast Session Breakdown	This table displays information relative to the multicast session status situation.
Projects	The number of project sessions that are either planned, executing or finished their execution within this project.
Running	The session is executing.
Pending	The session is waiting for the previous one to terminate to be able to start executing.
Starting	The previous session terminated and the new session is starting its execution.

The following table provides some more detailed information:

Parameter	Description
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)**: The transfer automatically starts after the defined number of minutes after the connection of the first target to the server is established. • **Registered Targets**: The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions**: The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running*.

This section includes the following topics:

- Multicast server history
- Multicast Session

Multicast server history

The **History** dashboard provides an overview of the multicast status situation of the multicast server.

In addition to the preceding information, you will get access to the individual sessions and their information via a subnode for each of them.

The view provides the following summary:

Parameter	Description	
Multicast Session Breakdown	This table displays information relative to the multicast session status situation.	
	Projects	The number of project sessions that are either planned, executing or finished their execution within this project.
	Done	The session executed successfully.
	Failed	The session failed.
Status Breakdown	This pie chart displays the multicast server data, that are listed in the table to the left in form of a pie chart, that is, the number of deployment sessions that succeeded or failed.	

The following table provides some more detailed information:

Parameter	Description
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)**: The transfer automatically starts after the defined number of minutes after the connection of the first target to the server is established. • **Registered Targets**: The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions**: The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.

Parameter	Description
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running* .

Multicast Session

This node shows summary of the selected multicast transfer session:

Parameter	Description
Server Status	This field displays the general status of the Multicast transfer for all target devices together.
Failure Reason	In case of a session failure, this field displays an error message indicating as to the reason why it failed.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)**: The transfer automatically starts after the defined number of minutes after the connection of the first target to the server. • **Registered Targets**: The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions**: The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Project Name	The name of the deployment project of which the session is part.
Proxy	The short network name of the OSD server executing this session.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Max Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Total Size (MB)	The total size of the transfer.
Progress (%)	The progress of the transfer expressed as a percentage.
Creation Time	The date and time at which the multicast transfer session was created.
Start Time	The date and time at which the multicast transfer of the session was started.
End Time	The date and time at which the multicast transfer of the session was finished.

Parameter	Description
Last Update Time	The date and time at which the data of the multicast transfer of the session displayed in this view were last updated by the OSD Manager.
Average Speed (Mbps)	The average speed at which the deployment packets were transferred to the target.

The table below the dashboard provides the following information about the transfer to the individual devices that are part of the session:

Parameter	Description
MAC Address	The MAC address of the device.
IP Address	The IP address of the target.
Quarantine	Shows if the device is set in quarantine, possible values are **Yes** if quarantined or **No** otherwise.
Sent (%)	Shows the advancement of the transfer as a percentage. If the device has been set in quarantine, this is the size of the all data that were transferred before it was set in quarantine.
Update Time	The date and time at which the data of the multicast transfer of the session displayed in this view were last updated by the OSD Manager.
Register Time	The date and time at which the multicast transfer for this device was started.

For more information about using multicast session, see Operations on multicast sessions.

Operations on Multicast Session

The following operations can be performed on Multicast Session:

- Editing the multicast speed of a specific session
- Starting the multicast transfer of a specific session
- Canceling the multicast transfer of a specific session

Editing the multicast speed of a specific session

If you notice, that for example the transfer takes too much bandwidth you can modify the transfer rate.

1. Click **Edit** next to the **Max Speed (Mbps)** field.
   The **Properties** window appears.
2. Click the editable **Max Speed (Mbps)** drop-down list and select the desired value or manually enter it.
3. Click **OK** to confirm.

The new transfer rate will become effective immediately.

Note:

Be aware, that if you define different bandwidths for the target devices, devices with lower bandwidth might not be able to follow the pace. These devices will then be put in quarantine and another multicast session will be planned for them.

Starting the multicast transfer of a specific session

It is possible to start the multicast transfer to a specific device manually:

1. Select the device for which to start the transfer in the table to the right.
2. Click **Start** for in top right corner of the right window pane.
3. The transfer will be started immediately.

Canceling the multicast transfer of a specific session

It is possible to cancel the multicast transfer to a specific device:

1. Select the device for which to cancel the transfer in the table to the right.
2. Click **Cancel** for in top right corner of the right window pane.
3. The transfer will be stopped immediately.

Managing OSD multicast sessions

The OSD manager can deploy multiple operating systems to multiple computers and perform both tasks simultaneously. With the application of multicast transfer sessions the server can also deploy a single project to multiple targets with little impact on the performance.

This view provides you with access to the different aspects of all Multicast Servers:

- Multicast dashboard
- Options
- Multicast session history
- Multicast server

You can also directly access the individual servers, which are represented via a subnode each.

Multicast dashboard

The **Dashboard** provides an overview in graphical and tabular format over all registered multicast sessions. Registered sessions are in this case active or pending multicast transfers.

Parameter	Description
Multicast Session Breakdown	
Projects	The number of project sessions that are either planned, executing or finished their execution within this project.

Parameter		Description
	Running	The number of currently executing sessions.
	Pending	The number of currently pending sessions. Pending in this case means that the session starts as soon as the current session finishes if it is the next session in the queue.
	Waiting	The number of sessions currently waiting for devices to connect or the timer to finish. Once it is manually started by the user or the automatic threshold(s) are reached its status becomes Pending.
Status Breakdown		This pie chart displays the ratio of the status values of the table to the left.

The following table provides the following information on the sessions:

Parameter	Description
Proxy	The name of the Multicast Server on which sessions are executed for this project.
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running* .

Options

The **Options** tab provides access to the general Multicast settings. A number of these settings can be modified, but be aware that some of them then require a full rebuild. These settings are shared with all multicasted projects and applied to all sessions except if they are already started.

Parameter	Description
Address Range	This parameter is only applicable to the multicast mode. The multicast mode requires infrastructure specific configurations and such address range defined in the network hardware devices.
Cache Location	This parameter allows the user to manually select the partition where the cache is downloaded, or specify a path. It may be a driver letter, or **System** or **Automatic** . The default value is **Automatic** , which selects the partition with the largest - and writeable - free space available.
Client Port Range	Defines the port the multicast clients need to use to communicate with the server. This port could be arbitrary, but it is recommended to control this port by entering the requested value, by default 1610-1611 (UDP).
Client Timeout (ms)	The time in milliseconds for each multicast client to wait any packet from the server before declaring the server offline and terminating with an error.

Parameter	Description
Delete Cache	Defines if and when the downloaded material is deleted on the client. The following values are available: • **Never** : The downloaded cache is never deleted and thus always available to the user if the deployment succeeds. This may be used for local system recovery, especially if using a setup installation. • **On Success** : The downloaded cache is only deleted if the deployment is successful, to reclaim the disk space. In case of a deployment failure the cache is not deleted and the user may access it for debugging purposes, especially if using the **do not reboot** option in the project parameters and perform manual operations. • **Always** : The downloaded cache is always deleted, on success and on failure of any type.
History	Defines the total number of days of completed sessions to be kept in the database for the user to look back, including connected devices by MAC address and status. Sessions are removed by order of completion past the defined amount of time. The default value is set to 30 days, the minimum is 1 and maximum 99.
Mode	Defines which mode, *Multicast* or *Broadcast* , is to be used for the deployment. The default selection is *Multicast* . *Broadcast* is the easier mode as the user is not required to modify his infrastructure switch configuration. However, this option may slow down the network if it is used in a production environment instead of a dedicated subnet.
Packet Size (KB)	Defines the payload the multicast server is to send to the clients for each packet. The allowed values are between *0* and *64* KB, with a default of *64* KB. You can decrease the packet size for cases where its network reliability is low. This way the default performs at the maximum speed for most of the users with a standard network.
Proxy Access	Specifies if an internal tunnel should be used when using an OSD proxy. The OSD proxy may not have direct access to the share on which the WIM image is stored. This setting allows the OSD manager to stream the image to the proxy which in turn multicasts the file to the clients. To activate this option check the **Use Tunnel** box.
Read Ahead size (MB)	The number of chunks of data the multicast server collects in advance from the source file to be multicasted. The values are between 10 and 50, the default being 10. The higher the number, the more memory is used to cache these chunks.
Retry Count	Defines the number of consecutive retries the multicast server should attempt to communicate with a particular client after unsuccessful attempts before declaring it as failed and ignore it for the rest of the session. The default value is 50.
Retry Timeout (ms)	Defines the time in milliseconds for the multicast server to wait for an acknowledgement before the client failure counter is incremented. The possible value must be between 100 and 10000, the default being 200.
Packets to Send Ahead	Defines the number of packets to send in advance before waiting for the feedback on the first packet, which vastly increases the transfer efficiency on reliable networks. The available values range from 1 to 500. The better the network, the higher the number should be. The default value is set to 5 to work for the majority of cases. This represents a maximum value to reach; if the network is fast the value is not exceeded. The multicast server has an auto-adjust feature to lower the send ahead and avoid failures.
Multicast Server Port (UDP)	This parameter determines on which port the multicast server should listen and to which port the clients should send their requests and acknowledgements. It is only available in the general configuration, not on project level. Modifying this parameters requires restarting the multicast server and, to be correctly applied, restarting all related OSD agents as well. In addition all projects need to be rebuilt if this parameter is modified as it is embedded during the WinPE ISO image build. The default would be the agent port in UDP, typically 1610.
Max Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.

Parameter	Description
Automatic Start Conditions	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)** : The transfer automatically starts after the defined number of minutes after the connection of the first target to the server. • **Registered Targets** : The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions** : The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Registered Targets	Check this box if the session is to be automatically started after a certain number of clients have connected. If the timer condition is also set the session starts when the first of the two set conditions is fulfilled.
After (Min.)	Check this box if the transfer is to be automatically started after a certain amount of time after the first client connected to the server. Clients connecting after the beginning of the transfer join an automatically created new session which starts once the current session is over. If the count condition is also set the session starts when the first of the two set conditions is fulfilled.

Multicast session history

The **History** displays the list of all completed multicast sessions on all existing OSD Managers, successful or not. This allows the administrator to visualize the status of each computer connected to the session and its completion state and makes it possible to identify issues with computers or sessions. Double-clicking any entry will navigate to the session under the relevant history node.

It provides the following information:

Parameter	Description
Completion Date	The date and time at which the session terminated, successful or not.
Proxy	The name of the Multicast Server on which sessions are executed for this project.
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Status	The current status of the multicast transfer, which is typically one of the following: Done or Failed.

Multicast server

A node exists for each OSD Server that executes multicast sessions of the project. It provides the following information about all its active sessions in its dashboard:

Parameter		Description
Multicast Session Breakdown		This table displays information relative to the multicast session status situation.
	Projects	The number of project sessions that are either planned, executing or finished their execution within this project.
	Running	The number of currently executing sessions.
	Pending	The number of currently pending sessions. Pending in this case means that the session starts as soon as the current session finishes if it is the next session in the queue.
	Waiting	The number of sessions currently waiting for devices to connect or the timer to finish. Once it is manually started by the user or the automatic threshold(s) are reached its status becomes Pending.

The following table provides some more detailed information:

Parameter	Description
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)** : The transfer automatically starts after the defined number of minutes after the connection of the first target to the server is established. • **Registered Targets** : The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions** : The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running* .

For more information about using multicast server node, see the following topics:

- Proxy server multicast history

- Session history

Proxy server multicast history

The **History** displays the complete list of all multicast sessions completed by the selected proxy server.

In addition to the preceding information you will get access to the individual sessions and their information via a subnode for each of them.

This dashboard provides the following summary:

Parameter		Description
Multicast Session Breakdown		This table displays information relative to the multicast session status situation.
	Projects	The number of project sessions that are either planned, executing or finished their execution within this project.
	Done	The session executed successfully.
	Failed	The session failed.
Status Breakdown		This pie chart displays the multicast server data, that are listed in the table to the left in form of a pie chart, that is, the number of deployment sessions executed on this server that succeeded or failed.

The following table provides some more detailed information:

Parameter	Description
Session	The automatically generated user friendly name of the multicast session.
Project Name	The name of the project for which this session is executed.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)** : The transfer automatically starts after the defined number of minutes after the connection of the first target to the server is established. • **Registered Targets** : The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions** : The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Maximum Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Overall Progress (%)	The overall progress expressed as a percentage of the multicast sessions that are currently executing or already executed for this project on this server.

Parameter	Description
Status	The current status of the multicast transfer, which is typically one of the following: *Waiting, Pending, Starting* or *Running* .

Session history

The **History** displays the complete history of the selected multicast session and its targets.

Parameter	Description
Server Status	This field displays the general status of the Multicast transfer for all target devices together.
Failure Reason	In case of a session failure, this field displays an error message indicating as to the reason why it failed.
Start Mode	Defines the start condition for a transfer. The following values are available: • **None** (clear both check boxes): No automatic start. The transfer can only be started manually through the **Start** button. • **After (Min.)** : The transfer automatically starts after the defined number of minutes after the connection of the first target to the server. • **Registered Targets** : The transfer automatically starts once the defined number of targets are connected to the server. • **Both conditions** : The transfer automatically starts when either the defined number of machines are connected or the defined number of minutes after the first targets connected to the server are reached, whichever comes first.
Project Name	The name of the deployment project of which the session is part.
Proxy	The short network name of the OSD server executing this session.
Interface	The IP address of the OSD server or its local interface on which the multicast is transferring on.
Max Speed (Mbps)	Defines the maximum speed network allowed in megabit per second (Mbps). The default value is *0* , which means the speed is adapted according to the conditions. The speed is re-estimated on a regular basis or if packets start to fail. You may adjust this parameter during a transfer.
Total Size (MB)	The total size of the transfer.
Progress (%)	The progress of the transfer expressed as a percentage.
Creation Time	The date and time at which the multicast transfer session was created.
Start Time	The date and time at which the multicast transfer of the session was started.
End Time	The date and time at which the multicast transfer of the session was finished.
Last Update Time	The date and time at which the data of the multicast transfer of the session displayed in this view were last updated by the OSD Manager.

Parameter	Description
Average Speed (Mbps)	The average speed at which the deployment packets were transferred to the target.

The table below the dashboard provides the following information about the transfer to the individual devices that are part of the session:

Parameter	Description
MAC Address	The MAC address of the device.
IP Address	The IP address of the target.
Quarantine	Shows if the device is set in quarantine, possible values are **Yes** if quarantined or **No** otherwise.
Sent (%)	Shows the advancement of the transfer as a percentage. If the device has been set in quarantine, this is the size of the all data that were transferred before it was set in quarantine.
Update Time	The date and time at which the data of the multicast transfer of the session displayed in this view were last updated by the OSD Manager.
Register Time	The date and time at which the multicast transfer for this device was started.

Editing the Multicast Speed of a Specific Session

If you notice, that for example the transfer takes too much bandwidth you can modify the transfer rate.

1. Click **Edit** next to the **Max Speed (Mbps)** field.
   The **Properties** window appears.
2. Click the editable **Max Speed (Mbps)** drop-down list and select the desired value or manually enter it.
3. Click **OK** to confirm.

The new transfer rate will become effective immediately.

> **Note:**
>
> Be aware, that if you define different bandwidths for the target devices, devices with lower bandwidth might not be able to follow the pace. These devices will then be put in quarantine and another multicast session will be planned for them.

osd_serverhistory_session_stop_title

osd_serverhistory_session_start_title

Creating an OSD PXE Menu

A PXE boot menu is a menu displayed on the target screen in which you can select which of a number of projects should be executed on the local device. The list of projects to select from are the projects currently on line and therefore immediately available. You can access the menu's parameters and definitions in its tabs.

The following topics are provided:

- The PXE menu General tab
- The Items tab
- Creating a PXE Boot Menu

The PXE menu General tab

The node of a PXE menu provides access to the menu's parameters and its values.

The **General** tab of this node displays the following information about the currently selected PXE menu:

Parameter	Default Value	Description
Menu Name	**New PXE Menu**	The title of the project that is displayed in the PXE menu.
Scope	1.1.1.*	Enter the IP address range of the targets which are to use this menu in the format of *94.24.127.** .
Timeout (sec)	30	Enter the amount of time the menu is displayed on the target screens in seconds before automatically starting with the default selection.
Status	**No**	This value shows if the menu is activated, that is, if it is online and can be used for deployment.

The Items tab

The PXE boot menu items are all those projects, active and inactive that are assigned to the boot menu.

A PXE Boot Menu provides the user with the choice of projects from which he can select the one to use for the local installation. Projects that are currently offline are not displayed in this view. When an offline project comes online, it is dynamically enabled in the menu and appear in this view.

The following information is provided for the assigned projects:

Parameter	Description
Name	The name of the project as it is defined under the **Projects** node.
Project Name	The title of the project that is displayed in the PXE menu.
Description	The project description that is displayed when the project title is selected in the PXE menu. This field is optional.

Parameter	Description
Status	This value shows if the menu is activated, that is, if it is online and can be used for deployment.
Default	Indicates which of the assigned projects is the default selection of the menu. The default project is marked via the green check sign.

Creating a PXE Boot Menu

To create a new PXE boot menu proceed as follows:

1. Go to **OS Deployment > PXE Menus** .
2. Select **Edit > Create Menu**
   The **Create a New PXE Boot Menu** dialog box appears.
3. Enter an explicative name for the new menu in the **Menu Name** box.
4. Enter the subnet mask into the **Scope** box.
5. Modify the time value if the menu is to be displayed longer or shorter on the target screen than defined by default in the **Display Time (sec)** box.
6. Change the value of the **Enabled** box to **Yes** if the new menu is to be activated right away.
7. Click **OK** to confirm.

The new PXE boot menu is created right away and added to the list of available menus.

Managing OS Deployment via the wizards

OS Deployment can be executed via a number of different ways. The operating system deployment functionality only has one wizard, the **OS Deployment** that, however, executes all available deployment types, that is, different ways to deploy the operating system and the possibility to create a WIM capture of such a system. The following different types of deployment are available:

1. **OS Deployment**
   - **Setup Mode**
   - **WIM Image Mode**
   - **Custom Mode**
2. **WIM Image Capture**

This topic displays all the different possibilities the wizard offers for operating system deployment.

1. From anywhere in the console select the **Wizards > OS Deployment** menu item.
2. The wizard appears with its first window.

All different types of deployment require the selection and configuration of the OSD Manager before any operation can be executed. This is the same for all types and is done in the first two windows of the **OS Deployment Wizard** . Whenever an already configured OSD Manager is used its values are prepopulated into these two windows.

This section includes following topics:

Selecting and adding the OSD Manager

The following topics guide you through selecting and adding OSD Manager

Selecting the OSD Manager

This window defines the device that is to act as the OSD Manager for the project to be defined. This can either be an OSD Manager that is already defined or a new OSD Manager that you define additionally.

The list in this window appears all devices that were defined as OSD Managers.

1. Select the OSD Manager device which is to execute the OSD project that is being defined via the wizard.
2. Click **Next** to go to the following wizard page.

The following topic provides information about adding an OSD Manager:

Adding an OSD Manager

To add a device as the OSD Manager proceed as follows:

1. Select **Add Device** on top of the list box.
   The **Add a new OSD Manager** pop-up menu displays displaying the list of all devices that can be OSD Manager due to their operating system.
2. Select the device to be added from one of the list boxes.
3. Click **OK** to confirm and close the window.

The device will be added to the table of OSD Managers and its configuration parameter will be updated.

Configuring and modifying the configuration of OSD Manager

The following topics guide you through configuring and modifying the OSD Manager:

- Configuring the OSD Manager
- Modifying the OSD Manager configuration

Configuring the OSD Manager

The second wizard window allows you to specifically configure the OSD Manager.

1. Enter the name of the new OSD Manager into the **Name** box.
2. Now enter all other required values into the respective boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** `OK - Initialization Complete` , the wizard cannot continue. If errors occur during the parameter verification, the wizard will highlight the respective boxes in red.

3. To verify click **Check Environment** to the right of the **Status** box.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directories and the access rights to them and the DHCP server address if it is installed on another device. If all values are correct the **Status OK** is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
4. After the **Status OK** is returned click **Next** to go to the following wizard page.

> **Note:**
>
> Be aware that the first initialization will take several minutes.

Modifying the OSD Manager configuration

To modify the configuration of the OSD Manager proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Configuration** in the left window pane.
2. Select **Edit > Properties**
   The **Properties** window appears.
3. Make the desired changes in the respective boxes.

After you made all required modifications they must be checked that they are correct. Until the verification is executed and returns the **Status** `OK - Initialization Complete` , the wizard cannot continue. If the wizard finds an issue during the verification it will highlighted the concerned box(es) in red.

4. Click **Check Environment** to the right of the **Status** box to verify your changes.

BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directories and the access rights to them and the DHCP server address if it is installed on another device. If all values are correct the **Status** OK is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.

5. Click **OK** to confirm the changes and close the window.

Any changes made are saved and applied to the OSD Manager.

Specifying the deployment type

In the third wizard window you need to select which type of deployment is to be executed. The following types of OS deployment are available:

- - **Setup Mode**
    Using the setup mode allows you to execute a regular installation of the operating system on the remote devices or targets via the operating system's setup executable file. The use of an unattended file makes the installation silent and automatic. This is also the preselected option.
  - **WIM Image Mode**
    The WIM mode allows you to deploy the new operating systems or images of other non-booting disks to the targets via a WIM image, that is either delivered on the operating system disk or via a custom created WIM image. This mode can only be used if the target hardware is compatible to the hardware of the source device.
  - **Custom Mode**
    This mode allows you to use other applications with which snapshots of existing installations can be created and then be "duplicated" on other devices, such as for example ghost images.
- **WIM Image Capture**
  The WIM capture mode allows you to create your own WIM images to be deployed via the WIM mode within your network. You can also use this mode create images of other, non-booting disks, such as drives that contain only applications or data and deploy these via the WIM mode to other devices within your infrastructure.

1. Select the radio button of the desired option.

2. Click **Next** to go to the following wizard page.

Defining the project parameters

The deployment of a new operating system to a number of targets is managed in its entirety by a CM object called project.

1. Enter the name of the new project into the **Name** box.
2. Select the architecture type the project is to apply to from the **Architecture** drop-down list.
3. Select the type of BIOS mode supported by the project, that is, if it is to support UEFI or legacy deployments or both.
4. Select if an operation is required after the installation has finished by selecting the corresponding value from the **Operation after Installation** drop-down list.
5. Select the driver letter for the drive on which the new OS is to be installed.

   > For a custom deployment this list box is used to configure the MBR file. It is accessible, HOWEVER, only to modify the prepopulated value if required.

6. Check the **Disable Automated Driver Detection** box if you want to manually add the required drivers.
7. Clear the **Use Model Drivers** box if you do not want to use the model drivers drivers.
8. Check this box if the operating system deployment to the targets is to be effected via Multicast.
9. This parameter allows the user to manually select the partition where the cache is downloaded, or specify a path. It may be a driver letter, or **System** or **Automatic** . The default value is **Automatic** , which selects the partition with the largest - and writeable - free space available.
10. Defines if and when the downloaded material is deleted on the client. The following values are available:
    - **Never**: The downloaded cache is never deleted and thus always available to the user if the deployment succeeds. This may be used for local system recovery, especially if using a setup installation.
    - **On Success**: The downloaded cache is only deleted if the deployment is successful, to reclaim the disk space. In case of a deployment failure the cache is not deleted and the user may access it for debugging purposes, especially if using the **do not reboot** option in the project parameters and perform manual operations.
    - **Always**: The downloaded cache is always deleted, on success and on failure of any type.
11. Click **Next** to go to the following wizard page.

Editing the multicast options

The deployment of a new operating system to the targets can be executed via multicast. This view provides the multicast parameter default values, which can be modified if required for this specific deployment.

If you are modifying an existing project via this window be aware, that a complete rebuild of the project is required if the parameters marked with an asterisks (*) are modified.

1. If required you can change the multicast mode to broadcast in the **Mode** field.

   > Be aware, that this option might slow down the network if it is used in a production environment instead of a dedicated subnet.

2. Make modifications to the speed, count timeout, size and packages values if required.
3. By default both **Automatic Start Conditions** are activated. Deselect the undesired option if only one is required and modify the number value according to your requirements or uncheck both if you want to manually start the multicast sessions.
4. Check the **Use Tunnel** option if you want to use an internal tunnel for the multicast transfer.

   > The **Use Tunnel** option is only applicable if you are using an OSD Proxy.

5. Check the **Disable Automated Driver Detection** box if you want to manually add the required drivers.
6. Modify the cache parameters if necessary.
7. Click **Next** to go to the following wizard page.

Selecting the image

This window defines the image to be used for the project. You can either select an existing or create a new operating system image which is to be deployed by the setup. Images exist for all types of deployment, but the list displayed in this window is already filtered and will only show the images created for the respective selected deployment type.

- Leave the preselected **Create a new OS image or setup** option to create a new image. Then click **Next** to go directly to the following wizard page to define the parameters of the new image.
- Select the **Use existing image** option to use an already existing image. In this case, the images available for the selected type of deployment will be displayed in the following list field. Select the desired image. Click **Next** and continue directly with step OS Drivers.

Defining the image parameters

In this next window, the parameters for the image must be defined. It will only be displayed for a new image.

1. Enter the name of the new image into the **Name** box.
2. Select the architecture type the project is to apply to from the **Architecture** list.
3. Select the type of BIOS mode supported by the project, that is, if it is to support UEFI or legacy deployments or both.
4. Select the type of image to create from the **Type** drop-down list.
5. Enter the network path to the image or setup folder, where you copied the image files required for the installation, for example, `\\192.168.196.13\Vista32` into the **Location** box.
6. Enter the login and password to be used by the deploying device to access the network location in read and write mode into the **Connection Parameters** boxes.
7. After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status OK** , the wizard cannot continue.
8. To verify click **Check Image** to the right of the **Status** box.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directory and the access rights to it.
9. If all values are correct the **Status OK** is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
10. After the **Status OK** is returned click **Next** to go to the following wizard page.

Selecting the OS drivers

This window is only applicable to a Setup Deployment or a Sysprep WIM Image Deployment.

In this step of the OSD wizard, the drivers must be defined which will be used by the Windows Setup after installation or that are required by the Sysprep installation. This is the equivalent for manually inserting the drivers floppy during the installation process. Here you can define all drivers that might be needed by the deployment operating system to properly run. The drivers must be defined here as well in their usual .inf format. If you are creating an XP setup and your targets use a SATA disk, do not forget to add the required SATA driver here as well.

By default no drivers are predefined, therefore this list box is empty. To add a driver, for example, an Ethernet network driver proceed as follows:

1. Click the **Create Driver** icon above the list box.
   The **Create a New Driver** window appears.
2. Enter the required data into the respective boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** OK, the wizard cannot continue.

3. To verify click **Check Driver** to the right of the **Status** box.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directory and the access rights to it and fill in the remaining boxes with the recovered information, such as the list of driver files. If all values are correct the **Status OK** is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
4. After the **Status OK** is returned click **OK** to add the new driver to the list and return to the **OS Drivers** window.
   Now the driver displays in the list of available drivers.
5. Repeat these steps to add other drivers. The drivers defined here must be compliant with the image to be deployed.
6. Select the required driver(s) in the list.
7. Click **Next** to go to the following wizard page.

Selecting the drivers by model

This window is only applicable to a Setup Deployment or a Sysprep WIM Image Deployment.

In this step of the OSD wizard, the drivers must be defined which will be used by the Windows Setup after installation or that are required by the Sysprep installation. This is the equivalent for manually inserting the drivers floppy during the installation process. Here you can define all drivers that might be needed by the deployment operating system to properly run. The drivers must be defined here as well in their usual .inf format. If you are creating an XP setup and your targets use a SATA disk, do not forget to add the required SATA driver here as well.

By default no drivers are predefined, therefore this list box is empty. To add a driver, for example, an Ethernet network driver proceed as follows:

1. Click the **Create Driver** icon above the list box.
   The **Create a New Driver** window appears.
2. Enter the required data into the respective boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status** OK, the wizard cannot continue.

3. To verify click **Check Driver** to the right of the **Status** box.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directory and the access rights to it and fill in the remaining boxes with the recovered information, such as the list of driver files. If all values are correct the **Status OK** is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.

4. After the **Status OK** is returned click **OK** to add the new driver to the list and return to the **OS Drivers** window.
   Now the driver displays in the list of available drivers.
5. Repeat these steps to add other drivers. The drivers defined here must be compliant with the image to be deployed.
6. Select the required driver(s) in the list.
7. Click **Next** to go to the following wizard page.

Configuring the target list

The next step in the OS deployment procedure is to select the deployment targets. Targets are not defined via groups, because these can only contain devices with a CM agent installed, they are managed via target lists, which can also contain devices without a CM agent . The individual targets are then added to these lists. This can be done in a number of different ways. In our example here we will only have one target device which will be added as a single device.

- Leave the preselected **Create a new target list** option to create a new image. Then click **Next** to go directly to the following wizard page to define the members of the new target list.
- Select the **Use existing target list** option to use an already existing list. In this case the target lists available for the selected type of deployment will be displayed in the following list field. Select the desired list. Click **Next** and continue directly with step [MBR Disk Configuration|MBR Disk Configuration] or [GPT Disk Configuration|GPT Disk Configuration] .

> **Note:**
>
> A target list can only be assigned to one project at a time. To use it with another project and have it be available in this list it must first be unassigned from its current project.

Defining target list

In this step of the wizard the deployment targets which are collected in the target list must be defined.

1. Enter name of the new target list into the **Name** box.
2. Select the architecture type the project is to apply to from the **Architecture** list.
3. Enter the path to the template of the unattended file that is to be used for the deployment into the **Vista Unattend File Template** box.
   a. To select the file click **Select** to the right.

b. A file manager window appears in which you can select the path to the desired file. You can either use the template which is provided by BMC Client Management - Software Distribution , which will be used in any case if the text box is left empty, or you can use you own custom defined file. If you use your own customized `Unattend.xml` file make sure it is in UTF-16 encoding.

> If you are using your own customized unattended file, make sure it is in UTF-16 encoding.

4. Devices can be added as targets in a number of different ways, depending on the type of deployment selected. Be aware that the target list for a **WIM Image Capture** can only contain one single device.

The following topics describe operations performed on Target List:

- Creating a target
- Adding a new target to a target list
- Adding an existing target to a target list

Creating a target

You can also create target devices by individually specifying their data or by specifying a subnet. Only one subnet per target list can be defined. When creating a new target in this way, it is added to the OS Deployment database specifically for this deployment.

To create a new target proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. **Edit > Create Target** .
   The **Create a New Target** window appears with its three tabs, **General Information** , **Parameters** and **Unattended Information**.
3. Enter the desired information into the respective boxes.

> Select the PXE Menu radio button, if the project is to be assigned to a PXE menu. In this case you cannot define a subnet, the PXE menu will take care of this.

4. Click **OK** to add the target device and close the window.

A new target for the selected target list was created.

Adding a new target to a target list

Devices can be added to the list of targets through a number of different ways. One is through different types of lists.

To add a target to a target list proceed as follows:

1. Select **OS Deployment> Your OSD Manager> Target Lists> Your Target List** in the left window pane.
2. Click **Edit> Add Targets**
   The **Select Devices from the List** window appears providing you with different methods to select the targets.

Select a method to add a target:

Method	Description / Steps
AutoDisc Object	The AutoDiscovery module provides a list of all devices of any type found in the network, such as printers or devices with and without the agent installed. However, the list displayed in this case will only show all clients of type device and only those with a status of Verified or Learned, which means that all devices in this list were verified for existence either by the local client or a neighbor client and exist on the network. To add a device from the list of all autodiscovered devices known to the database proceed as follows: 1. a. Select the **AutoDisc Object** tab in the left window bar. The **Available Devices** box appears the list of all available devices. You will find more information about the list of autodiscovered devices in the main manual. b. Select the device/devices to be added as targets from the list. c. Click **Add** to move the selected devices to the list of **Selected Devices**. d. Click the **OK** to confirm the selections and close the window.
AutoDisc Device	The tab AutoDisc Device allows you to select your target devices from a list of autodiscovered devices by one specific network device. Proceed as follows: 1. a. Select the **AutoDisc Device** tab in the left window bar. The Select a Device window appears. b. Select the device of which the autodiscovered list is to be used from one of the tabs of the **Select a Device** dialog box. c. Click **OK** to confirm the selection and close the window. The **Select Devices from the List** dialog box now only displays the devices that were discovered by the selected network device. d. Select the device/devices to be added as targets from this list. e. Click **Add** to move the selected devices to the list of **Selected Devices**. f. Click the **OK** to confirm the selections and close the window.
Network	You can add a device from the list of your Microsoft network neighborhood. To do so, proceed as follows:

Method	Description / Steps
	a. Select the **Network** tab in the left window bar. The box **OK** displays the **Microsoft Windows Network Neighborhood** structure on the screen. b. Select the device/devices to be added to the list from one of its groups. c. Click the **OK** to confirm the selections and close the window.
CSV List	To add a device to the deployment from an existing .csv file proceed as follows: 1. a. Select the **CSV List** tab in the left window bar. The **Open** window appears, in which you need to select the file containing the device list. b. Navigate to the desired .csv file and click **Open** at the bottom of the window. The box **Available Devices** displays now the list of all devices contained in the selected CSV list. c. Check the **Header** box, if your CSV file has a title line which is to be removed. d. Select the device to be added to the deployment from the list in the window. You can also select all devices in the list by using **Select All**. e. Click the OK to confirm the selections and close the window.

The selected target device(s) will be added to the selected target list.

Adding an existing target to a target list

This is the easiest way to add a device to the target list if you deploy only to devices that are already known to the CM database. Devices without agents are not available in this window, that is, devices that have not yet been scanned and added as unconnected devices.

To add an existing target to a target list, proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Target Lists > Your Target List** in the left window pane.
2. Select **Edit > Add Device** .
   The **Select a Device** window appears.
3. Select the device to be added from one of the tabs in the window's sidebar.
4. Click **OK** to confirm.

The selected device was added to the target list.

Specifying an MBR disk configuration

This wizard window allows you to define the configuration of the disk on which the operating system will be installed for legacy installations. A number of disk configurations are predefined for these cases and are made available. They are ready for use with all of the deployment types for legacy installations.

1. Select the desired disk configuration for the project.
2. Click **Next** to go to the following wizard page.

> Be careful not to select a disk configuration that will format the drive or partition for a **WIM Image Capture** .

You can execute following operations on MBR disk configuration.

- Creating a new disk configuration
- Creating a disk configuration
- Modifying a partition

Creating a new disk configuration

If none of the predefined disk configurations answer the requirements of your distribution you can create a new disk configuration. Creating new disk configurations consists of the following two steps:

1. Create a new disk configuration
2. Create partitions for the new configuration

> **Note:**
>
> Be aware that WinPE has a number of limitation as described on the Microsoft website (http://technet.microsoft.com/en-us/library/cc507857.aspx) such as the fact that drive letter assignments are *not* persistent between sessions. This means that no matter which drive you assigned specific drive letter in the disk configuration of an OS deployment, the drive letter assignments will be in the default order after WinPE is restarted.

Creating a disk configuration

To create a new disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration** in the left window pane.
2. Select **Edit > Create Disk Configuration**
3. Enter the necessary data for the parameters in the **Create a New Disk** window:

Parameters	Description
Name	A descriptive name of the object.
Description	This is a free text field into which you can enter any type of description and information that is pertinent to the new disk configuration.
Size (GB)	The size of the disk. It is only used to estimate if the partitions overall size is sensible. It has no impact on the real disk.
Delete Disk Partitions	Defines if any partitions that already exist on the target device are deleted. This option should be used with caution, as any data on the disk is lost irretrievably if selected.
Partition Type	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, etc.
Status	Before the disk configuration can be created it must be verified that all entered data is correct. To execute a check on the disk click Test next to the non-editable Status box. Be aware that the disk creation cannot be confirmed until the disk verification succeeded, that is, the status value OK is displayed.
Notes	This free text field can contain additional information concerning the selected object.

4. Click **OK** to confirm the data for the new disk configuration.

The new disk configuration with the specified data is created.

Modifying a partition

1. Select the partition to edit in the list.
2. Click **Properties** .
3. Click **Yes** in the appearing **Warning** window.
4. Select the partition which you want to modify in the partition properties window.
5. Make the necessary modifications by selecting the respective icon above.
6. Click **OK** to confirm the modifications.

Your modifications of the parameters were saved and applied to the selected partition.

Specifying a GPT disk configuration

This wizard window allows you to define the UEFI configuration of the disk on which the operating system will be installed. A number of disk configurations are predefined for these cases and are made available. They are ready for use with all of the deployment types for UEFI installations.

1. Select the desired disk configuration for the project.
2. Click **Next** to go to the following wizard page.

> Be careful not to select a disk configuration that will format the drive or partition for a **WIM Image Capture** .

The following topics describe the operations performed on GPT Disk Configuration:

- Creating a new disk configuration
- Creating a disk configuration
- Modifying a partition

Creating a new disk configuration

If none of the predefined disk configurations answer the requirements of your distribution you can create a new disk configuration. Creating new disk configurations consists of the following two steps:

1. Create a new disk configuration
2. Create partitions for the new configuration

> **Note:**
>
> Be aware that WinPE has a number of limitation as described on the Microsoft website (http://technet.microsoft.com/en-us/library/cc507857.aspx) such as the fact that drive letter assignments are *not* persistent between sessions. This means that no matter which drive you assigned specific drive letter in the disk configuration of an OS deployment, the drive letter assignments will be in the default order after WinPE is restarted.

Creating a disk configuration

To create a new disk configuration proceed as follows:

1. Select **OS Deployment > Your OSD Manager > Disk Configuration** in the left window pane.
2. Select **Edit > Create Disk Configuration** .
3. Enter the necessary data for the parameters in the **Create a New Disk** window:

Parameters	Description
Name	A descriptive name of the object.
Description	This is a free text field into which you can enter any type of description and information that is pertinent to the new disk configuration.
Size (GB)	The size of the disk. It is only used to estimate if the partitions overall size is sensible. It has no impact on the real disk.
Delete Disk Partitions	Defines if any partitions that already exist on the target device are deleted. This option should be used with caution, as any data on the disk is lost irretrievably if selected.
Partition Type	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, etc.

Parameters	Description
Status	Before the disk configuration can be created it must be verified that all entered data is correct. To execute a check on the disk click Test next to the non-editable Status box. Be aware that the disk creation cannot be confirmed until the disk verification succeeded, that is, the status value OK is displayed.
Notes	This free text field can contain additional information concerning the selected object.

4. Click **OK** to confirm the data for the new disk configuration.

The new disk configuration with the specified data is created.

Modifying a partition

1. Select the partition to edit in the list.
2. Click **Properties** .
3. Click **Yes** in the appearing **Warning** window.
4. Select the partition which you want to modify in the partition properties window.
5. Make the necessary modifications by selecting the respective icon above.
6. Click **OK** to confirm the modifications.

Your modifications of the parameters were saved and applied to the selected partition.

Selecting the deployment drivers

In this step of the OSD wizard, the drivers required for the WinPE must be selected. For the deployment to work at least one driver must be selected, that is, the network driver, and the SATA driver if the target disk is a SATA disk. By default no drivers are predefined, therefore this list box is empty.

To add a new WinPE driver, for example, an Ethernet network driver, proceed as follows:

1. Click **Create Driver** above the list box.
   The **Create a New Driver** window appears.
2. Enter the required data into the respective boxes.

> After all parameters are defined they must be checked that they are correct. Until the verification is executed and returns the **Status OK** , the wizard cannot continue.

3. To verify click **Check Driver** to the right of the **Status** box.
   BMC Client Management - Software Distribution will now verify all entries of this page, that is, the directory and the access rights to it and fill in the remaining boxes with the recovered information, such as the list of driver files. If the driver is a valid deployment driver the box **Deployment Driver** displays a green **Yes**.

> **Note:**

> If the box **Deployment Driver** displays a red **No** , the driver might be a valid driver but not a deployment driver. If you click **OK** nevertheless the driver will be created but it will not appear in this view, because it was added to the available image drivers.

4. If all values are correct the **Status OK** is returned, otherwise an error message displays in the **Status** box indicating where the parameter value is not correct.
5. After the **Status OK** is returned click **OK** to add the new driver to the list and return to the **Deployment Drivers** window.
6. Now the driver displays in the list of available drivers.
7. Repeat these steps to add a SATA driver if you are using a SATA disk, be aware that also the SATA drivers must be Windows 7 compliant.
8. Then in the **Deployment Drivers** window mark both check boxes next to the added drivers to indicate that they are to be used.
9. Click **Next** to go to the following wizard page.

You can execute following operations on drivers:

Modifying a driver

1. Select **OS Deployment > Your OSD Manager > Drivers** in the left window pane.
2. Select the desired driver in the left window pane.
3. Select **Edit > Properties** .
   The **Properties** window appears.
4. Make the desired modifications in the respective boxes.
5. Click **Check Driver** to the right of the **Status** box.
6. If the **Status** box displays:
   a. Click **OK** at the bottom of the window to confirm the modifications.
   b. Anything other than **OK** , reverify your modifications for errors and repeat steps 5 and 6.

Your modifications were saved and applied to the selected driver.

Selecting drivers by tag

1. Click **Select drivers by Tag** .
2. In the **Select drivers by Tag** window select the required drivers.
3. Click **OK** to confirm.

The selected drivers are added to the project.

Defining the PXE menu parameters

This step allows you to add the new project to a PXE start menu to make it available whenever this menu is used on the subnet.

> **Note:**
>
> If you defined a target list for this project it is ignored if you add it to a PXE menu. In this case ONLY the subnet mask defined for the menu will be applied.

1. Check the **Add the project to the PXE start menu** box.
2. Enter the item name under which the current project will appear in the menu, for example, *Windows XP Dell GX280*.
3. Select the menu to which to add it from the following list.
4. Click **Next** to continue.

Specifying the project build date

In the last step of the operating system deployment wizard, the schedule for the project build and its activation is defined. Building the project signifies to check that all parameters and values of the project are correct and that all required elements are available and in their correct location.

There are the following build schedule possibilities:

- Either schedule the build immediately, this is also the default selection.
- Postpone the build to a specific date. In this case select the **Deferred to** radio button. The two time boxes to the right will become available. Enter the desired date and time in the respective boxes. Click the arrow in the drop-down box next to the **Deferred to** box for the calendar to pop-up. Select the date for the project to be built. Then, in this following list box select the assign time from the list. You can modify the minute value by selecting the :00 and modify it to your needs, for example, 12:30 to launch the assignment at this time.
- Activate
  For a project to become available for deployment or WIM Capture it must be activated. By default this option is checked in the wizard.

> **Note:**
>
> Be aware that only one project per OSD Manager at a time can be active. If you have more than one deployment project you must schedule them in such a way that they are not launched at the same time and that the first deployment has finished before the next one starts, that is, that they are not active at the same time. It is however possible to execute simultaneous deployments via different OSD Managers in different subnets. If you activate a new project via this wizard any other project in the same subnet will automatically be deactivated.

> **Note:**

In case of a Sysprep **WIM Image Capture** , the target *must* be running before the project becomes active! Also, you must manually launch the provided batch file `//OSD Manager/PXETFTP/SYSPREP/RUNSYSPREP.BAT` , that will sysprep the target and finally reboot it. The file must be executed as a privileged user (admin), on Windows Vista and above, the file must be executed using "Run As Administrator" even if the user belongs to the administrator group. If the file cannot be found in this location the project is not activated or not set as a Sysprep image type.

Click **Finish** to either launch the project build or confirm the project and its schedule.

Distributing software

With the average organization possessing dozens of business applications, the process of deploying and updating this software across all enterprise workstations becomes an endless task. Through its software packaging and deployment modules, BMC Client Management - Software Distribution is able to automate the tasks of distributing, installing, and configuring all enterprise software. Whether deploying or migrating operating systems, updating service packs or upgrading product versions, or rolling out virus protection patches, BMC Client Management - Software Distribution enables the fast and efficient distribution of software to all workstations simultaneously.

Using BMC Client Management - Software Distribution , you can control and manage software installation and distribution across the entire network with ease. The architecture supports pull systems whereby the individual CM agent s collect (or pull) software packages from the master and proceed to install and configure the software on the managed devices. The master is not encumbered by this process, because its role is minimized to the initiation of the overall distribution and to receiving progress information from the agents.

Creating ready-to-distribute packages is very easy using the BMC Client Management - Software Distribution . Software applications and the necessary customizations are automatically turned into packages with a few mouse clicks. In addition, the powerful Chilli language provides you with full control over any advanced changes or installations you want to carry out on the clients.

The automatic rollback function ensures that in case of unforeseeable problems the device configuration is reset to its original state before the software distribution started. The support for user profiles provides the possibility to distribute software to one or all user accounts. System files are updateable through use of the standard Windows reboot mechanism.

Related topics

- Software distribution overview
- Distributing your first package
- Creating an MSI Package and making it available

- Assigning an existing package to the targets for distribution
- Killing Firefox before starting the distribution
- Distributing only to devices with a minimum amount of RAM
- Using multicast distribution (predefined bandwidth)
- Rebooting the device at the end of the distribution
- Scheduling distribution
- Distributing with Wake-On-LAN enabled
- Managing Packages
- Software distribution wizards

Software distribution overview

By using the BMC Client Management - Software Distribution, you can control and manage software installations and distributions across the entire network. The architecture offers a "pull" system, whereby the agents collect (or pull) software packages from the software depot, the master or a relay on the network and proceed to install and configure the software on the clients.

The following topics provide more information about software distribution:

- The four steps of software distribution
- Types of software packages
- Types of software distribution
- Defining the type of software distribution

The four steps of software distribution

Software Distribution consists of four consecutive steps:

- **Creating** the package to distribute in the **Package Factory** and publish it to the master/relay.
- **Assigning** the package to the target device and distributing it.
- **Installing** the package on the target.
- **Monitoring** the installation progress and the results.

Types of software packages

The BMC Client Management - Software Distribution supports the creation and installation of the following software package types:

- **MSI Packages**
- **Snapshot Packages**
- **Custom Packages**
- **RPM Packages**

Types of software distribution

Depending on the package type different types of distribution are also available for the packages.

Distribution type	Description
Normal installation	This is the regular type of package installation which can be used for all different types of installation. It is also the default type of installation and the only one activated by default.
Administrative installation	Administrative installation in this case means, that the package is not downloaded to the target client but remains on the relay and the installation is executed from the relay. An administrative installation installs the package on the network and the targets simply execute the installed package. The advantage of an administrative installation compared to a network installation lies with regards to patches which are to be applied to packages: If the package is patched, future target clients directly install the patched version of the package. If a network installation is used clients first install the version without the patch and then need to install the patch on it separately. This type of installation is only applicable to MSI packages.
Network installation	The network installation is very similar to the administrative installation with the difference that the package is only extracted at the relay and the clients launch a normal installation via the network. Network installation is possible for MSI and custom packages.

Be aware that network and administrative installation is only applicable to packages which were created with a packager of version 5.3.1 or later. If you would like to use packages created with an earlier version, you need to send them back to a packager, modify them (the checksum must change) and then republish them.

Defining the type of software distribution

The network and administrative installation must be activated specifically before assigning packages to their destinations. The option is activated via the **Packages** tab of the **System Variables** node. To activate the option, proceed as follows:

1. Select the **System Variables** node in the console and go to its **Packages** tab.
2. Select the **Activate Network Installation Option** entry in the table in the right window pane.
3. Double-click the entry or **Edit > Properties** .
   The Properties pop-up menu appears.
4. Check the box for the option to activate it.
5. Click **OK** to confirm the modification and to close the window.
   The option is activated immediately and from now on MSI/custom packages may also be installed on the target devices via the network or administrative installation.

This section includes following topics:

- Licenses, capabilities and access rights
- Production environments and reference clients

Licenses, capabilities and access rights

To be able to work with packages and their associated objects, an administrator requires a specific license, capabilities and access rights on these BMC Client Management - Software Distribution objects.

Licenses

Software distribution is part of the BMC Client Management - Software Distribution and requires a specific license, **Software Distribution** which is based on the number of devices assigned to the created packages. If the license is exceeded no more device assignments can be assigned to packages.

Access rights and capabilities

To be able to create, manage and assign the different package types, an administrator needs specific capabilities and access rights:

- To access the main **Packages** node and all its subnodes the **View packages** capability is required.
- The **Manage** capability is required to create, modify or delete a package.
- The **Assign** capability is required to assign a package to a target and the assign access right on the package. In this case the administrator also requires at least the **View** capability on devices or device groups and at least read access to the target objects.
- To publish a package the administrator also requires the **Manage** capability and the **View** capability and read access on the device on which the package is to be published.

Production environments and reference clients

The power of the CM software distribution system can be increased significantly by setting up a proper production environment for it. By using the BMC Client Management - Software Distribution you can quickly upgrade thousands of managed devices across the entire enterprise. But equally you can cause trouble for many users, if your upgrade contains bugs or is incompatible with the existing operating environment. This section explains what to consider and how to do it.

In relation to IT systems, a production environment is a well defined set of hardware and software where all working parameters and operating procedures are well known, that is, documented and tested. One of the cardinal rules applying to such a production system is that changes are introduced in a carefully controlled manner whereby all applicable documentation, reports and procedures are kept up-to-date. In most cases, it also means that changes are introduced only after careful evaluation, testing and certification to ensure the change does not adversely affect other parts of the overall system.

When focusing on the managed devices of the enterprise it means that a subset of the total number of devices are considered as being production devices. Production devices are kept under strong control and their operating parameters are well known. A partial list of the operating parameters for each device include:

- Location
- Hardware profile
- Software profile
- Operating status

- History of changes
- Usage pattern

To test and certify changes before they are rolled out in production a small laboratory is needed. It is in this laboratory environment that the device support engineers can safely manipulate and test new software applications, upgrades and configuration changes. Equally important is the ability to customize standard software before releasing it to the users. In most medium to large networks standard software is invariably preconfigured or customized to work smoothly with the company network and servers or to comply with company templates and other basic rules.

The following topic provides more information about creating a production environment:

Creating a product environment

A production environment establishes standards and acts as a foundation for measuring and improving the service level. Without a production environment the support engineers face a monumental task and each support incident takes longer to close. User reported malfunctions often cannot be reproduced by the support staff without having to go to the actual user device and carry out the diagnosing/debugging/fixing cycle. After the event it is difficult or even impossible to tell if other devices have the same issue - waiting to surface.

The cost of establishing a production environment is saved many times over by eliminating costly mistakes, providing the means to plan ahead properly and maintaining a stable environment for the user community.

The reference device is the device on which you create a new package. In most production environments a device should be set aside for this purpose. Since a package is created from changes, the state of the device before the installation of your software is of little consequence.

The reference device should have the same operating system as the target devices on which you want to install the finished package. Most other differences between the reference device and the target are taken care of by the SmartDelta system and the intelligence that is built into the package.

Distributing your first package

The following topics direct you through the four steps required to create and distribute your first package . You get to know the quickest way to create a **Custom Package** and distribute it to its targets. After successfully installing the you have a basic idea of the general process and you can find out how to make it even more efficient.

- Configuring software distribution
- Creating your first custom package
- Monitoring the custom package distribution
- Uploading software distribution events
- Generating software distribution reports

Configuring software distribution

If you are, for example, on a Windows packager and you want to create and distribute RPM packages you need to define a another packager with a Linux operating system. To define another packager, proceed as follows:

1. Make sure you have the **Packages > Package Factory** node selected in the left tree hierarchy.
2. Go to **Packages > Package Factory**.
   All available **Patch Manager** are listed in the right window pane.
3. Click **Add Packager** .
   The **Add a New Packager** dialog displays.
4. Click **All** .
   All available devices are listed.
5. Select the new device which is to be a **Packager** from the list.

   > To create MSI packages your **Package Factory** must be a Windows operating system, for RPM packages it must have a Linux operating system.

6. **OK** to add it and close the window.
   The device will be added to the table of **Packagers** and its configuration parameter will be updated.

Creating your first custom package

⚠ To do this example you need to have a setup file for an application available for distribution. If this is not yet the case, you can for example download an application from the Internet, for example, the newest version of Mozilla Firefox.

1. Click the **Wizards > Package Creation** menu item to call the **Package Creation Wizard** .
   The **Package Creation Wizard** displays on the screen and guides you through the individual steps required to create a new custom package.
2. Make the following changes in the **Package Factory** window:
   a. Select the **Packager** to use if you have more than one defined.
   b. Click **Next** to continue.
3. Make the following changes in the **Custom Package** window:
   a. Enter the name for the new package into the respective field, for instance *Firefox Installation* .
   b. If your antivirus heavily attacks .zip files, select the *PKG* **Archive Type** .
   c. Leave all other options as they are.
   d. Click **Next** to continue.
4. Make the following changes in the **Installation Options** window:

a. In the **Destination Path** field enter the path in which you want the Firefox setup.exe to be stored temporarily, for instance *c:/temp* .
b. In the **Run Command** field enter the destination path to which the executable file is to be copied, for example, *c:/temp/Firefox Setup 3.0.7.exe /S* .
c. Check the **Overwrite Non-system Files** , **Overwrite older file versions only** and **Overwrite read-only files** boxes in the **Overwrite** panel.
d. Leave all other options as they are.
e. Click **Next** to continue.

5. Make the following changes in the **Add Files** window:
   a. Click **Add File** on top of the table.
   b. In the **Add Files to Package** tab go to the drive and directory in which you stored the *setup.exe* file to distribute and select it.
   c. Clear the option **Enable Full Path** .
   d. Click **OK** to confirm.
   e. Click **Next** to continue.
6. Make the following changes in the **Publication** window.
   a. No operation is required in this window as for this example the package will be published to the master.
   b. Click **Finish** confirm all settings and finish this wizard.
   c. In the **Confirmation** dialog box, check the **Deploy the Package** radio button and click **Yes** to continue directly with the distribution of the new package.
7. Make the following changes in the **Package** window:
   a. If you want to schedule the distribution at a specific later time, clear the **Default Schedule** option.
   b. To distribute the package to a device select the **Devices** from the **Target Type** field.
   c. To make a default distribution to a device group leave all selections as they are.
   d. Click **Next** to continue.
8. Make the following changes in the **Assigned Devices** window:
   a. Click **Assign Devices** .
   b. Click **All** on the left bar.
   c. Select the device from the list box.
   d. Click **OK** to confirm.
   e. If you are using the default schedule click **Finish** now to confirm all settings and finish this wizard. In the **Confirmation** dialog box, check the **Go to Package** radio button to change the focus of the console window to the package distribution view. Click **Yes** to confirm the activation and the proceed with step **Check Status** in this guided task.

Monitoring the custom package distribution

The software distribution now informs the target clients that the new package is available and the installation can begin. To follow this process, proceed as follows:

1. The focus of the console was moved to the **Device Groups** under the **Assigned Objects** node of the newly created package if you checked the **Go to Package** box. If not you need to go to the **Packages > package > Assigned Objects > Device Groups > Your Device Group** node now.
   In the right window pane you can see the entry for the assigned group with its status `Activated` .
2. To follow the execution of the distribution via the different status values the process passes select the *package* subnode.In the table to the right you should see all members of the group with the following successive status values:

- `Activated`
- `Assignment Sent`
- `Assigned`
- `Ready to run`
- `Executed`

At any moment you can use **Refresh** .

The bottom right counter tells you the seconds before the status is refreshed automatically.

Uploading software distribution events

Up to now, the event data about software distributions are only available locally on the agent. However, to be able to generate reports on this topic and to view them in the console together with other data these events must be specifically uploaded to the master and its database. After data is available on software distributions on your network, you can generate different reports to summarize the general situation or detail specific distributions. The following topic will guide you through some of these possibilities. You can find the general information about reports in the Reporting topic.

1. Click the **Wizards > Operational Rule Creation Wizard** menu item.
   The **Operational Rule Creation Wizard** window appears.
2. Make the following changes in the **Definition** window:
   a. Enter a descriptive name into the **Name** box, for example, *Upload Software Distribution Events* .
   b. Click **Next** to continue.
3. Make the following changes in the **Steps** window:
   a. Click **Add Step** .
      The **Select a Step** pop-up menu appears, and displays the list of available steps.
   b. Click the **Event Log Manager** folder.
   c. Select the step **Upload Events** and click **Add** .
      The **Properties** pop-up menu appears.
   d. From the **Model Name** list, select the **Software Installations** value and leave all other boxes as they are.
   e. Click **OK** to confirm the parameters.

f. Click **OK** again to add the step to the rule.
g. After all steps are added, click **Finish** to confirm the new rule and finish this wizard.
h. In the **Confirmation** dialog box, click **Yes** to continue directly with the distribution of the new rule.
The operational rule is now configured and must be assigned to the targets.

4. Make the following changes in the **Operational Rule** window:
   a. Click **Next** to continue without any modifications.
   b. Make the following changes in the **Assigned Targets** window:
   c. Click **Assign Device Group** .
   The **Select a Device Group** pop-up menu appears.
   d. Select the device group(s), for example *All Devices* from the list box.
   e. Click **OK** to confirm.
   f. Click **Finish** now to confirm all settings and finish this wizard.
   g. In the **Confirmation** dialog box, select the **Go to Operational Rule** radio button to change the focus of the console window to the rule distribution view of the assigned group. Click **Yes** to confirm the activation.
   In the table to the right, you can see the entry for each of the assigned devices and you can follow the upload process in the view's schedule **Status** column. The initial status is `Assignment Sent` and the final stage should be `Executed` . After this, status displays the events that are uploaded to the master database.
5. Go to the subnode *All Devices* and follow the execution of the operational rule for the individual group members.
6. To verify this, go to the **Alerts and Events** node of *Your Device Group* , for example, the *All Devices* group.
   This node displays the list of all events registered by the event log models for the selected device group.
7. From the **Model Name** drop-down box select the **Software Installations** option and then click **Find** .
   The following table will now display all software installation events that were uploaded and are continued to be uploaded.

Now all data is uploaded and ready and the report can be generated.

Generating software distribution reports

The BMC Client Management provides a number of predefined reports for the software distribution with its out-of-the-box objects. They are all collected in the **Distribution Statistics** folder. Proceed as follows to generate a report:

1. Open the **Reports > Distribution Statistics** folder.
2. Select a report, for example **Software Distribution Results by Group** .
3. Click **Generate Report** .
4. A confirmation window appears on the screen, click **OK** to confirm.
   The report will be created immediately using the current data of the database.
5. To view the report, click **View Last Result** .

A new browser window or tab opens and displays the report.

Creating an MSI Package and making it available

To do this example you need to have an MSI file for an application available for distribution. If this is not yet the case, you can for example download an application from the Internet.

1. Click the **Wizards > Package Creation** menu item to call the **Package Creation Wizard** . The **Package Creation Wizard** displays on the screen and guides you through the individual steps required to create a new custom package.
2. Make the following changes in the **Package Factory** window:
    a. Select the **Packager** to use if you have more than one defined.
    b. Click the **MSI Package** option in the panel **Package Type** .
    c. Click **Next** to continue.
3. Make the following changes in the **MSI Package** window:
    a. Click **Select** to the right of the **Name** field.
    The **MSI Packages from [IP Address]** displays on the screen and provides you with a list of all available drives from which you can select the *MSI package* .
    b. Browse down into the directory tree and select the package to distribute
    c. If your antivirus heavily attacks .zip files, select the *PKG* **Archive Type** .
    d. If the *MSI package* requires further files check the **Additional Files** box in the **Options** panel.
    e. Leave all other options as they are.
    f. Click **Next** to continue.
4. Make the following changes in the **Installation Options** window:
    a. In the **User interface** field, select the **None** option instead of the preselected value.
    b. Leave all other options as they are.
    c. Click **Next** to continue.
5. Make the following changes in the **Additional Files** window:
    a. Click the **Add File** on top of the table.
    A dialog box with the name of the package appears, providing the list of all available drives.
    b. Leave all other options as they are.
    c. Find the storing location either on your hard drives or on the CD/DVD drive and select the additional files required for installation. Such files can be, for example the `sku026.cab` and `sku0a4.cab` files, located on the same level as the .mis file.

    > ⚠ Be aware that here you can only add files that are required by the MSI package, not any that you would like to also have distributed.

    d. Click **OK** to confirm.
    e. Click **Next** to continue.

6. Make the following changes in the **Publication** window.
    a. No operation is required in this window as for this example the package will be published to the master.
    b. Click **Finish** to confirm all settings and finish this wizard.
    c. In the **Confirmation** dialog box, check the **Deploy the Package** radio button and click **Yes** to continue directly with the distribution of the new package.
7. Make the following changes in the **Package** window:
    a. If you want to schedule the distribution at a specific later time, clear the **Default Schedule** option.
    b. To distribute the package to a device, a user or a user group, select the desired value from the **Target Type** field.
    c. To make a default distribution to a device group leave all selections as they are.
    d. Click **Next** to continue.
8. In this window you need to define the targets of the package distribution. Depending on the choice in the preceding window you must add either devices, device groups, users or user groups as follows:
    a. Click **Install the package on the assigned devices** .
    The respective assignment dialog appears.
    b. Click **All** on the left bar.
    c. Select the object(s) from the list box.
    d. Click **OK** to confirm.
    e. If you are using the default schedule, click **Finish** now to confirm all settings and finish this wizard. In the **Confirmation** dialog box, check the **Go to Package** radio button to change the focus of the console window to the package distribution view. Click **Yes** to confirm the activation and the proceed with step **Check Status** in this guided task.
    f. If you are using the default schedule click **Finish** now to confirm all settings and finish this wizard. In the **Confirmation** dialog box, check the **Go to Package** radio button to change the focus of the console window to the package distribution view. Click **Yes** to confirm the activation.
    g. To use a different schedule click **Next** to continue with the wizard.
9. Make the following changes in the **Schedule** window:
    a. Check the **Deferred to** radio button in the **Assignment Date** box and select the desired date and time in the list boxes to the right.
    b. Check the box **Wake-up Devices** , if you want to use the Wake-On-LAN option.
    c. To schedule the actual distribution at a specific date select the **Validity** and select the desired moment for the provided options.
    d. Click **Finish** now to confirm all settings and finish this wizard.
    e. In the **Confirmation** dialog box, check the **Go to Package** radio button to change the focus of the console window to the package distribution view. Click **Yes** to confirm the activation.
10. If you did not check the **Go to Package** box at the end of the wizard select the newly created package (for example, *Firefox Installation*) in the left tree hierarchy under the **Packages** node and then its **Assigned Objects -> Devices** subnode.

11. In the table to the right you can see the entry for each of the assigned devices and you can follow the patching process in the view's schedule **Status** column. The initial status is *Assignment Sent* and the final stage should be *Executed*.

Assigning an existing package to the targets for distribution

To assign an existing package that has not yet been assigned or that must be assigned to other devices or device groups, proceed as follows:

1. Open the **Packages > Assigned Objects > Your Package > Device Groups** node.
2. Select *Your Device Group* entry in the right window pane.
3. Click **Properties** .
   A confirmation window appears, click **OK** . The **Scheduler** window appears.
4. In the **When do you want this rule to be run on devices?** box either check **Right now** to directly launch the installation or the **Run repeatedly on a schedule** option and then define the desired date and time via the new boxes that appear to start the installation at a later time.
5. Click **OK** to confirm the schedule.

The relation between the package and the targets is not established and the assignment and installation is started according to the defined schedule.

Killing Firefox before starting the distribution

If you are using this software distribution to upgrade existing Firefox versions, BMC recommends to make sure that any existing version of the Firefox browser is stopped on the target devices before starting the installation. To do so, proceed as follows:

1. Select the **Operational Rules** top node in the left window pane.
   The right window pane displays the list of existing operational rules and folders.
2. Select *Your Package Distribution Rule*.
3. Go to the **Steps** tab.
4. Click **Add Step** .
   The **Select a Step** dialog appears.
5. In the **Available Steps** box open the folder **Process Management** and select step **End Processes** .
6. Click **Add** .
   The **Properties** dialog appears.
7. Make the following changes in the window: the option **The rule fails** for box **Stop Condition** and enter 256 in the RAM (MB) text box.
   - Select the option **The rule fails** from the **Stop Condition** list.
   - Enter `firefox.exe` into the box **Process Names** .
8. Click **OK** to add the step to the list.

9. In the table to the right select the line **RAM (MB)** and then click **Move Up** once.
   Now the required new step is added and at the right position: If any version of Firefox is currently being executed on a target device, it is stopped before the installation process is started.
10. Now you can continue to assign the package to its targets or to reactivate the package assignment if you modified an existing package

Distributing only to devices with a minimum amount of RAM

When a package is assigned for distribution, an operational (distribution) rule of the same name as the package will automatically be created, containing the necessary actions (steps) to execute the package installation on the target device. This operational rule is editable, that is, conditions can be added to it before the package installation, such as making sure the package will only be installed on a device with Windows 2003 as its operating system and at least 512 MB RAM. Proceed as follows:

1. Select the **Operational Rules** top node in the left window pane.
   The right window pane displays the list of existing operational rules and folders.
2. Select *Your Package Distribution Rule*.
3. Go to the **Steps** tab.
4. Click **Add Step** .
   The **Select a Step** dialog appears.
5. In the **Available Steps** box open the folder **Monitoring** and select step **Check Installed RAM** .
6. Click **Add** .
   The **Properties** dialog appears.
7. Make the following changes in the window:
   - Select the **The rule fails** option from the **Stop Condition** drop-down list.
   - Enter 512 into the box **RAM (MB)** .
8. Click **OK** to add the step to the list.
9. In the table to the right select the line **RAM (MB)** and then click **Move Up** once.
   Now the required new step is added and at the right position: If a target device does not have at least 512 MB of RAM, the distribution will not be executed.
10. Now you can continue to assign the package to its targets or to reactivate the package assignment if you modified an existing package

Using multicast distribution (predefined bandwidth)

> **Note:**
>
> You need the special Multicast license if you want to execute software distributions via multicast. For trial purposes this license is included in the temporary license.

Multicast delivery enables parallel software distribution to an unlimited number of client systems while simultaneously reducing server and network resource requirements and bandwidth consumption for high-volume, high population software distribution. It enables software to be distributed to thousands of desktops in the same time it takes to deliver software to a single desktop, while making optimal use of server and network resources. The multicast principle is to send a file on a virtual multicast address advertised to all target clients where each of these will get the file. Contrary to unicast the server sends the file only one time.

A software distribution via multicast consists of the following steps:

1. Modify the multicast parameters on the relay if you have a specific configuration for which the default values cannot be used. The default values are specified for a speed of 128 KB/s which should work for all types of networks.
2. Create a multicast transfer window and assign it to the multicast relay. Be aware that if a transfer window of type multicast is assigned to a relay, this relay can only execute multicast software distributions, no unicast distributions.
3. Assign the package to distribute via multicast to the targets.

This section includes following topics:

Defining the Transfer Window

To now distribute our Firefox software package to all clients without Firefox in the network, proceed as follows. BMC will assume that the default parameters can be used with our network and thus require no specific configuration.

1. Go to the **Transfer Windows** node under the **Global Settings** top node.
2. Click **Create Transfer Window** .
   The **Properties** dialog displays.
3. Enter the desired name, for instance *Standard Multicast* , select **Multicast** as the transfer channel and **KBytes/second** from the **Slot Type** list.
4. Click **OK** to confirm these settings and to close the window.
5. Select the newly created window, for example, *Standard Multicast* , in the left pane and select its **Planning** tab.
   The right window pane displays an hour/day of the week grid.
6. Mark the periods for which the bandwidth restrictions are to apply by selecting the first slot, for example, *Monday 08:00* and move your mouse cursor to the last slot, for example, *Friday 18:00* , to restrict the bandwidth for all working days from *8am to 6pm* .
7. Click **Define Time-slot** .
   The **Define Transfer Window Time-Slots** window appears.
8. Enter `128` (or any other desired value) and click **OK** to confirm.
9. Select the **Assigned Objects > Devices** node of the *Standard Multicast* window.

10. Click **Assign Device** .
    A confirmation window appears, click **OK**. The **Select a Device Group** dialog displays.
11. Select **All**.
12. Select the device to which you want to apply bandwidth control, that is, the relay, and click **OK** to confirm.

From now on, and in the time slot defined, no communication between the selected device and its parent (the master or a relay) will ever exceed 128 KB/second, in both the ascending (inventories) and descending (distributions) directions. You can now distribute the Firefox package without any risk of limiting the network access to the end-user.

Distributing the package via the transfer window

Now the required transfer window is defined and the distribution of Firefox can be continued:

1. Open the **Packages > Assigned Objects > Your Package > Device Groups** node.
2. Select *Your Device Group* entry in the right window pane.
3. Click **Properties** .
   A confirmation window appears, click **OK**. The **Scheduler** dialog appears.
4. In the **When do you want this rule to be run on devices?** box either check **Right now** to directly launch the installation or the **Run repeatedly on a schedule** option and then define the desired date and time via the new boxes that appear to start the installation at a later time.
5. Click **OK** to confirm the schedule.
   The software distribution process via multicast to the clients is now started.
6. To verify that the distribution was correctly executed via multicast go to *Your Device Group* subnode.
   In the table to the right all member devices of the group are listed with their status values and other data.
7. Check the column **Transport Mode**.

> As long as the software distribution has not executed it will display the value `Unknown` . After the distribution started it displays `}}` , `if the multicast distribution worked properly. If this is not the case the software distribution is executed in the regular way and this text box displays {{Unicast` .

Rebooting the device at the end of the distribution

Some software installations or upgrades require that the device is rebooted after the installation. This operation can be directly integrated with the software distribution rule of the package in either of the following ways:

1. Add a new step *reboot* to the distribution rule.
2. Add a separate existing *reboot* rule to the software distribution rule as a dependency.
3. Define the device reboot after the distribution as a user choice.

The following topics provide more information about rebooting a device:

- Adding Reboot step to software distribution rule
- Adding a Dependency with the Reboot Rule
- Adding the Reboot step to the software distribution as a dependency
- Defining the Device Reboot after the distribution as a user choice

Adding Reboot step to software distribution rule

1. Select the **Operational Rules** top node in the left window pane.
   The right window pane displays the list of existing operational rules and folders.
2. Select *Your Package Distribution Rule*.
3. Go to the **Steps** tab.
4. Click **Add Step** .
   The **Select a Step** dialog appears.
5. In the **Available Steps** box open the folder **Tools** and select step **Reboot Device**.
6. Click **Add** .
   The **Properties** dialog appears.
7. No modifications are required here, therefore click **OK** directly to add the step to the list.
   In this case, the required new step is directly added at the right position: at the end and after the installation. It will be executed right after the installation of the package.
8. Now you can continue to assign the package to its targets or to reactivate the package assignment if you modified an existing package.

Adding a Dependency with the Reboot Rule

> **Note:**
>
> A dependency is ALWAYS defined in the rule that follows another, that is, for the rule that is executed after a specified other rule.

If you are using this software distribution to upgrade existing Firefox versions BMC recommends to ensure that any existing version of the Firefox browser is stopped on the target devices before starting the installation. To do so, proceed as follows:

1. Select the **Operational Rules** top node in the left window pane.
   The right window pane displays the list of existing operational rules and folders.
2. Select your *Reboot* rule.
3. Go to the **Dependencies** tab.

4. Click **Add Dependency** .
   The **Select an Operational Rule** dialog appears.
5. Select *Your Package Distribution Rule* .
6. Click **OK** .
   The dialog closes and the **Operational Rule** is listed in the right window pane.

You added the dependency of your *Reboot* rule to *Your Package Distribution Rule* .

Adding the Reboot step to the software distribution as a dependency

1. Click the **Wizards > Operational Rule Creation** menu item to call the **Operational Rule Creation Wizard**.
   The **Operational Rule Creation Wizard** is displayed on the screen and guides you through the individual steps required to create a new operational rule.
2. Make the following changes in the **Definition** window:
   a. Enter the name for the new operational rule into the respective field, for instance *Device Reboot* into the **Name** field.
   b. Check the **Add Dependencies** option.
      The **Dependencies** wizard step in the left window bar has now become visible to indicate that this step needs to be defined.
   c. Click **Next** to continue.
3. Make the following changes in the **Steps** window:
   a. Click **Add Step** .
      The **Select a Step** dialog appears.
   b. In the **Available Steps** box open the folder **Tools** and select step **Reboot Device**.
   c. Click **Add** .
      The **Properties** dialog appears.
   d. No modifications are required here, therefore click **OK** directly to add the step to the list.
      In this case, the required new step is directly added at the right position: at the end and after the installation. It will be executed right after the installation of the package.
   e. Click **OK** again to confirm the list of steps.
   f. After all steps are added click **Next** to continue.
4. Make the following changes in the **Dependencies** window:
   a. Click **Add Dependency** above the table.
      The **Select an Operational Rule** dialog appears.
   b. Select *Your Package Distribution Rule*.
   c. Click **OK** .
      The dialog closes and the **Operational Rule** is listed in the right window pane.
5. Click **Finish** now to confirm all settings and finish this wizard.
6. In the **Confirmation** dialog box, click **No**.

The reboot rule is now properly set up and you can assign both rules, the reboot and the software distribution rules to the target lists or reassign them if you modified them.

Defining the Device Reboot after the distribution as a user choice

It is also possible to define the reboot of the target device in such a way as to let the user choose if he wants to reboot the device at all, or when he wants to do it. This use case can be implemented in two different ways:

1. **Two Operational Rules with a Dependency**
    a. Create an operational rule for the Firefox distribution. Depending on where in the distribution process you interrupt, this rule might already be created.
    b. Create a second operational rule to control the reboot process.
    c. Create a dependency between these 2 rules.
    d. Assign and activate the 2 rules.
2. **One Operational Rule with an Additional Reboot Step**
    a. Create an operational rule for the Firefox distribution. Depending on where in the distribution process you interrupt, this rule might already be created.
    b. Add the steps to control reboot to this rule.
    c. Assign and activate this rule.
    The drawback of this second method is that if the user chooses not to reboot, the whole distribution result will be reported as `Failed` , while in the first case, the distribution rule will be `Executed` (**OK**) and the *Reboot* rule will be `Executed` (normal as the user decided not to reboot).

The following topics provide more information about defining the device reboot:

- Adding a Reboot step with user confirmation to the software distribution rule
- Two Operational Rules with a dependency

Adding a Reboot step with user confirmation to the software distribution rule

1. Select the **Operational Rules** top node in the left window pane.
   The right window pane displays the list of existing operational rules and folders.
2. Select *Your Package Distribution Rule*.
3. Go to the **Steps** tab.
4. Click **Add Step** .
   The **Select a Step** dialog appears.
5. In the **User Message Box** box open the folder **Tools** and select step **User Acknowledgement via Message Box**.
6. Click **Add** .
   The **Properties** dialog appears.
7. Enter the following data in the respective boxes:
    a. **Stop Condition** : select the **The rule fails** option.
    b. **Message Title** : Firefox Distribution.
    c. **Message Text** : Do you want to reboot now or later?
    d. **Validation Button Label** : Now
    e. **Cancel Button Label** : Later

f. **Number of Retries** : 20
g. **Retry Interval (min)** : 5

8. Click **OK** to confirm and add the step to the list.
9. Expand the folder **Tools** and select step **Reboot Device** .
10. Click **Add** .
    The **Properties** dialog appears.
11. Click **OK** to add the step to the list.

> In this dialog, no modifications are required.

The reboot step has now been added to the software distribution rules. You now can continue to assign the package to its targets or to reactivate the package assignment if you modified an existing package.

Two Operational Rules with a dependency

> **Note:**
>
> A dependency is ALWAYS defined in the rule that follows another, that is, for the rule that is executed after a specified other rule.

The software distribution rule is already created therefore we only need to create the reboot rule as follows and add its dependency to the distribution rule:

1. Click the **Wizards > Operational Rule Creation** menu item to call the **Operational Rule Creation Wizard**.
   The **Operational Rule Creation Wizard** is displayed on the screen and guides you through the individual steps required to create a new operational rule.
2. Enter the name for the new operational rule into the respective field, for instance *Device Reboot with User Confirmation* into the **Name** field.
3. Check the **Add Dependencies** option.
   The **Dependencies** wizard step in the left window bar has now become visible to indicate that this step needs to be defined.
4. Click **Next** to continue.
   You now reach the **Steps** window.
5. Click **Add Step** .
   The **Select a Step** dialog appears.
6. In the **User Message Box** box open the folder **Tools** and select step **User Acknowledgement via Message Box**.
7. Click **Add** .
   The **Properties** dialog appears.

8. Enter the following data in the respective boxes:
   - **Stop Condition** : select the **The rule fails** option.
   - **Message Title** : Firefox Distribution.
   - **Message Text** : Do you want to reboot now or later?
   - **Validation Button Label** : Now
   - **Cancel Button Label** : Later
   - **Number of Retries** : 20
   - **Retry Interval (min)** : 5
9. Click **OK** to confirm and add the step to the list.
10. Expand the folder **Tools** and select step **Reboot Device** .
11. Click **Add** .
    The **Properties** dialog appears.
12. No modifications are required here, therefore click **OK** directly to add the step to the list.
13. Click **OK** again.
14. Click **Next** to continue.
15. Make the following changes in the **Dependencies** window:
    a. Click **Add Dependency** above the table.
       The **Select an Operational Rule** dialog appears.
    b. Select *Your Package Distribution Rule*.
    c. Click **OK**.
       The dialog closes and the **Operational Rule** is listed in the right window pane.
16. Click **Finish** now to confirm all settings and finish this wizard.
17. In the **Confirmation** dialog box, click **No**.

The reboot rule is now properly set up and you can assign both rules, the reboot and the software distribution rules to the target lists or reassign them if you modified them.

Scheduling distribution

With the default schedule, packages are distributed immediately. However, depending on its size, distributing a package to a number of devices can be resource consuming and might decrease the efficiency of your network. In this case it is recommended to execute distributions when the network load is low, that is, at night, during lunch break or on the weekend. For this purpose a scheduler is provided which allows you to define specific times for distribution.

In this example you define that the package is assigned to the devices at 1:00 AM. This means that the package will pass through your device hierarchy and be installed early in the morning thus not affecting the regular working day.

1. In the **Assignment** tab of the **Schedule** view define when you want the package to be assigned to the respective devices.To assign the package, for example, over night, select the **Deferred to** radio button and select **Tomorrow** from the first list and `01:00` from the second list.

2. Click the **Frequency** tab and define the timeframe for the deployment of the package.To allow deployment between 1:00 AM and 6:00 AM, select 01:00 from the **between** drop-down list and 06:00 from the **and** drop-down list in the **Frequency** group box.
3. Click **Finish**.
   The **Confirmation** dialog box appears.
4. Select the **Go to Package** radio button and click **Yes**.
   The dialog closes and in the right window pane the new package opens.

Distributing with Wake-On-LAN enabled

BMC Client Management - Software Distribution allows you to use the Wake-On-LAN functionalities to ensure that the software is distributed to all assigned devices no matter their current state.

Make the following changes in the **Schedule** window if you unchecked the **Default Schedule** option in the first window of the wizard:

1. In the **Assignment** tab of the **Schedule** view, check the box **Wake-up Devices**, to enable the WOL option.
2. Click **Finish**.
   The **Confirmation** dialog box appears.
3. Select the **Go to Package** radio button and click **Yes**.
   The dialog closes and in the right window pane the new package opens.

Managing Packages

Packages are one of the key components of software distribution. They contain the instructions necessary to install software on a target device and all the files of the application to install. The package is essentially a compressed archive of new files plus some intelligence. The intelligence is automatically built into an operational rule containing the scripts that deal with creating directories, installing the files, adding icons, changing the Registry and starting services. The scripts also deal with error checking during installation and the creation of log files. Packages should be created on a reference device in a Production Environment.

The **Packages** node of the CM console provides all published packages of any type which are available within your network for software distribution. The packages are not created here, they are created on individual clients through the Package Factory, they are only stored under this node to be available to everybody. Under this node you can define the devices and device groups to which the packages will be distributed and the schedules for the package executions.

Like other objects in CM, published packages are stored in folders. These folders are for grouping one or more packages by type to make organisation and finding packages easier.

Package Folders are created as organisational containers for different types of packages. They can contain any number of predefined or custom-made packages and package folders for software distribution within your network.

Automatically creating packages and folders

A number of Packages and Package Folders are created automatically:

- The **CMUpgrade** folder is created automatically when the master is installed or updated. It contains the files necessary to update the relays and clients in your network to the current version.
- The **Patches** folder is created when the first patch download is requested and executed. All patches that are downloaded and published will be located in their respective directories under this main folder. Be aware that the packages created by this patch download and publication process can be edited via the **Package Factory** but their object associations are not modifiable.
- The **ConfigFiles.cst** package is created if you have a valid Patch Management license. This file is the database file for the patch inventory generation and when the agent is started for the first time, it will download and publish the newest version of this group of files in the form of a custom package.

Related topics

- Managing a Custom Package
- Managing an MSI Package
- Managing an RPM Package
- Managing Snapshot Packages
- Managing Package Folders
- Managing Package Factory
- Packager - Software Distribution
- Bulk-importing MSI packages
- Managing Transfer Windows
- Managing Storage Relays
- Multicast software delivery
- Managing common content and configuration

Managing a Custom Package

Custom packages are installation packages of any type which are specifically created for a software distribution, such as setup, UNIX, file distribution, and so on. They can be used with all platforms supported by BMC Client Management.

How does a Custom Package Work?

Similar to the MSI packages Custom packages are already created before they are 'copied' to a specific location on the remote computer through **Packager**. There all further files and scripts necessary for the software distribution will be added to the base package before it will be published to the master database.

1. The **Packager** allows for selecting the files that are included in the package and wrapping this information into a .zip file. You can also select another file extension for your compressed package in the respective configuration file.
2. The **Packager** then forwards the .zip file to the master server.
3. The master server distributes the .zip file through the cascade of servers and relays to the target computers.
4. The agent on the target opens the .zip file and calls the configured command line.

The following topic provides more information about adding files to custom package:

Adding files to a Custom Package

After having defined all installation options through the contents of the **Configuration** and **Contents** nodes, the custom package is created. You can add now files to this package which will then be sent to the targets for installation. To add files, proceed as follows:

1. Click **Edit > Add Files to Package**  .
   The **Add Files to Package** dialog box appears on the screen.
2. The **Add Files** tab provides the list of all available drives through which you can go down in their hierarchy to select the files to be added to the `.zip` file.
3. Specify if the package is to include the full path of the file or put the file at the root of the installation by checking/unchecking the **Enable Full Path** box.
4. Define through the **Fast File Collection** check box, if the files are to be added in normal (unchecked) or fast (checked) mode. Fast mode can be useful if you add large numbers of files to a package.
   However, you need to be very careful when using this option, because there will be no verification taking place, that is, if the files already been added before, they will be added a second time and will not replace the already existing version, thus possibly causing the package to become very large.
5. Click **OK** at the bottom of the window to confirm the additions or **Cancel** to stop and close the window.

Managing an MSI Package

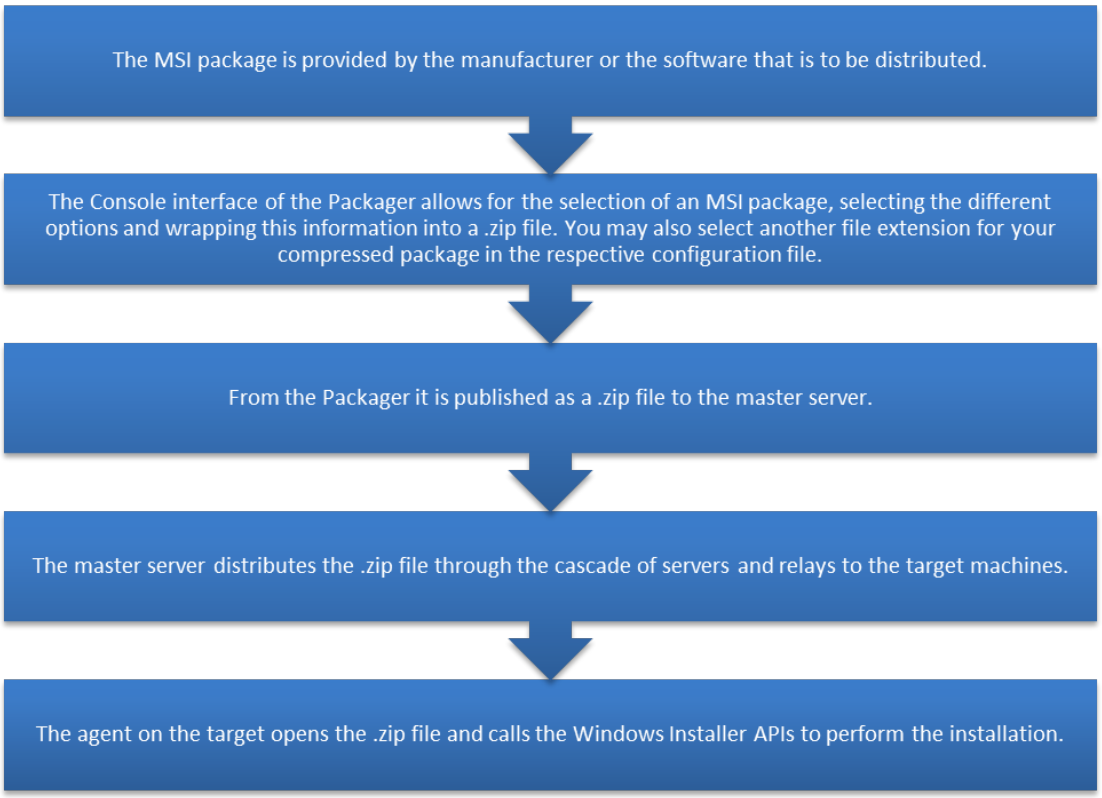
With Windows Installer and the .msi package file format, software installation and removal has become more reliable and resilient while providing a larger set of installation options. Windows Installer manages the installation and removal of applications by applying a set of centrally defined setup rules during the installation process. These setup rules define the installation and configuration of the installed application. In addition, you use this service to modify, repair, or

remove an existing application. The Windows Installer technology consists of the Windows Installer service for the Windows operating systems and the package (.msi) file format used to hold information about the application setup and installations.

Windows Installer is not only an installation program; it is also an extensible software management system. Windows Installer manages the installation, addition, and deletion of software components, monitors file resiliency, and maintains basic disaster recovery by way of rollbacks. Additionally, Windows Installer supports installing and running software from multiple sources, and can be customised by developers that want to install custom applications.

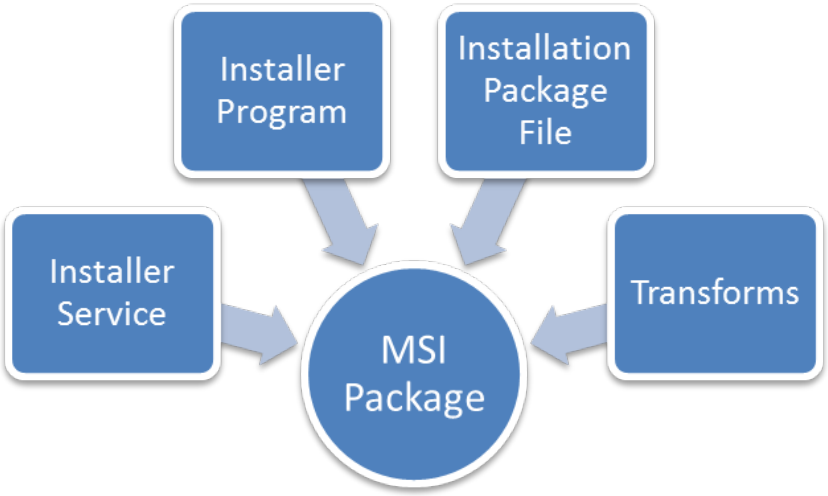
How does an MSI Package work?

The BMC Client Management - Software Distribution **Packager** includes a specific node to wrap MSI packages and the Windows Installer options into a new package containing all necessary installation information. The agents on the remote computers can perform an MSI package installation with those options using the native Windows Installer APIs. The following diagram explains the MSI distribution process:



What are the MSI Package Components?

Windows Installer technologies are divided into two parts that work in combination: a client-side installer service (Msiexec.exe) and a package file (.msi file). Windows Installer uses the information contained within a package file to install the application.



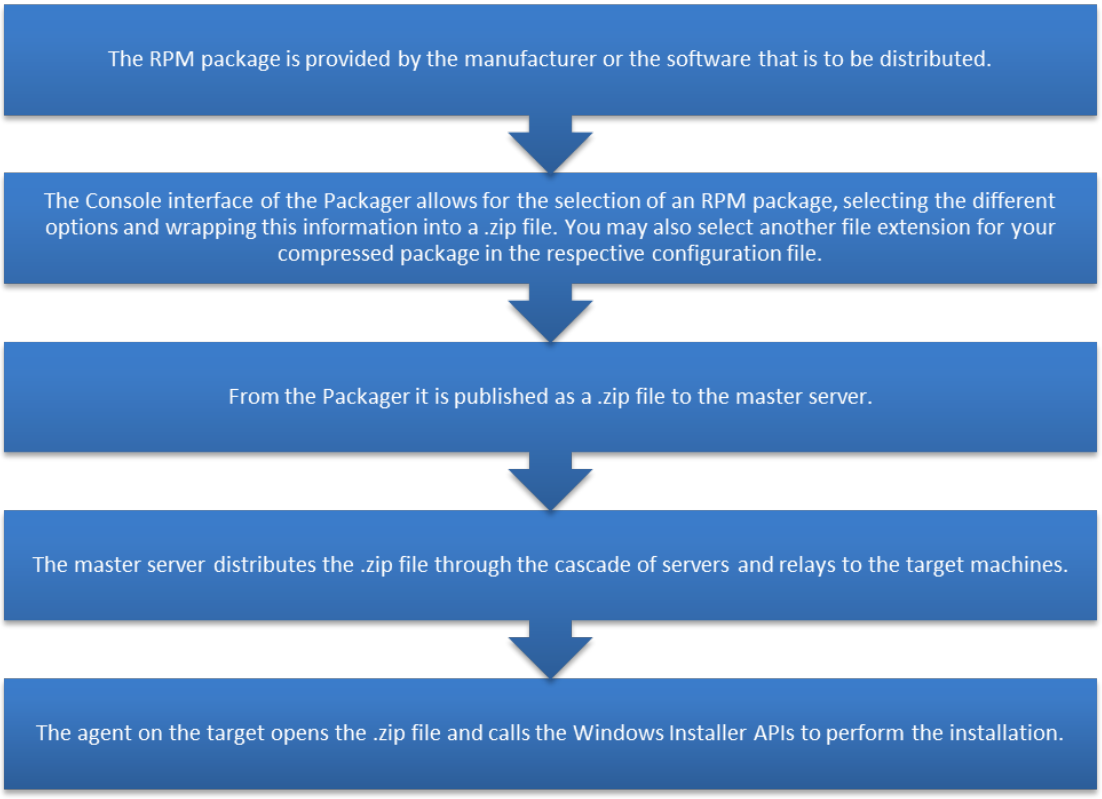
Component	Description
Installer Service	Windows Installer is an operating system service that allows the operating system to manage the installation process.
Installer Program	The Msiexec.exe program is a component of Windows Installer. This program uses a dynamic link library, Msi.dll, to read the package files (.msi), apply transforms (.mst), and incorporate command-line options. The installer performs all installation-related tasks: copying files onto the hard disk, making registry modifications, creating shortcuts on the desktop, and displaying dialog boxes to query user installation preferences when necessary. When Windows Installer is installed on a computer, the file association capabilities of the operating system are modified to recognise the .msi file type. When a file with the .msi extension is double-clicked, the operating system associates the .msi file with Windows Installer and runs the Msiexec.exe application.
Installation Package File	Each package (.msi) file contains a relational type database that stores all the instructions and data required to install (and uninstall) the program across many installation scenarios. For example, a package file could contain instructions for installing an application when a earlier version of the application is already installed. The package file could also contain instructions for installing the software on a computer where that application has never been present.
Transforms	The installation process can be manipulated by applying transforms (.mst) to the installation database. A transform makes changes to elements of the database. For example, Windows Installer can use a transform file to change the language in the user interface of an application. The Windows Installer transform files modify the installation package file at installation time, and can therefore dynamically affect the installation behaviour. Customisation transforms, much like patches, remain cached on the computer. These transforms are applied to the base package file whenever Windows Installer needs to perform a configuration change to the installation package. Transforms are applied at initial installation; they cannot be applied to an already installed application.

Managing an RPM Package

The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files information about the package like its version, a description, and the like. There is also a related API, permitting advanced developers to bypass 'shelling out' to a command line, and to manage such transactions from within a native coding language. RPM is commonly found in the Linux computer operating system environment, but was extended far beyond those initial confines.

How does the RPM Package work?

The BMC Client Management - Software Distribution Packager includes a specific node to wrap RPM packages and installer options into a new package containing all necessary installation information. The agents on the remote computers can perform an RPM package installation with those options. The following diagram explains the rpm distribution process:



Managing Snapshot Packages

The basic philosophy behind the Snapshot Mode of the BMC Client Management - Software Distribution is very simple: Memorize the configuration of a system before an installation and use it to find the changes, which took place after the installation. The **Package Factory** is responsible for the generation of the software package, which is to be distributed to a number of clients. The generated package file will be placed on the master server from where each client will collect it and install the contents via their relays. This means that you need one or more reference devices on which the applications can be installed and customized before distributing the resulting package throughout your network.

> **Note:**

You need to pay some thought to what software you want to distribute. Make it small and simple so you can work with it easily and satisfy yourself that it installed correctly. Select something you are familiar with and make some simple configuration changes. You can then verify that a configured package arrived and not just the canned version installed by the setup program.

Note:

You will need to ensure that you have 2 devices at hand. One on which to create the package, your reference device, the other will become your target device. The CM agent must be configured and working correctly on the target device.

The console operation of the snapshot packages is based on the idea of a snapshot, which contains all the system configuration information. This is created by the console in a custom format file, which is used later on to find the changes. After the snapshot has been created the software product(s) to be distributed to your network are installed on the reference device.

With the required software product or products installed, use the console and the saved snapshot file to find the system changes. These changes are stored in temporary lists, which are then processed to create the actual distributable software package.

The distributable software package is an archive file which contains all the new files on the system and an installation script which describes where the files are to be placed and which configuration files have to be changed. The package can only be created if the Console has already created the list of changes.

Note:

This node will only appear in the **Package Factory** for devices running on any type of Windows operating system.

Creating a snapshot package consists of three major steps which are reflected in the subnodes of the snapshot package:

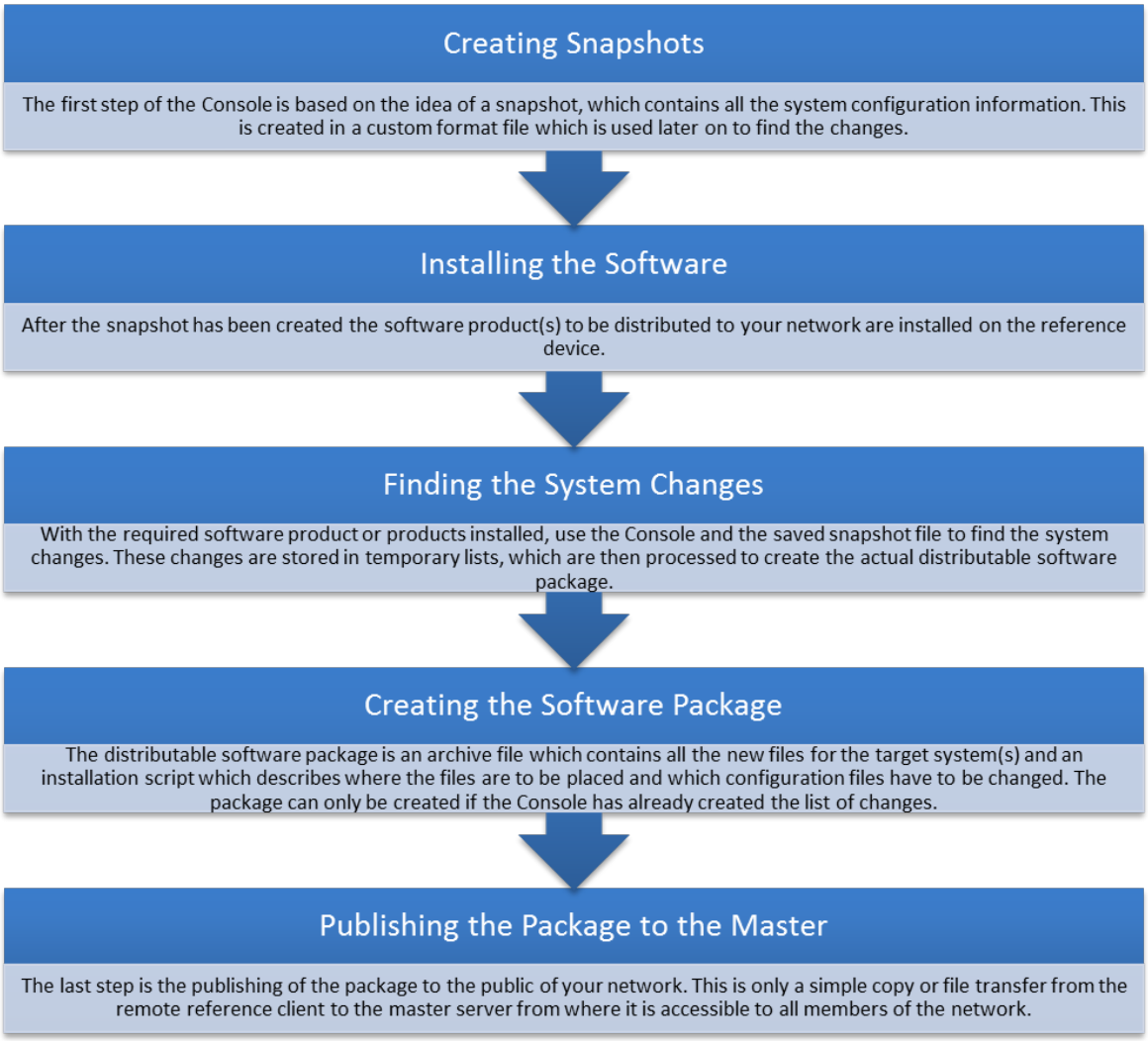
1. Snapshot: Creating a snapshot of the reference device and then installing the new software.
2. Changes: Finding all the changes of before and after installation.
3. Package: Creating the actual software package.

How does a snapshot package work?

A snapshot is an image of the state of the system taken by the console and kept for later reference. The snapshot contains information about all files and directories on the reference device together with information about the Registry and services and drivers.

1. The **Packager** allows for selecting the files that are included in the package and wrapping this information into a .zip file. You can also select another file extension for your compressed package in the respective configuration file.
2. The **Packager** then forwards the .zip file to the master server.
3. The master server distributes the .zip file through the cascade of servers and relays to the target computers.
4. The agent on the target opens the .zip file and calls the configured command line.

The following chart illustrates the steps of creating a **Snapshot Package** :



The following topics provide more information about managing snapshot packages:

Creating a new snapshot package

It is also possible to directly create a new package in this tab. To create a new package, proceed as follows:

1. Select **Edit > Create Package** .
   The **Create a Snapshot Package** window will appear on the screen.
2. Enter the name of the new package into the **Name** field.
3. In the **Publication Folder** field you can enter the path under which the package is to be published on the master or relay.
4. Below the list of drives select the **Archive Type** in which the package is to be stored.

> You have the choice between the .zip format and the proprietary `.pkg` format. Which type to select depends on your network environment, because it does not have any impact on the software distribution process itself. For example, if your virus scan software scans `.zip` files, it is recommended to select the `.pkg` archive type, to avoid the virus scan taking 100% CPU.

5. Click **OK** to confirm the creation of the new package.
   It will automatically be created in the table in the right pane.

> **Note:**
>
> When you create a new snapshot package it will be stored in a newly created folder with its own name under the `data/PackagerSnapshot` subdirectory of the local installation directory on the remote computer.

Snapshot

When a snapshot is created the console collects information about all parts of the system, e.g, files, directories, registries, icons and groups, and so on. The collected data is then stored in a single user selected file, usually with a .SNP extension, and is used by the console to determine the changes which took place after a particular software product was installed on the reference device.

Together with the snapshot file, the console will create an archive of the same name but with a .STA extension which contains all text configuration files on the system. This is necessary for the console to be able to find the exact changes for every modified configuration file.

The **Snapshot** node displays the following general information about the selected package. If the package has just been created the values for all these attributes will be 0, because the snapshot has not yet been created:

Parameter	Description
Creation Date	This field uses the system clock to fill in the date and time of creation of the snapshot.
File Size (KB)	This field displays the total size of the snapshot file in bytes.
Number of Scanned Directories	This entry displays the number of directories contained in the snapshot. Note, that the settings defined through the Drive and Directory tabs in the Configuration subnode can affect this number.
Number of Scanned Files	This entry displays the number of files contained in the snapshot. Note, that the settings defined through the Drive and Directory tabs in the Configuration subnode can affect this number.
Number of Scanned Text Files	This entry displays the number of text files contained in the snapshot. Note, that the settings defined through the Text File Extensions tabs in the Configuration subnode can affect this number.
Number of Scanned Registry Keys	This field displays the number of Windows registry keys contained in the snapshot archive.
Number of Scanned Registry Values	This field displays the number of Windows registry values contained in the snapshot archive. Note, that there might be many more values than keys, because a key can hold multiple values.
Status	Displays the current status of the snapshot during execution.

Creating a Snapshot of a package

> **Note:**
>
> Before you create a snapshot make sure ALL programs are stopped, this includes such programs as antivirus software, e-mail programs or browsers.

> **Note:**
>
> Before creating your snapshot make sure you have configured what is to be included and excluded from the snapshot via the Configuration node. If you create a snapshot without configuration the whole system will be included, which make take a very long time to create!

To create a snapshot:

1. Click **Create Snapshot** .

Configuring snapshot

When you create a new snapshot, the console will try and collect information about all files, directories, groups, icons and registry values on the hard disks of the device. A typical device contains approximately 10,000 files and 800 directories, which will result in a snapshot file of a few MBs and an equally large Snapshot Text Archive file. A snapshot like this is usually a waste of space as most software installations are limited to creating new directories and modifying the contents of the Windows directory. A new installation will very rarely place files in an unrelated program directory, it is therefore unnecessary to include these unrelated directories and files in the snapshot.

Drive

In this tab you can define the drives to be included into the snapshot. If, for example your device has more than one drive but all programs are installed on the c drive, it is not necessary to include any of the other drives in the snapshot.

Adding a Drive

To add a drive to the list of drives to be scanned, proceed as follows:

1. Select **Edit > Add Drive**  .
   A configuration window appears.
2. Select the desired drive from the displayed list.
3. Click **OK** to confirm the addition and to close the window.

Directory

For directories the snapshot function operates in either one of two modes, the **Include listed directories** or **Exclude listed directories** mode.

If the Snapshot mode is set to **Include listed directories** , the snapshot will be limited to the entries in the directory list. This is useful if your system has a large number of directories and it would be easier to include the few important directories such as those for the Windows and DOS system files.

If the directory mode is set to **Exclude listed directories** , the console will ignore all directories, which are in the directory list. Compared to a snapshot defined with **Include listed directories** , a snapshot with excluded directories will usually be larger, but it has the advantage of better coverage of system changes. Typically, the best directories to exclude are those, which contain a large number of files for products totally unrelated to the software package, you are about to install. Exercise care when selecting excluded directories since selecting directories like the Windows home directory will prevent the console from detecting important changes to the system.

The following topics provide information about using directories:

Adding a directory

To add a directory to the list of directories to be scanned, proceed as follows:

1. Select **Edit> Add Directory**  .
   A configuration window appears.
2. Select the desired directory from the list of displayed drives and directories.
3. Click **OK** to confirm the addition and to close the window.

Switch between include and exclude mode

To modify the snapshot mode of operation , proceed as follows:

1. Click the arrow to the right of the **Mode** field to open the drop-down box.
2. Select the desired mode of operation.

Text File Extensions

Together with the snapshot file, the console will create an archive of the same name but with a `.STA` extension (Snapshot Text Archive) to contain all text configuration files on the system. Through this file the console will be able to find the exact changes, which took place for every modified configuration file. The files stored in the text archive are all files with extensions specified in the **Text File Extensions** tab. If you do not specify a list, the console will use a default list containing the file extensions `.BAT, .CFG, .INI, .INF` and `.SYS` .

Adding File Extensions

To add a file extension to the list of files to be included into the text archive, proceed as follows:

1. Select **Edit > Add File Extension**  .
   The **Properties** window appears.
2. Enter the file extension to be added into the respective field.

> You can only add one extension at a time.

3. Click **OK** to confirm the addition and to close the window.

Registry

This tab allows you to include or exclude specific branches of the Windows Registry. Not scanning all registry branches reduces the time for snapshot creation and provides, for example, the possibility to exclude all branches which are not save to be transported to other clients. The specifications defined in this tab are valid for all steps of the snapshot process.

The following registry branches can be specified:

Parameter	Description
Scan the Classes (HKCR) Registry Branch	This branch includes all keys which are located under HKEY_CLASSES_ROOT to be scanned if set to true, if set to false all these keys will be ignored.
	This branch scans all keys under the HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft branch if set to true, if set to false all these keys will be ignored.

Parameter	Description
Scan the Microsoft (HKLMSOFTWAREMicrosoft) Registry Branch	
Scan All Branches Other than Classes and Microsoft	If set to true, this option scans all registry keys which are not included in any of the two previously mentioned groups, if set to false all these keys will be ignored.

Modifying the Registry settings

To edit the registry branch scanning settings , proceed as follows:

1. Select a registry entry in the right window pane.
2. Select **Edit > Properties** .
   The **Registry** window appears.
3. Check or clear the desired branch options. Checking activates scanning for the branch, unchecking deactivates.
4. Click **OK** to confirm the modification or **Cancel** to abandon without modification.

Contents of a snapshot

After a snapshot was created or loaded its contents can be viewed in the **Contents** tab. You cannot modify the snapshot contents as these tabs are provided for informational purposes only.

The following topics provide information about using Contents node of a snapshot:

- Files included in a snapshot
- The Registry node
- The Services node of a snapshot
- The snapshot Drivers node

Files included in a snapshot

The **Files** node displays a list of all drives included into the snapshot.

Below the node you can see a node per listed drive with the complete listing of all directories and files contained in that drive very much in the same form as the Explorer. You can move down into the directory hierarchy by selecting it in the left window pane. The right window pane displays the following information about all files included in the snapshot:

Parameter	Description
File Name	This field displays the full name of the file.
Size	This field shows the size of the respective file in bytes.
Modified	This field displays the date and time of the last modification of this file in the default format defined in the user preferences.

The Registry node

The **Registry** node displays all keys and values included into the snapshot.

Below the node you can see a node per listed key with the complete listing of all subkeys contained in the form of an Explorer. You may move down into the hierarchy by selecting a key it in the left window pane. The right window pane displays the following information about all keys and values included in the snapshot:

Parameter	Description
Name	This field displays the complete name of the value of the selected key.
Type	This field displays the type of the value. Possible value types are `String, Binary` and `DWORD` .
Size	This field displays the size of the value in bytes.
Value	This field shows the data of the value. This may either be an integer, a binary value or a string such as `YES` , or a directory path for example.

The Services node of a snapshot

The **Services** node displays all services found on the system at the time of the snapshot. The view in the right window pane displays in tabular format the following information about the included services:

Parameter	Description
Name	This column displays the name of the service.
Path	The **Path** column displays the full path to the executable file of the service.
User	The **User** column displays the account which started the service, normally `LocalSystem` .

The snapshot Drivers node

The **Drivers** node displays all drivers found on the system at the time of the snapshot. The following list box displays in tabular format the following information about the included drivers:

Parameter	Description
Name	This column displays the name of the driver.
Path	The **Path** column displays the full path to the executable file of the driver.
User	The **User** column displays the account which started the driver.

Changes

After you installed (or removed) applications and customized their configuration, all changes made to the reference device system need to be found. This is done in the second step of the snapshot package creation of the console.

In the tabs of this node you can view the details of the changes found and you can also delete any unwanted or irrelevant entries. The console will always find all changed files, regardless of whether they were created as part of the software installation or otherwise. For this reason, it is possible

that the console can find system changes, which are not required to be part of the distributable software package. If this happens, you can manually edit the Change lists by removing entries in any of the lists, which you do not think are correct. You cannot add any entries to any of the lists, but if required you can add any changes or new files directly to the package file later on.

The **Changes** node displays the following general information about the selected package. If the package has just been created the values for all these attributes will be 0, because the list of changes has not yet been created:

Parameter	Description
Creation Date	This field uses the system clock to fill in the date and time of creation of the list of changes.
File Size (KB)	This field displays the total size of the file containing the list of changes in bytes.
Total Archived Files	This field displays the total amount in bytes of the files that were added since the snapshot was taken.
New	The entries of the following fields display the number of new objects added to each group, that is, the number of directories added during installation/uninstallation/update, and thus were added to the list of changes. • **Total New Directories** • **Total New Files** • **Total New Registry Keys** • **Total New Registry Values** • **Total New Services/Drivers**
Changed	The entries of the following fields listed the number of modified objects of each group, that is, the number of registry keys that were changed during installation/uninstallation/update, and thus were added to the list of changes. • **Total Changed Directories** • **Total Changed Files** • **Total Changed Registry Keys** • **Total Changed Registry Values** • **Total Changed Services/Drivers**
Deleted	The entries of the following fields listed the number of objects deleted from each group, that is, the number of files that were removed during installation/uninstallation/update, and thus were added to the list of changes. • **Total Deleted Directories** • **Total Deleted Files** • **Total Deleted Registry Keys** • **Total Deleted Registry Values**

Parameter	Description
	• Total Deleted Services/Drivers

Snapshot package

The main purpose of the **Package** subnode is to create a distributable software package, which can be collected by client devices across a network for automatic installation. The software package is essentially a delta image of the system created after the software product to be distributed was installed on the system. The creation is based on comparing a system snapshot with the state of the system after the software installation and determining the changed files, groups, icons and registry information if applicable. As such, the package can be successfully created only if the Snapshot and Change List creation steps previously described were carried out correctly.

The following topics provide information about using **Package** subnode:

- Compiling package
- Stopping file collection
- The Configuration node of the package factory
- The Contents node of a final snapshot package

Compiling package

After all **Configuration** and **Contents** definitions were executed you proceed to actually create the snapshot. To do so, proceed as follows:

1. Select **Edit > Compile Package**  .
   A confirmation window appears, because this process may take quite some time.
2. To confirm the creation of the snapshot click **Yes** and the process will be launched.

When the process is finished the status bar displays **Done**.

Stopping file collection

The building of a snapshot cannot be interrupted, it can only be cancelled. Being a very lengthy process, be sure to plan you snapshot creation at an appropriate time. Nevertheless, if you have to cancel the process do as follows:

1. Select **Edit > Stop File Collection**  .

The snapshot creation process will be stopped and abandoned immediately.

The Configuration node of the package factory

The **Configuration** displays information about the package that was created via its tabs.

The Contents node of a final snapshot package

The **Contents** node displays a resume of the contents of the created package. It shows the following information:

Parameter	Description
Total Archived Files	This field displays the total number of files that are included in the archive.
File Size (KB)	This line displays the total size of the archive file in KB.
Average Compression	This line displays the average rate of compression of the files included in the archive.

General information of the snapshot package

The **General** tab displays the following general information about the selected package. If the package has just been created the values for all these attributes will be 0, as the list of changes has not yet been created:

Parameter	Description
Archive Type	The **Archive Type** in which the package is stored. Possible values are the .zip format and the BMC proprietary .pkg format.
Creation Date	This field uses the system clock to fill in the date and time of creation of the package.
File Size (KB)	This field displays the total size of the file of the package in bytes.
Total Archived Files	This field displays the total number of files that are included in the package.
Package Status	Displays the status of the package.

Files included in a snapshot package

The **Files** node shows all files in their directory structure which are contained in the snapshot package and which will be installed on the targets.

Below the **Files** node, you can see all files contained in the snapshot package in their tree hierarchy of all directories. When selecting a directory in the left window pane the table in the right pane displays the following information about the files contained in that specific directory:

Parameter	Description
Path	This field displays the full path of the original file location.
Date	This line displays the date and time of creation of the stored file in the default format defined in the user preferences.
Size	This line displays the original size of the file in bytes.
Ratio	This line displays the compression rate.
Stored Size	This line displays the size of the compressed file as stored in the package file in bytes.

Managing Package Folders

For all types of packages, folders can be created. Similar as for any other type of object in the BMC Client Management, Package Folders are created as organisational containers for different types of packages. They can contain any number of package folders and packages for the management of the client system.

It also contains the following subnodes:

- One node for each package folder created under it.
- One node for each package of the respective type that was created directly under the node.

The following topics provide information about managing package folders:

- Creating a new package folder
- Adding a package to a folder
- Creating a new package in a folder
- Renaming an existing package or package folder

Creating a new package folder

To create a new package folder, proceed as follows:

1. Select the respective **Packages** node in the left window pane under the **Package Factory**.
2. Select **Edit> Create Packages Folder** .
   The **Package Folder Name** window appears.
3. Enter the name for the new folder.
4. Click **OK.**
   The new folder will automatically be created and be displayed in the right pane.

Adding a package to a folder

Depending on their type, packages are either added or created: MSI and RPM packages are added as the MSI and RPM package already exists it only needs to be "wrapped" by the in the proper format to be handled. Custom and Snapshot packages are created from the beginning. To add either an MSI or an RPM package, proceed as follows:

1. Select the respective **Packages** node in the left window pane.
2. Select **Edit > Add Package** .
   The respective **Packages** window will appear on the screen. This dialog box provides you with a list of all available drives from which you can select the package to add to the folder.
3. To find the package browse down into the directory tree. Be aware that the package will be copied to its new location, not moved.

4. Below the list of drives select the **Archive type** in which the package is to be stored. You have the choice between the `.zip` format and the BMC Client Management - Software Distribution proprietary `.pkg` format. Which type to select depends on your network environment, because it does not have any impact on the software distribution process itself. For example, if your virus scan software scans `.zip` files, it is recommended to select the `.pkg` archive type, to avoid the virus scan taking 100% CPU.
5. Click **OK** to confirm the operation and to close the window.

When you add an MSI package or an RPM package it will be stored in a newly created folder with its own name under the `data/PackagerMsi` subdirectory, `data/PackagerRpm` , of the local installation directory on the remote computer.

Creating a new package in a folder

Depending on their type packages are either added or created: MSI and RPM packages are added while Custom and Snapshot packages are created from the beginning. To create a new package proceed as follows:

1. Select the respective **Packages** node in the left window pane.
2. Click **Edit > Create Package** .
   The respective **Create a Custom Package** window appears.
3. Enter the name for the new package into the respective field.
4. Through the following check box you can define if the contents of the package are to be compressed or not.
5. Below the list of drives select the **Archive type** in which the package is to be stored. You have the choice between the `.zip` format and the BMC Client Management - Software Distribution proprietary `.pkg` format. Which type to select depends on your network environment, because it does not have any impact on the software distribution process itself. For example, if your virus scan software scans `.zip files` , it is recommended to select the `.pkg` archive type, to avoid the virus scan taking 100% CPU.
6. Click **OK** at the bottom of the window to confirm the new package or **Cancel** to abandon the action.

When a new custom or snapshot package is created, it will be stored in a newly created folder with its own name under the `data/PackagerCustom` subdirectory, `data/PackagerSnapshot` , of the local installation directory on the remote computer.

Renaming an existing package or package folder

You can rename a folder as long as it has no children. After it contains packages it cannot be renamed, because the folder name is integrated into the package path and not modifiable. The name of a package can be changed at any time. To change the name, proceed as follows:

1. Select the package folder node in the left window pane.

2. Right-click you mouse on it and select the **Properties** menu item from the pop-up menu that appears.
   The **Package Folder Name** window appears.
3. Enter the desired name for the folder in the **Folder Name** field.
4. Click **OK** to confirm the operation and to close the window.

Managing Package Factory

BMC Client Management - Software Distribution provides a module which provides several different ways of creating packages and is also responsible for publishing the finished packages to the master server or a collection/depot server for distribution.

1. The user interface of the **Packager** allows for the creation of all types of packages. It handles the different creation types and proposes the appropriate options based on the selected type. Then it creates a container .zip file including all files required for the distribution.
2. In a second step the **Packager** publishes the .zip file. Publishing can be done either directly to the master to store it in the database and make the package available to the whole network. Otherwise the package can be published to a relay, which makes the package available to all its children only. At the same time an information is sent apprising the master of this fact.

All packages created through the **Packager** contain the following information stored in the package's properties file and stored in the master database:

- A unique package identifier which is generated at the time of package creation on a random basis to uniquely tag a package.
- The package name which will be displayed in the master server database to access the package.
- The file checksum which is the checksum of all files and the scripts included in the package.
- A package description which contains further comments on the package.
- The date of creation.
- The date on which the package was last modified.
- The name of the administrator who last modified it.

Any type of device can be a Packager, however, because the **Package Factory** is a restricted module a device must be declared as such. This is done in the client's properties, for more information about this subject refer to the Managing devices topic. By default the master is defined as a Packager. This functionality, the **Package Factory** , is accessible remotely on any computer of the network through the main **Packages** node of the console.

The first-level of the **Package Factory** node lists all devices which are Packagers and the following information about these:

Parameter	Description
Name	The name of the packager device.
IP Address	The IP address of the packager device.
Operating System	The operating system running on the packager device.

The following topics provide information about managing package factory:

- Adding a new packager
- Cleaning up packages that are no longer used

Adding a new packager

To be a **Packager** a device must be declared as such. This can either be done in the properties of the device or in the **Package Factory** node. To add a device to the **Package Factory** as a **Packager** proceed as follows:

1. Select the **Package Factory** node in the left window pane.
2. Select **Edit > Add Packager** .
   The **Add a New Packager** pop-up menu appears.
3. Select the device to be added from one of the list boxes.
4. Click **OK** to confirm and close the window.

The device will be added to the table of Packagers and its configuration parameter will be updated. Also the modules about the available packager types for the device's operating system are automatically loaded, if not done so yet.

Cleaning up packages that are no longer used

This menu item of the **Tools** menu allows you to delete old packages of any type from its storing location (data/Vision64Database/packages) when a new version of the same package displays, that is, when a package was modified and republished. If you have activated the RemoveOldPackages option in the database configuration (Vision64Database.ini) file this operation will automatically be executed, that is, a package will automatically be deleted when a new version of it is published.

To clean up all obsolete packages, proceed as follows:

1. Anywhere in the console select the **Tools > Clean-up Old Packages** menu item.
   The obsolete packages will be automatically deleted.

Packager - Software Distribution

The **Packager** node will provide access to the types of package which are applicable to the operating system of the respective device, that is, under a Windows client you will be able to create MSI, snapshot and custom packages, on a Linux device rpm and custom packages, while on a MacOS computer you can only create custom packages. The types of packages are indicated also via their icons:

Icon	Package Type
	Custom Package
	MSI Package
	RPM Package
	Snapshot Package

The **Packager** nodes have a subnode for each type of package which can be created on the respective device.

The following topics provide more information about using **Packager** node:

- Publishing a package to the master
- Publishing a package to a relay
- Referencing a package
- Sending a package back to a packager

Publishing a package to the master

When you publish an package you make it available to the general public in you network by placing it on the master. To publish a package, proceed as follows:

1. Select the package to be published in the left window pane.
2. Click **Edit > Publish to Master**  .
   The package will copied to the master server and added automatically to the **Packages** node with its existing name.
3. If the package already exists on the master and was tagged with a renaming order when being sent to the device for modification, a window appears to inform you of this fact. Click **OK** to acknowledge.
   Then the **Properties** dialog displays on the screen, in which you must enter a new name for the package.
4. Click **OK** to confirm.

You can follow the status of the publication process in the **Package Status** line in the right window pane of the package. Be aware that the status **Package successfully published to the direct parent.** only indicates that the package has arrived at the parent of the current device and not yet at the master. The status **Package successfully published to target device.** indicates, that the package has arrived at the master and is available for general use.

Publishing a package to a relay

A package does not necessarily have to be made available to the whole network, it can just be needed and thus be published to a specific group of devices. To do so the package can be published to a relay. Be aware that packages cannot be published to relays installed on Window 95 /98/ME operating systems, these cannot be used as **Storage Relays**. To publish a package to a relay, proceed as follows:

1. Select the package to be published to the relay in the left window pane.
2. Click **Edit > Publish to Relay** .
   The **Select a Storage Relay** pop-up menu displays displaying the list of all available relays.
3. Select the desired relay from one of the list boxes.
   The package will copied to the relay and added automatically to its **Packages** node with its existing name.

You can follow the status of the publication process in the **Package Status** line in the right window pane of the package. Be aware that the status **Package successfully published to the direct parent.** only indicates that the package has arrived at the parent of the current device and not yet at the target relay. The status **Package successfully published to target device.** indicates, that the package has arrived at the target relay and the master has received this information, thus the package is now available for general use.

Referencing a package

A package can also only be referenced by the master, that is, the master receives all information about the package but not the package itself. The package in this case is stored in a specific location, which, for example, can also be a removable unit such as a CD/DVD or a USB key, and a relay which requires the package for itself or its clients will verify the given location before requesting it from the master. To reference a package, proceed as follows:

1. Select the package to be referenced in the left window pane.
2. Click **Edit > Reference Package** .
   All information about the package is directly sent to the master.

Sending a package back to a packager

A package, once published to the master, might have to be modified again later on, either on the device it was created on or on another device. Make sure that the device you intend to send the package to is enabled with the **Package Factory** , that is, it is a Packager, and that it's operating system is compatible with the package type, otherwise it cannot be modified. To send the package for modification to a device, proceed as follows.

1. In the **Packagers** tab of the package to be sent to another device select **Edit > Send Package** .
   The **Send Package to Packager** pop-up menu appears.
2. Select the device to which to send the package to from one of the list boxes.
3. You can also specify if the package is to be renamed when it is being uploaded to the master again. In this case mark the **Force Rename** check box below the list of devices.
4. Click **OK** to confirm and to close the window.

The package is now sent to the device, you can follow the progress via the **Status** value of the table.

Bulk-importing MSI packages

BMC Client Management allows you to import a whole group of MSI files and automatically create the MSI packages. This functionality is available on the browser agent interface and must be executed on the packager device.

> **Note:**
>
> To access this page you must log on as an administrator.

To import MSI files proceed as follows:

1. Enter the the following information into the browser window: `http://<host name>:<console port number>/msiimport`

   > The host name is in this case the name or IP address of the packager device. The msi files that you want to import must also be stored somewhere on this device.

   The **Import Multiple MSI Files** page appears.
2. Enter the required information into the following boxes:
   a. **Folder Containing MSI Files** : Enter into this text the full path to the folder that contains the .msi files to import, for example **C:\temp\import\msi**

      > Be aware, that only .msi files located directly under this folder are imported, any files located in subdirectories will be ignored.

b. **Destination Folder in Console** : Enter into this text box the name of the folder and its path relative to the **Packages > Package Factory > Your Package Factory > MSI Packages** node, into which the automatically created packages are to be saved, for example **Import** . If the folder does not yet exist it is created.
c. **Publish to Master (after Creation)** : Check this box if the packages are to be automatically published to the master, once they are created in the CM database. This means that they are immediately available for package distribution within the CM environment.

> The packages will be published in a subdirectory directly under the main **Packages** node with the same name as that into which they were imported under the package factory, for example, **Import** .

d. **Package Compression Format** : Under this label select the corresponding radio button to either save the MSI package in the standard .zip format or in the proprietary .pkg format.
e. **User Interaction Level** : Select from this list box to which extent the local user should be implicated in the installation of the msi package when it is sent to the target device.
f. **Delete MSI After Installation** : Check this box to delete the package after it was installed on all targets.

3. Click **Process** to launch the msi import and package creation process.
   The browser refreshes and displays the **MSI Import Ready to Process** page. It displays the number of msi files found in the specified folder.
4. If all is correct click **Yes** to confirm.
   The browser displays the **Yes** page which shows the progress of the import, the overall status of the import in the form of a bar, that changes color and displays the progress as a percentage. The **Detailed Status** panel of the view shows the list of all msi files found and their current import status.
   The import is finished when the bar is completely green and displays 100% and all individual status values for all msi files to import display **Success**.

Managing Transfer Windows

Bandwidth management is the ability to plan when data transfer to a client workstation takes place. This function helps optimize network utilisation by providing the ability to define a period (days or hours), a transfer speed and a size threshold for multicast distribution. Bandwidth management is done from the CM console through transfer windows.

All transfer windows are created and managed under the **Global Settings > Transfer Windows** node. A transfer window (or Distribution Window) permits you to assign one or several timeframes to a group of clients, during which the transfer of data is permitted. They are used to manage the list of allowed or disallowed hourly "slots" during which the agents in the network can communicate

with each other. A transfer window's role is to provide a simple lookup service to verify whether the data transfer can take place through the **Data** channels and if yes, at what speed. Be aware that the transfer window only provides the lookup service and does not have direct control over the network usage.

Transfer windows address issues with LAN/WAN configurations in such a way that, for instance, it is possible to configure WAN transfers as unicast and LAN transfers as multicast. This will avoid sometimes complex router configuration (multicast being available by default on LAN).

Generally transfer windows are assigned to the targets, because it is the target side that limits the bandwidth. However, if the relay uses the same bandwidth for its communication with the master as the clients use with the relay, the transfer window only needs to be assigned the relay and share its transfer window with its children.

Each transfer window consists of information about network usage for every hour of the week, starting from 0:00 on Monday all the way to 23:00 on the following Sunday. As such the window does not, and cannot, control network traffic based on anything such as predefined calendar dates or times. As an example, the setting configured for the 8:00 slot on Wednesday controls network communication between 8:00 and 8:59:59 for every Wednesday regardless of date. A transfer window authorizes, for example, the transfer of the package to the client, but does not execute it, and it might have more than one client. However, a device cannot be assigned to more than one transfer window of the same type.

Transfer windows also define if a file transfer is executed as unicast, that is, if the file is sent directly and individually to each target client, or if the delivery is executed via a multicast. For more detailed technical information about this delivery mode refer to Multicast Software Delivery . The parameters for the multicast transfer are defined in the configuration file of the FileStore module, which deals with all data transfers of the BMC Client Management . You will find details on these in the File Store module parameters topic.

The following topics provide more information about managing transfer windows:

- Planning - Transfer Windows
- Creating transfer window
- Defining transfer window time-slots
- Locally Accessing Transfer Windows

Planning - Transfer Windows

Transfer windows allow for a better optimization of network traffic by defining when transfers should take place and what percentage of bandwidth to use at each transfer period. The hourly slots are represented in the visual form of a spreadsheet. Each slot or cell represents the allowed network activity of one hour of the week. By consulting this planning, agents know if they can communicate using the network and to what extent. The numbers defined in each slot are interpreted depending on the window's settings.

The first step in managing the network bandwidth is to define the network unit and the channel for the data. These settings apply to all slots in the window, meaning that slot types cannot be mixed in the same window.

Parameter	Description
Unit	This drop-down box appears for the unit in which the bandwidth is calculated for the table following it. To change the value, click the arrow at the right of the box and select the desired value from the list. The units marked with Total are useful when hourly bandwidth amounts are fixed, for example, 400 MB per hour.
Channel	This drop-down box defines the channel of the data for the transfer window. The possible values are: • **Notification:** The master, server or relay informs its children that data (for example, packages, operational rules) are waiting for them on the parent. • **Data:** Interagent data transfer (from one level to another: upstream/downstream or downstream/upstream). Data can be operational rules, packages, inventories, etc. • **Multicast send** To change the value, click the arrow at the right of the box and select the desired value from the drop-down list. This setting indicates whether the window controls apply to data delivery and reception, notification communications or if it defines a multicast software delivery mode.
Shareable	Check this box if the transfer window is to be applied as well to all children of the device (relay) this transfer window will be assigned to. Be aware, that if a child already has a transfer window of this type assigned, it will ignore this new transfer window, because a device can only be assigned one transfer window of each type. Also the client will only check for transfer windows shared by its relay after an agent restart. This option is deactivated if the channel is **Multicast send.**

Creating transfer window

It is also possible to directly create a new transfer window in this tab. To create a new transfer window, proceed as follows:

1. Select **Edit > Create Transfer Window**  .
   The **Properties** dialog box appears.
2. Enter the desired data into the respective boxes.
3. Click **OK** at the bottom of the window to confirm the data for the new transfer window.

Defining transfer window time-slots

To define or modify the network load in the table for the different time-slots proceed as follows. If the transfer window is to be used for multicast delivery, at least one slot must be filled in, otherwise the file transfer will be executed via unicast.

1. Select the **Unit** and the **Channel** above the table.
2. Click the slot which is to be edited.

> You can also select a range of slots by dragging your mouse button over the desired range.

3. Click **Edit > Define Time-slot** .
   The **Define Transfer Window Time-Slots** window appears.
4. Edit the value into the text box for the selected time-slot.

> Make sure to use a value in accordance with the **Unit** you have previously chosen.

5. Click **OK** to confirm the value and close the window.
   The value you entered was defined for either the one box or for the whole range of boxes you selected.
6. Repeat these steps for all other slots or ranges to be defined or modified.

Locally Accessing Transfer Windows

The **Transfer Windows** node shows if there are any transfer windows associated with the remote device and if so displays the following information about them. Clients can only have a maximum of three transfer windows assigned, one of each type.

Parameter	Description
Name	The name of the transfer windows associated with this client.
Shareable	Shows if the transfer window is to be used by the relay's children as well as the relay itself, which can be either true for shareable or false for not shareable.
Channel	This field indicates the transfer window channel which can be one of the following: • **Notification** - the master server or relay informs its children that data (for example, packages, operational rules) are waiting for them on the parent. • **Data** - interagent data transfer (from one level to another: upstream/downstream or downstream /upstream). Data can be operational rules, packages, inventories, and so on. • **Multicast send** - defines a multicast software delivery mode.
Slot Type	This field displays the unit in which the bandwidth is calculated. Possible values are **Bytes/second** , **KBytes/second** , **MBytes/second** , **Total Bytes Sent** , **Total KBytes Sent** and **Total MBytes Sent** .

Managing Storage Relays

The **Storage Relays** tab is available for all different types of packages and provides the list of all relays to which a copy of the package was sent, to be stored for download by the target clients and the master, that automatically also receives a copy.

The following device list table provides the information about managing Storage Relays:

Parameter	Description
Status	Above the table the current status of the package displays, that is, where in the whole process it currently is.

Parameter	Description
Device Name	Displays the names of the relays to which a copy of the package was sent and the master.
Status	Displays the current status of the package on the respective relay device, possible values are `Waiting to Publish` ( ), `Package Sent` ( ), `Package Published` ( ) or `Publication Failed` ( ).
Package Up to Date	Indicates if the package currently stored on the relay is up to date, possible values are **Yes** , if it is up to date or **No** , if modifications were made to the package and it was not yet resent to the storage relay.
Retry Count	This field lists how many times the package was sent before the operation was successful or failed, up to the maximum number of retries defined for the module.
Last Send Time	The date and time the package was sent for the last time to the storage relay or the master in the standard time format.

The following topics provide information on publishing packages:

- Publishing a package to the master
- Publishing a package to a relay
- Publishing to selected device

Publishing a package to the master

When you publish a package you make it available to the general public in you network by placing it on the master. To publish a package, proceed as follows:

1. Select the package to be published in the left window pane.
2. Click **Edit > Publish to Master** .
   The package will copied to the master server and added automatically to the **Packages** node with its existing name.
3. If the package already exists on the master and was tagged with a renaming order when being sent to the device for modification, a window appears to inform you of this fact. Click **OK** to acknowledge.
   Then the **Properties** dialog displays on the screen, in which you must enter a new name for the package.
4. Click **OK** to confirm.

You can follow the status of the publication process in the **Package Status** line in the right window pane of the package. Be aware that the status **Package successfully published to the direct parent.** only indicates that the package has arrived at the parent of the current device and not yet at the master. The status **Package successfully published to target device** indicates, that the package has arrived at the master and is available for general use.

Publishing a package to a relay

A package does not necessarily have to be made available to the whole network, it can just be needed and thus be published to a specific group of devices. To do so, the package can be published to a relay. Be aware that packages cannot be published to relays installed on Window 95 /98/ME operating systems, these cannot be used as **Storage Relays**. To publish a package to a relay , proceed as follows:

1. Select the package to be published to the relay in the left window pane.
2. Click **Edit > Publish to Relay** .
   The **Select a Storage Relay** pop-up menu displays displaying the list of all available relays.
3. Select the desired relay from one of the list boxes.
   The package will copied to the relay and added automatically to its **Packages** node with its existing name.

You can follow the status of the publication process in the **Package Status** line in the right window pane of the package. Be aware that the status **Package successfully published to the direct parent.** only indicates that the package has arrived at the parent of the current device and not yet at the target relay. The status **Package successfully published to target device** indicates, that the package has arrived at the target relay and the master has received this information, thus the package is now available for general use.

Publishing to selected device

If a package was modified it must be resent to all its relays and the master to ensure that the available packages are up-to-date. To to so, proceed as follows:

1. Select all devices to which the package is to be republished in the table in the right window pane.

   > Be aware, that in this case you must also select the master, if the package is to be published to it again, this will not be automatically be done as with the first publication.

2. Select **Edit > Publish to Selected Device** .

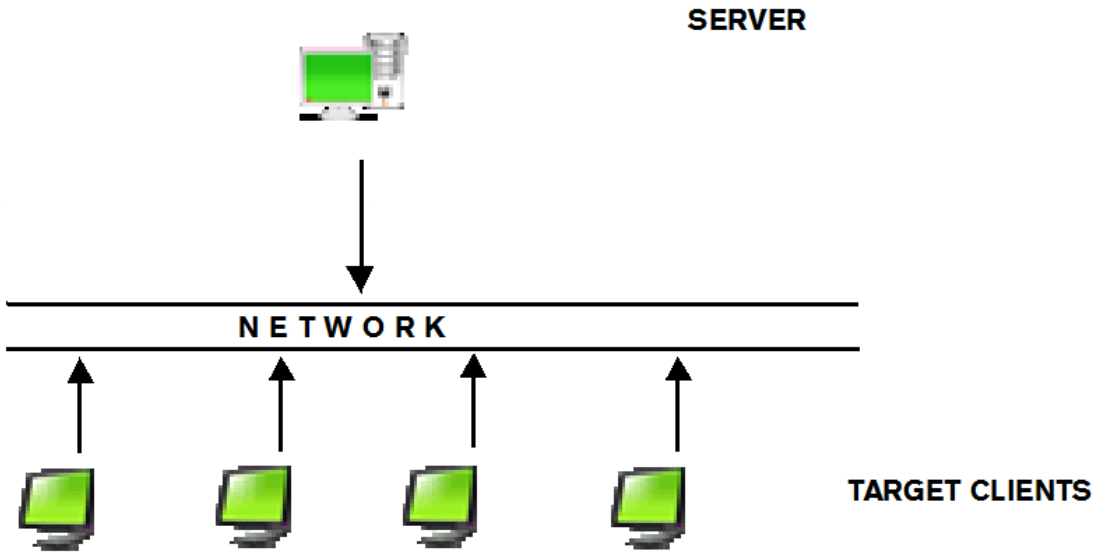
The package will now be sent directly to all selected devices.

> **Note:**

When the package is published it is stored on the master server with its original name in a folder of the same name either under the default directory `.../data/Vision64Database/Packages` subdirectory of the local installation directory or in a directory specified in the configuration file `Vision64Database.ini` .

Multicast software delivery

Multicast delivery enables parallel software distribution to an unlimited number of client systems while simultaneously reducing server and network resource requirements and bandwidth consumption for high-volume, high population software distribution.



The CM multicast capabilities enable software to be distributed to thousands of desktops in the same time it takes to deliver software to a single desktop, while making optimal use of server and network resources.

Unicast	A separate copy of the information is sent to each client individually and at the same time. This can be done at any time. This is the regular way of transferring data in the BMC Client Management - Software Distribution and will thus not be explained in any detail in this document.
Multicast	One copy of the file information is sent to all clients at once via a unicast transfer at notification time, to advise the client to listen on the specified address and port to recuperate the blocks of the multicast transfer.

Multicast delivery enables parallel software distribution to a virtually unlimited number of client systems while simultaneously reducing server resource and network bandwidth requirements for high-volume, high-population software distribution. The multicast principle is to send a file on a virtual multicast address advertised to all target clients where each of these will get the file. Contrary to unicast, the server sends the file only one time.

Based on UDP protocol, it also has the advantage of being able to transfer this data without knowing beforehand when the targets connect nor how long they remain connected. It is therefore the perfect transport mode for e-business application distribution or for nomad targets. The clients can connect and disconnect at any time to recover the data frames. Depending on the settings of the multicast parameters the server might never stop sending packets to the multicast address, therefore clients can pick them up whenever it is the most convenient for them. This is specially useful to meet the software distribution needs of remote and mobile devices where network access and bandwidth are irregular or unpredictable.

The choice to transfer a package via the multicast channel is defined through a transfer window. If the multicast option is selected, the files can be transferred in multicast mode if they respect some conditions.

1. Server Unicast Announcement
   If a transfer window is configured for multicast transfer the Server contacts each client concerned by the transfer through the notify thread of the FileStore module and informs it that a transfer is going to start on a specified address and port. The client immediately begins listening on this address and port and answers the request that it is listening. The server stores the replies and checks if all conditions are valid for the transfer in multicast mode:
   - The size of the file to be transferred has to be larger than the size defined in the configuration parameters.
   - A minimum number of clients must have replied to the announcement.
   - The maximum retry number must not yet were reached.
   - A delay is necessary before the start of the notification, to allow clients to answer to the assignment.
   - In multicast mode the relay never informs the clients that files are available.
     After all parameters were verified and found to be valid, the notify thread informs the multicast thread by setting a flag (TransferToBeStarted) to start sending the file in multicast mode.If one parameter is found to be invalid the transfer will start as well, but it will be sent in unicast mode.
2. Client Unicast Reception
   If the client is online and has received the notification from the server, the client:
   - starts listening on the specified address and port, and
   - replies to the server that it has received the notification and is listening.
     If target clients are currently not connected or are nomads, the multicast parameters may be specified in such a way, that they can send back their request when logging on, and still have the opportunity to recover all data frames without having to reschedule the software delivery.
3. Multicast Data Transfer
   The server waits for the specified delay and then begins to send blocks of the file to be transferred. The header of each block contains the starting and stopping offset of the file. The client receives the block, determines its position and inserts it in the file. No processing of the file will be carried out until the client has received all blocks and the file is complete.

Clients that did not receive the announcement the first time, because they were switched off, for example, will receive further notification by the server. Depending on the parameter settings either of the following situations can ensue:

- Based on the number of requests, the server will again decide whether to use multicast or unicast transfer for the retry.
- If the number of retries is set very high, the blocks of the file continue to be sent through the network and the clients, which just relogged on to the network, can start recuperating the blocks.

4. **Post-Transfer**
   At the end of the first transfer of all blocks, the relay asks the clients if they have recovered the complete file. In this case they stop listening. If it is missing blocks it will wait for a retry to recover the missing pieces. If the file is not complete when the multicast mode is stopped according to the retry parameter (MulticastRetry), the relay demands the client to stop listening. The multicast transfer can also be stopped after a transfer if the specified success rate (MulticastMinimumSuccessRate) is reached. After the transfer the retry parameter will be reset to allow for a new multicast delivery of this package.

Due to the fact that Multicast is integrated with the **Transfer Windows** node of the console, the use of this protocol is generic and no specific configuration is required for each distribution. The parameter settings for the multicast functionality are defined in the configuration file of the FileStore module, `FileStore.ini` , of the server which sends the data.

The following topics provide more information about using multicast software delivery:

- Configuring multicast
- Locally accessing multicast delivery information

Configuring multicast

Multicast transport must be properly configured before it can be used in your network. It is defined with standard settings for 128KB/s transfer speed within the network, if this fits your requirement no other configuration is necessary.

The multicast configuration parameters are part of the File Store module and can be defined and edited in the respective node under the **Agent Configuration** -> **Module Configuration** node of the individual devices. To modify these parameters, proceed as follows:

1. Select the device for which the multicast settings are to be defined in the left window pane.
2. Then go to the device's **Agent Configuration > Module Configuration > File Store** node in the left window pane.
3. Select any line in the table in the **Parameters** tab of the right window pane of the respective module.
4. Select **Edit > Properties**  .
   The **Properties** pop-up menu appears.
5. Make the appropriate modifications to the individual values.

6. Click **OK** to confirm the modifications and close the window.

The new module settings will be taken into account immediately.

Locally accessing multicast delivery information

The **File Store** module is used by all other modules of the agent and is used to move data between higher-level and lower-level devices via the **Data** and **Notification** channels. A cascading system is used from one device to another to transport the data.

This topic includes:

- Multicast
- Multicast details

Multicast

This tab displays the following details about the executed Multicast transfers and those currently being transferred. After the transfer is terminated the information will be removed from the table:

Parameter	Description
Multicast Address	This is the virtual address from which the target clients are collecting their transfer. There can be duplicate addresses in this field, one for each status listed in the following table, which is currently assigned to a connected device.
Status	The status of the current transfer.
Count	The number in this field indicates how many devices are currently connected to the virtual address with the respective status.

Multicast details

This tab displays the Multicast details individually per device after it has finished recovering a package per Multicast. After a transfer is terminated the information will be removed from the table. It provides the following details:

Parameter	Description
Multicast Address	This is the virtual address from which the target clients are collecting their transfer. There will be duplicate addresses in this field, one for each device that is currently trying to recover or having finished to recover a package from this address.
IP Address	The IP address of the target device.
Status	The status of the current transfer.

Managing common content and configuration

The following sections explain the nodes and tabs which are common in their function and about their content to the different types of packages.

- The Contents node
- Packages configuration

The Contents node

The **Contents** node provides you with a list of the contents of the package, through which you can verify that the package is complete and provides you with access to the scripts included with the packages for possible modifications.

This topic includes:

Adding files to a package

After having defined all installation options through the contents of the **Configuration** and **Contents** nodes, the RPM package is created. You can add now files to this package which will then be sent to the targets for installation. To add files, proceed as follows:

1. Click **Edit> Add Files to Package** .
   The **RPM Packages** dialog box appears.
2. The **Add Files** tab provides the list of all available drives through which you can go down in their hierarchy to select the files to be added to the `.zip` file.
3. Click **OK** at the bottom of the window to confirm the additions or **Cancel** to stop and close the window.

Files for a custom package

Below the **Files** node you can see all files contained in the package in their tree hierarchy of all directories. When selecting a directory in the left window pane, the table in the right pane displays the information about the files contained in that specific directory.

Adding Files to the custom package

To add files to the custom package proceed as follows:

1. Select **Edit> Add File** .
   An Add Files dialog box appears on the screen providing the list of all available drives.
2. Go down in their hierarchy to select the files to be added to the package.
3. Click **OK** at the bottom of the window to confirm the additions or **Cancel** to stop and close the window.

Mapping Files to a different location at the target

To map a file or directory to another target location or to modify an existing mapping, proceed as follows:

1. In the **Mapping** tab select **Edit> Map** .
   The **Mapping** window opens on the screen.

2. Enter the source and destination paths into the respective text boxes or modify them.

   > You can enter the path as a relative or complete path and it is possible to use environment variables as well.

3. Click **OK** at the bottom of the window to confirm the mapping or **Cancel** to stop and close the window.

Files for an MSI package

The **Files** node for MSI packages displays all files in their directory structure which are contained in the original package. No file can be added here.

Below the **Files** node you can see a tree hierarchy of all directories and files contained in the MSI package. When selecting a directory in the left window pane, the table in the right pane displays the information about the files contained in that specific directory.

The Additional Files node

Through the **Additional Files** node you can add extra files to the package which are needed by the MSI package for its installation, no other files can be added here.

Scripts

The **Scripts** subnode of the **Contents** node of all different types of packages of allows you to edit the default scripts which are included with the package to be executed at a specific time during installation.

The **Scripts** node has the following subnodes:

- **Pre-Install Script**
  The `preinstall.chl` will be executed before the installation. This script is automatically created when the package is created. By default it already contains a number of predefined procedures, such as error handling. If you intend to use it, don't forget to provide the error information at the respective location.
- **Post-Install Script**
  The `postinstall.chl` will be executed after the installation. This script is automatically created when the package is created. By default it already contains a number of predefined procedures, such as error handling. If you intend to use it, don't forget to provide the error information at the respective location.

Editing a script

To edit an existing or newly created script, proceed as follows:

1. Select the script to edit in the left window pane.
   The right window pane will open as a normal text editor.
2. Create/Edit the script in the right window pane.

3. After you finish the script and return to another point in the console, the console will try to compile the script to verify it is correct.
   If it is not correct an error message appears.

Packages configuration

The **Configuration** node provides access to different aspects available for the configuration of the different packages. Depending on the type of package some of the tabs might *not* be available.

The following topics provide more information about different configuration aspects available for different packages:

- Overwrite
- The Installation tab
- Files to be present
- Files to be absent
- Run as
- Mapping
- Dependencies
- Package installation options

Overwrite

The **Overwrite** tab defines which files the package can overwrite when installing on the target and which it is not to touch.

> **Note:**
>
> This tab is only available for custom packages.

Modifying the overwrite options

To modify any of the previously listed options proceed as follows:

1. Select either one of the lines in the table of the right window pane.
2. Select **Edit** > **Properties** .
   The **Properties** window appears.
3. Make the required modifications in the two drop-down boxes.
4. Click **OK** to confirm the modifications and to close the window.

The Installation tab

The **Installation** tab provides information about the execution of the installation of the package on the target(s).

MSI Package

The options provided in this tab depend on which type of installation you selected in the **General** tab. The possible values for most of these options are true and false, true meaning the entry will be applied, false not applied or you might have to provide data in a text field. Following you will a selection of possible options. For more information about these and other options not mentioned here refer to the Microsoft MSI documentation.

Files to be present

The **Files to be Present** tab for all types of packages is concerned with the definition of files that must absolutely be already installed on the target computer. If these files are not there, the installation or later execution of the installed software will fail. This tab is not available for MSI packages.

An example of files required for successful operation might be the OLE 2.0 DLLs, which are resident in the Windows directory but are used by most large applications. Such files are not usually added to the system if already present, so it is vital that the console detects the software dependencies on them.

Adding a file to the list of the files to be present

To add a file to the list of files to be present on the target, proceed as follows:

1. Select the **Configuration** node in the left window pane and the **Files to be Present** tab in the right pane.
2. Select **Edit> Add File**  .
   The "configuration" window appears.
3. Select the required file from the file hierarchy displayed in the list window.
4. Click **OK** to confirm the addition and to close the window.

Files to be absent

The **Files to be Absent** tab is concerned with files which must absolutely not be found anywhere on the target computer for the installation to proceed. Examples for such files might be the largest executable files to ensure that the same software will not be installed twice. This tab is not available for MSI packages.

As with the required present files, these files will be automatically added to the list of files, which must be absent from the client system. Same as with the present files, you can specify additional files, which will be required to be absent by the client agent before the installation starts, or you can remove files from the list.

Adding a file to the list of files to be absent

o add a file to the list of files to be absent on the target, proceed as follows:

1. Select the **Configuration** node in the left window pane and the **Files to be Absent** tab in the right pane.
2. Select **Edit> Add File**
   

.
A configuration window appears.
3. Select the required file from the file hierarchy displayed in the list window.
4. Click **OK** to confirm the addition and to close the window.

Run as

The **Run as** tab defines which login the script is to use and what to do if the login fails. This tab is not available for RPM packages.

Editing the Run as definitions

To modify the definitions of the run as function proceed as follows:

1. Select any line in the table in the right window pane.
2. Click **Edit** > **Properties** .
   The **Properties** pop-up menu appears.
3. Make the appropriate modifications to the individual values.
   The new definitions will be taken into account immediately.

Mapping

This tab allows you to define specific mappings for files and directories. It is only available if mapping was selected as an option when the package was created.

Mapping a file or a directory to another path

1. In the **Mapping** tab select **Edit** > **Map** .
   The **Mapping** window opens on the screen.
2. Enter the source and destination paths into the respective text boxes or modify them.
   You can enter the path as a relative or complete path and it is possible to use environment variables as well.
3. Click **OK** at the bottom of the window to confirm the mapping or **Cancel** to stop and close the window.

Dependencies

The tab displays installation and execution information recovered from the RPM package. This information is view only and cannot be modified.

Package installation options

The **Installation Options** tab provides information about the execution of the installation of the package on the target(s).

The options provided in this tab depend on which type of installation you selected in the **Installation** tab. The possible values for most of these options are true and false, true meaning the entry will be applied, false not applied.

Software distribution wizards

Packages in the BMC Client Management - Software Distribution can be created and executed in different ways. The BMC Client Management - Software Distribution wizards are one of the easiest ways to create and distribute software packages across your whole infrastructure in a quick and easy way. BMC Client Management - Software Distribution provides several wizards for the these tasks. The following wizards are available and can be launched from different locations in the console:

- Package Creation Wizard
- Package Distribution Wizard

Managing Package Creation Wizard

The **Package Creation Wizard** guides you through the individual steps required to create a new MSI, RPM or custom package. Depending on the selections, the wizard will be composed of different windows. Below you can see explanations for the wizard in its most complete form.

The wizard can be launched from anywhere in the console via the **Wizards > Package Creation Wizard** menu item or directly from the dashboard.

The section includes following topics:

- Package Factory
- Custom Package
- MSI Package
- RPM Package
- Present and Absent Files
- Run as options
- Pre-install script and post-install script
- Add Files
- Additional Files
- Map Files
- Publication

Package Factory

In this first window, **Package Factory** , you need to select the **Package Factory** on which the new package is to be created and the type of the package to be created.

1. Select the name of the device which is to be used as the **Packager** from the list.
    a. To add a new **Packager** click **Packager** .
    The **Add a New Packager** pop-up menu appears.
    b. Select the device to be added from one of the list boxes.
    c. Click **OK** to confirm and close the window.
    d. Now select the newly added **Packager** from the list.
2. In the panel **Package Type.**

- the **Custom Package** option will always be available
- the **MSI Package** option only on Windows **Packager**
- the **RPM Package** option only for **Packager** with a Linux operating system

3. Click **Next** to continue.

Custom Package

In this window, the basic parameters of the new *custom package* must be configured:

1. Enter a name for the new *custom package* .
2. Define the basic parameters for the package by selecting the necessary options from the drop-down lists or checking/unchecking the respective options.
3. In the **Options** panel define which other package configuration operations you need to make by checking the respective boxes.
4. Click **Next** to continue.

The following topic provides more information about installing custom packages:

Custom Package installation options

In this window, all parameters about the actual installation process must be defined:

1. Enter the required information in text boxes of the **Installation** panel and make your selections by checking the respective boxes.
2. In the **Overwrite** panel define which files the package can overwrite when installing on the target and which it is not t o touch, by checking the respective boxes.
3. Click **Next** to continue.

MSI Package

In this window, the basic parameters of the new *MSI package* must be configured:

1. Select the MSI package by clicking **Select** to the right of the **Name** box.
   The **MSI Packages from [IP Address]** dialog displays on the sceen.
2. Find the desired package in the hierarchy of the device and select it.
3. Define the archive type for the *MSI package* in the **Archive Type** box.
4. Specify a folder if the new *MSI package* is to be created in a specific folder.

> If no value is entered in this text box the new package will be published directly under the **Packages** top node.

5. Click **OK** to confirm.
   The dialog closes and the name of the selected msi package displays in the wizard box.
6. Define the basic parameters for the package by selecting the necessary options from the drop-down lists or checking/unchecking the respective options.

7. In the **Options** panel define which other package configuration operations you need to make by checking the respective boxes.
8. Click **Next** to continue.

The following topic provides more information about installing MSI package:

MSI Package installation options

In this window, all parameters about the actual installation process must be defined:

1. Make the required selections in the drop-down lists of the **Installation** panel.
2. The **Overwrite** panel allows you to more specifically configure the installation of the *MSI package* . The options provided in this panel depend on which type of installation you selected in the **Installation** panel above. The possible values for most of these options are `true` and `false` , `true` meaning the entry will be applied, `false` not applied or you might have to provide data in a text field. For more information about these and other options not mentioned here refer to the Microsoft MSI documentation.
3. Click **Next** to continue.

RPM Package

In this window, the basic parameters of the new *RPM package* must be configured:

1. Enter a name for the new *RPM package* .
2. Define the basic parameters for the package by selecting the necessary options from the drop-down lists or checking/unchecking the respective options.
3. In the **Options** panel define which other package configuration operations you need to make by checking the respective boxes.
4. Click **Next** to continue.

The following topic provides more information about installing RPM package:

RPM Package installation options

In this window all parameters about the actual installation process must be defined:

1. Enter the required information in text boxes of the **Installation** panel and make your selections list.
2. In the **Installation Options** panel define which files the package can overwrite when installing on the target and which it is not to touch, by checking the respective boxes.
3. Click **Next** to continue.

Present and Absent Files

This window allows you to add files that must be present or absent when distributing the package. The first table adds files that must be present, the second panel lists files that must be absent.

> **Note:**

This window is not available for MSI packages.

The **Files to be Present** panel for all types of packages is concerned with the definition of files that must absolutely be already installed on the target computer. If these files are not there, the installation or later execution of the installed software will fail.

An example of files required for successful operation could be the OLE 2.0 DLLs, which are resident in the Windows directory but are used by most large applications. Such files are not usually added to the system if already present, so it is vital that the console detects the software dependencies on them.

The **Files to be Absent** panel is concerned with files which must absolutely not be found anywhere on the target computer for the installation to proceed. Examples for such files could be the largest executable files to ensure that the same software will not be installed twice.

As with the required present files, these files will be automatically added to the list of files, which must be absent from the client system. Same as with the present files, you can specify further files, which will be required to be absent by the client agent before the installation starts, or you can remove files from the list.

To add a file to the list of files to be present or absent on the target, proceed as follows:

1. Click **Add File** .
   The **Files Present from [IP Address]** dialog appears.
2. Find the desired package in the hierarchy of the device and select it.
3. Click **OK** to confirm.
   The dialog closes and the name of the selected msi package displays in the wizard field.
4. Click **Next** to continue.

Run as options

This window defines which login the script is to use and what to do if the login fails.

1. Enter the required information into the respective boxes.
2. Click **Next** to continue.

Pre-install script and post-install script

This section provides information about pre-install and post-install scripts.

Pre-install Script

The **preinstall.chl** will be executed before the installation. This script is automatically created when the package is created. By default it already contains a number of predefined procedures, such as error handling. If you intend to use it, don't forget to provide the error information at the respective location.

1. You can directly create and edit the script in the provided panel.

2. To verify that the script compiles click **Compile Script** a the top of the panel.
   Any compilation errors that might occur are displayed in the following panel.
3. Click **Next** to continue.

Post-install Script

The **postinstall.chl** will be executed after the installation. This script is automatically created when the package is created. By default it already contains a number of predefined procedures, such as error handling. If you intend to use it, don't forget to provide the error information at the respective location.

1. You can directly create and edit the script in the provided panel.
2. To verify that the script compiles click **Compile Script** at the top of the panel.
   Any compilation errors that might occur will be displayed in the following panel.
3. Click **Next** to continue.

Add Files

This window shows all files in their directory structure which are contained in the custom package and which will be installed on the targets:

To add files to the custom package, proceed as follows:

1. Click **Add File** .
   The **Files Present from [IP Address]** dialog appears, providing the list of all available drives.
2. Find the desired file(s) to be added to the package in the hierarchy and select it/them.
3. Click **OK** to confirm.
   The dialog closes and the files were added to the view and the package.
4. To map a file or directory to another target location select it in the view.
5. Click the **Map** icon.
   The **Mapping** dialog appears.
6. Enter the source and destination paths into the respective boxes.

> You can enter the path as a relative or complete path and it is possible to use environment variables as well.

7. Click **OK** at the bottom of the window to confirm the mapping.
8. Click **Next** to continue.

Additional Files

This window allows you to add extra files to the package which are needed by the MSI package for its installation, no other files can be added here.

To add files to the MSI package, proceed as follows:

1. Click **Add File** .
   The **Files Present from [IP Address]** dialog appears, providing the list of all available drives.
2. Find the desired file(s) to be added to the package in the hierarchy and select it/them.
3. Click **OK** to confirm.
   The dialog closes and the files were added to the view and the package.
4. Click **Next** to continue.

Map Files

This window allows you to define or modify specific mappings for files and directories, that is, to define the location on the target device if it is different from the original package location.

> **Note:**
>
> This window is only available for *custom package* .

To map a file or directory to another target location or to modify an existing mapping, proceed as follows:

1. Select the entry to be mapped to another location in the list view.
2. Click **Map** .
   The **Mapping** dialog appears.
3. Enter the source and destination paths into the respective boxes.You can enter the path as a relative or complete path and it is possible to use environment variables as well.
4. Click **OK** at the bottom of the window to confirm the mapping.
5. Click **Next** to continue.

Publication

This window allows you to define on which device in your network, the newly created package is to be published. Publishing a package signifies in this case making it available for distribution within the network after creation or modification.

1. Select the radio button for the option to use for publication.
   - Select the **Publish to Master** radio button if the package is to be made available to the general public in you network.
   - Select the **Publish to Relay** radio button to publish the package on one or more relays. This option should be used if the package does not need to be available to your whole network, only to one or more subnetworks.

- Select the **Reference Package** radio button to publish the package as a reference. The package in this case is stored in a specific location, which, for example, can also be a removable unit such as a CD/DVD or a USB key, and a relay which requires the package for itself or its clients will verify the given location before requesting it from the master.A package can only be referenced by the master, that is, the master receives all information about the package but not the package itself.

2. If you selected the **Publish to Relay** option you need to define to which relays the package is to be published. For this click **Add Relay** .
   The **Select a Storage Relay** dialog appears.
3. Select the desired relay from one of the list boxes.
4. Click **OK** at the bottom of the window to confirm.
5. Click **Finish** to confirm all values and to create and publish the package.

Managing Package Distribution Wizard

This wizard allows to distribute packages of any type to all possible targets within your system, that is, you can distribute custom, MSI, RPM and snapshot packages, to either *devices* and *device groups* and to *users* and *user groups* . It is also possible to advertise packages to the targets.

The wizard can be launched from anywhere in the console via the **Wizards > Package Distribution Wizard** menu item or directly from the dashboard.

This section includes:

- Defining package for dstribution
- Defining targets for package distribution
- Scheduling the package distribution
- Creating task for package distribution

Defining package for dstribution

In the first window of the wizard you define which package to distribute and some distribution options.

1. Enter the name of the package to distribute.
   a. If you are not sure of the name of the rule, click **Find** next to the field.
      The **Select a Package** pop-up windows appears.
   b. Select the package to assign from one of the list boxes.
   c. Click **OK** to confirm the assignment and close the window.
2. Select the type of the target to which the package is to be sent to and its assignment type.
3. Via the **Options** panel you can select which of the options need to be specifically defined for the package distribution. Only the selected options will be displayed in the following windows of the wizard.
4. Click **Next** to continue.

Defining targets for package distribution

In this next window you need to define the targets of the package distribution. Depending on the target type you either add *devices* and *device groups* here or *users* / *user groups* .

1. Select **Install the package on the assigned devices** .
   The **Assign to Device** or **Select a User** pop-up menu appears.
2. Select the *devices* /*device groups* /*users* or *user groups* from one of the list boxes.
3. Depending on the object selected, the following further definitions must be executed:
   - **devices/device groups**

- if the package is of type MSI and the administrative installation option is activated in the **System Variables** the **Select Installation Type** window appears. Select the desired type with which the package is to be installed.

  > **Note:**
  >
  > Be aware that the administrative or network installation will work only with packages which were created with version 5.3.1 or later and if the respective system variable is activated.

  - **users/user groups**

- Check the **Install the selected rule as user (not as system)** box if the rule is to be executed on the device as the user and not as *LocalSystem* .

1. Click **OK** to confirm the assignment and close the window
2. Click **Next** to continue.

Scheduling the package distribution

The schedule of package distribution is defined in the **Schedule** window by selecting options to answer the questions. Depending on the answer more options might become available.

When the schedule page is first opened it displays in the top part the default schedule that is defined for execution. As you go along with your schedule specifications this line changes to show the execution schedule you define in verbal form.

1. First the assignment needs to be defined. Make the necessary selections for the following parameters:
   a. - **Assignment Date:** Define when a job or a rule is to be assigned. Possible options are.
   - - **Assign Immediately**: the assignment is carried out immediately after defining the assignment.

- **Specific Date** : the assignment of the job or rule will be carried out at a specific date and time.
- *Optional:* **Wake-up Devices** Check this box if the agent is to wake up any devices which are currently switched off, to immediately execute the assignment instead of waiting for the next startup to do so.
- *Optional:* **Run as Current User** Check this box if the distribution is to be executed and installed on the local device as the logged user and not as LocalSystem. If you are using environment variables in any of the step parameters you must check this box to make sure the variables of the local user are used and not the default values.
- *Optional:* **Advanced** Click this link if you require more assignment options.
- *Optional:* **Bypass Transfer Window** Check this box, if the distribution assignment is to be sent directly, ignoring any transfer window specifications which exist for the targets.
- *Optional:* **Upload Intermediary Status Values** Define if only the final status values, that is, *Executed* or *Failed* are to be uploaded (unchecked), or if each and every status that the operational rule execution is passing through is uploaded (checked). This option is only available if the corresponding system variable is activated.
- *Optional:* **Run while the execution fails** Defines if the operational rule/package is to be executed until its execution finally succeeds, that is, the final status *Executed* is uploaded.
- *Optional:* **Upload status after every execution** Defines that the status value is uploaded after every execution of the rule, even if it has not changed.
- *Optional:* **Assignment Activation** Defines the overall status of the software distribution rule for the respective device group. You can deactivate a group by unchecking the **Assignment Activation** box of the scheduler. By default this box is checked and the status is either *Activated* or *Paused* , if the default schedule was not selected during the assignment.
- *Optional:* **Back to Previous** Click this link to return to the main assignment options and continue with the execution schedule definition.

2. Select one of the following options for question **When do you want this rule to be run on devices?** to define when the actual distribution and package installation is to be launched:

> Depending on the choice you make in this list box, additional options become available.

- **Right now** Select this option to start the distribution immediately.
- **At Startup** Select this option if the object is to be executed every time the device is started.
- **At Session Startup** Select this option if the object is to be executed every time the agent is started

- **At Session Close** Select this option if the object is to be executed every time a session is closed.
- **Run repeatedly on a schedule** Check this option, if the execution is to be scheduled repeatedly.
- **Use Cronspec to Schedule** Select this option if the execution schedule is to be created via a cronspec.

3. *(Optional)* If you selected the **Run repeatedly on a schedule** option fill in the newly appeared boxes to create the execution schedule:
   a. Select if the schedule is to run every day, week or month.

      Be aware, that the weekly option is not available for agents of version 11.5.0 or earlier. If in your target groups there are agents of these versions, the final status is always `Sending impossible` .

      If you already used previous versions of CM , be aware that it is not possible any longer to define a schedule that executes *on the nth day of the month* .

   b. If you select the weekly schedule you also need to select on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one weekday.
   c. If you selected a monthly schedule you also need to select in which week of the month by selecting the respective number and on which days of the week the schedule is to run by clicking the respective days represented by their initials in the table that appears. You can select more than one week and one weekday.
   d. Select the **Once daily** radio button to only execute the object once per day. Then, in the list box next to it specify the time at which it is to be run.
   e. Select the **Multiple times** radio button to execute the object more than once per day. Then, in the boxes appearing below, specify the frequency and the unit for the frequency. Check the **between** box if in addition these multiple times are to occur within a specific timeframe and define the start and end time of this interval in the newly list that appears boxes.
4. *(Optional)* If you selected the **Use Cronspec to Schedule** option fill in the values that appeared for the cronspec definition:

Each set of ranges can be preceded by a % sign which will change the meaning from absolute to relative number. For instance if minutes equals 29 the timer will get fired each time the absolute time ends with a number of minutes equal to 29 (for example, 11:29) whereas %20 means every 20 minutes every hour, that is, at 13:00, 13:20, 13:40, 14:00, and so on.

- Ranges are comma-separated lists. A range is made of a number eventually followed by a '-' sign and another number
- The wildcard character asterisks (*) can be used to indicate any value.

- **Minute** Enter the minute value, it can vary from 0-59.
- **Hour** Enter the hour value, it can vary from 0-23
- **Day** Enter the day value, it can vary from 1-31.
- **Month** Enter the month value, it can vary from 1-12 (1 is January)
- **Week Day** Enter the week day value, it can vary from 0-6 (0 is Sunday).
- **Weeks of the Month** Enter the weeks of the month value, it can vary from 1-5.

5. *(Optional)* If the schedule is not to start immediately you need to select its starting moment from the **Do you want to configure a window in which this rule can run?** box.
   - **Prevent this object from running on a schedule** Select this option if you want to disable a schedule.
   - **Start the schedule immediately** Select this option if you want to start the schedule immediately.
   - **Start the schedule at next startup** Select this option if you want to activate the schedule only after the next startup of the device.
   - **Start the schedule window on** Select this option if you want to start the schedule at a specific date and time.
6. *(Optional)* If you selected the **Start the schedule window on** option you now need to select the date and time at which the schedule is to start in the boxes that appear.
7. *(Optional)* Select after how many executions the schedule is to stop. To have it run without any limits select the option **Unlimited** from the list box.
8. *(Optional)* If the execution is to stop at a specific date and time check the **End on** box and select the desired values from the list boxes next to it.
9. Click **Next** to continue if you selected to create a new task for this distribution or click **Finish** to confirm all choices and to activate the distribution.

Creating task for package distribution

This step of the wizard allows you to directly create a task for the package distribution defined via this wizard or to assign it to an existing task. This option is only available if you checked the corresponding box in the first window of the wizard.

1. Enter the required information in the available boxes.
2. Click **Finish** to confirm all choices and to activate the distribution.
   A **Confirmation** dialog box appears.

3. Check the respective box to change the focus of the console window to the respective object. Then either click **Yes**, to go to the object, otherwise click **No** to keep the focus of the console on the currently selected view. Click **Cancel** to abandon and return to the wizard.

Managing patches

The BMC Client Management - Patch Manager is mainly for the systems administrators and it provides both general user information and some in depth explanations of the internal workings of the BMC Client Management - Patch Management.

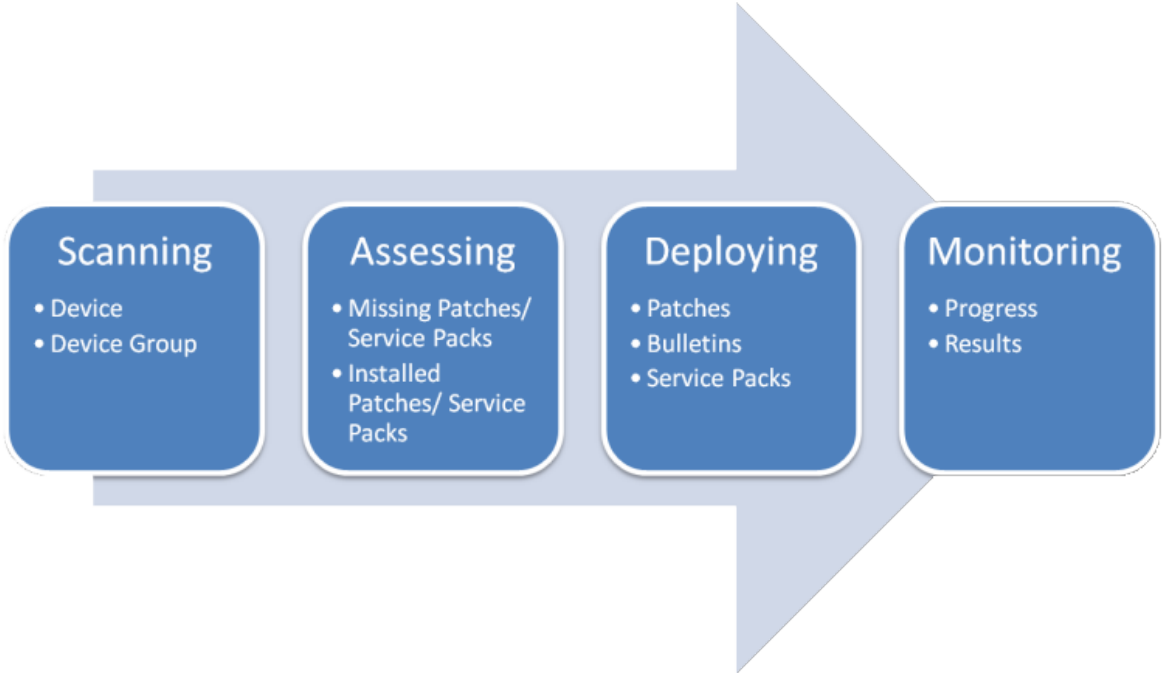
About 90% of computer attacks exploit security holes for which patches already exist. Yet many organizations find it difficult and time-consuming to keep patches current and properly installed across the company. As a result, incorrectly installed patches or patching delays can be expensive and seriously disruptive to productivity.

With BMC Client Management - Patch Management , you can easily and quickly manage, update, and download all of your patches for Microsoft operating systems, Microsoft applications, and selected third party applications, such as Firefox, installed across your network.

Related topics

- Getting started with patch management
- Prerequisites
- Patching Your First Device
- Automating Patch Management
- Regularly scanning a device group for missing patches
- Deploying a Bulletin to Affected Devices
- Scheduling Deployment
- Generating Patch Group Reports
- Automatically Downloading Patches
- Viewing the Patch Detection dashboard
- Managing patch inventory
- Working with patch groups
- Managing patch jobs
- Managing bulletins
- Managing service packs
- Managing dynamic downloader
- Locally accessing patch management
- Patch Service Pack Distribution Wizard

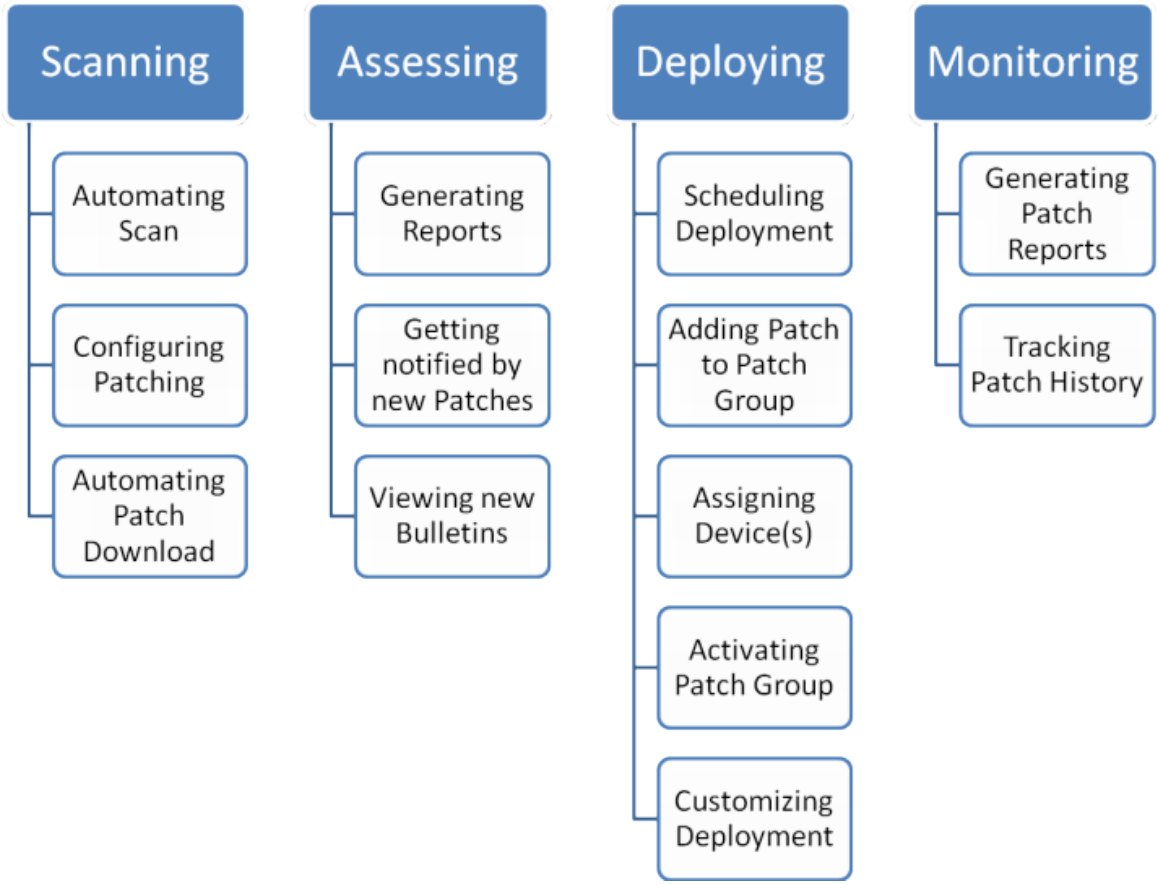
Getting started with patch management



Patch Management consists of four consecutive steps:

- **Scanning** : Selecting devices/device groups and scanning them for patches.
- **Assessing** : Assessing the results of the scan arranged in **Missing Patches/Service Packs** and **Installed Patches/Service Packs** . You can order the results, for example, by severity or product name.
- **Deploying** : Selecting patches/bulletins/service packs and deploying them to the affected devices.
- **Monitoring** : Monitoring the deployment progress and the results.

By executing these four steps your devices are protected from potential attacks. Additionally for each step you have several options to further automate and optimize your processes.



You have the following main options for improving your patching processes:

- **Automating scan** : Setting up Patch Management to automatically scan your devices for missing patches/service packs according to your schedule.
- **Scheduling deployment** : Deploying patches at times of low network load (like over night) to maintain CPU capacity during the working day.
- **Generating patch reports** : Generating reports in different formats (PDF, HTML, XML) to visualize and track patching results.
- **Automating patch download** : Automatically downloading patches based on certain criteria (severity, product name, etc.) to ensure they are immediately available for deployment.

Prerequisites

Before executing Patch Management ensure that you meet the following requirements:

- Device deploying patches (Patch Manager)
- Devices to be patched
- License

Device deploying patches (Patch Manager)

The device executing all actions of Patch Management needs to have:

- at least 2GB disk space to store patches
- one of the following operating systems:
  - Windows Server 2003 32 and 64-bit (Standard, Web, Enterprise and Small Biz editions)
  - Windows Server 2008 32 and 64-bit (Standard, Web, Enterprise and Small Biz editions)
  - Windows 2008 R2 64 bit
  - Windows XP 32 and 64-bit
  - Windows Vista 32 and 64-bit (Business, Enterprise and Ultimate editions) with SP1 or later
  - Windows 7 32 and 64 bit
  - Windows 8 32 and 64 bit
  - Windows 8.1 32 and 64 bit
  - Windows 2012 R2 64 bit

> **Note:**
>
> The patch manager cannot only have an IPv6 address.

Also, ensure that the root certificate of the device is up to date. Should this not be the case you must apply the update bulletins MSRC-001 or MSRC-002 to the Patch Manager before downloading any Knowledge Base updates.

Devices to be patched

The devices to be patched must have:

- one of the following operating systems:
  - Windows Server 2003 32 and 64-bit (Standard, Web, Enterprise and Small Biz editions)
  - Windows Server 2008 32 and 64-bit (Standard, Web, Enterprise and Small Biz editions)
  - Windows 2008 R2 64 bit
  - Windows XP 32 and 64-bit
  - Windows Vista 32 and 64-bit (Business, Enterprise and Ultimate editions) with SP1 or later
  - Windows 7 32 and 64 bit
  - Windows 8 32 and 64 bit
  - Windows 8.1 32 and 64 bit
  - Windows 2012 R2 64 bit
- MSXML 6.0 SP2 or later installed

License

Ensure that you have a valid **Patch Management** license to patch devices.

To be able to keep your Patch Knowledge Base up to date you must also have a valid **Patch Knowledge Base Update** license.

Patching Your First Device

The following topics guide you through the four steps required to patch your first device. You get to know the quickest way to ensure that your device is protected from attacks. After successfully patching your first device you have a basic idea of the general process and you can find out how to make patching even more efficient.

- Scanning a device for missing patches
- Assessing missing patches
- Applying patches
- Monitoring deployment

Scanning a device for missing patches

Before you can start deploying patches, you must find out which patches and service packs are missing on the respective devices. To do so, proceed as follows:

1. Click the **Patch Management** view in the left window pane.
   All elements of **Patch Management** are displayed.
2. Click **Patch Detection** .
3. Click the **Edit > Scan Device** menu item.
   The **Assign to Device** dialog appears.
4. Click **Scan Device**  .
5. Click **All**  in the left window bar.
   All available devices are now displayed in the right window pane.
6. Select the desired target.
7. Click **OK** .
   The window is closed and the **Scheduler** window appears.
8. Click **OK** to to confirm the default schedule and scan immediately and only once for missing patches.
   The device is scanned for missing patches and added to the **Scanned Devices** under the **Patch Detection** .
9. Click **Patch Detection > Scanned Devices** .
   In the right window pane you can follow the progress of the scan via the **Status** column.
10. Wait until the status `Scan completed` is displayed.
    The missing patch inventory is now generated.

You successfully scanned a device for missing patches. An overview of the missing patches was created and can be used to fix security problems.

Assessing missing patches

The scan of a device has determined all:

- Missing patches,
- Missing service packs,
- Installed patches and
- Installed service packs.

In this step you check the installed and missing patches to get an idea which patches you want to deploy first. To do so, proceed as follows:

1. Go to **Patch Management> Patch Detection> Scanned Devices> Your Scanned Device> Installed Patches** to check which patches already been installed.
   All installed patches for this device are listed in the right window pane. They are ordered by severity and you find further information such as name, product and language.
2. Click **Missing Patches** in the left window pane to check which patches are missing.

> Missing patches with the status `Critical` should be fixed immediately, whereas `Low` indicates the lowest severity.

You got an overview of all installed patches as well as missing patches which pose a threat to the security of the device in your network.

Applying patches

After you have scanned a device for patches and got an overview of the current situation, your next task is to fix the most urgent ones. All you have to do, is to select the patches that must be deployed and the Patch Manager will automatically download and apply the patches on the device. To do so proceed as follows:

1. Ensure that **Patch Management> Patch Detection> Scanned Devices> Your Scanned Device> Missing Patches** is selected.
2. Select the patches you want to deploy for the device.

> You can select multiple patches at the same time. BMC recommends to deploy patches with the highest severity first.

3. Click **Fix** .
   The **Patch/Service Pack Distribution Wizard** dialog appears.
4. Ensure that the **Select the type of deployment you would like to perform.** radio button is selected and click **Finish** .The wizard closes and under **Patch Management> Patch Deployment** a new patch group is listed.

You created a new patch group which immediately downloads and deploys the selected patches to the target device.

Monitoring deployment

Patch management automatically undertakes all steps from downloading, assigning to installing patches. You can monitor the deployment process in real-time to follow its progress. To do so, proceed as follows:

1. Go to **Patch Management> Patch Deployment> Your Patch Group** and select the **Patches** tab to follow the download progress.

   > Before being deployed to a device, patches must be downloaded first.

2. When all patches have the status `Available` go to **Your Patch Group> Assigned Objects> Devices** in the left window pane to follow the progress of the patch deployment.

   > In this table you can follow the actual patching progress for the device via the **Details** column. The final status is either
   > - `Reboot may be necessary` if all patches were installed but a restart of at least one device is required before proceeding,
   > - `Some patches failed` if at least one patch could not be installed on at least one device or
   > - an empty field for a successful installation.

3. Wait until the device has the status `Patch group successfully installed` , that is, that the **Details** box becomes empty.
   After the installation the device is immediately scanned for patches again and the list of **Missing Patches** and **Installed Patches** is updated.
4. To verify the successful installation go to **Missing Patches** and **Installed Patches** of **Patch Detection> Scanned Devices> Your Scanned Device** .
   Notice that the deployed patches have disappeared from the **Missing Patches** view and moved to the **Installed Patches** .

You installed patches on a particular device and thereby made the device more secure. To further improve security install other missing patches that affect your device.

Automating Patch Management

After you defined all your patching requirements and understood how the patching process works, you can set it up in such a way that it is completely automated. The following topics guide you about automating patch management:

Defining automated patch management

Patch jobs are designed to define the application of a specific type of patches for specific products and targets once and then run continuously without having to manually interfere in its operation. This means that any new patches that become available for the defined product will automatically be downloaded, assigned to the concerned devices and installed on these without you having to do anything. Patch jobs are created via the patch wizard.

1. Click the **Wizards > Patch/Service Pack Distribution** command to call the **Patch/Service Pack Distribution Wizard** .
2. Enter a name in the **Add patches to this patch job:** field.
3. Click **Next** .
4. Check the **Patch only these selected products:** radio button and select one product from the list, that is, the operating system of one of your target devices. Do not select Microsoft Office, as this product requires specific configurations which is explained in another example.
5. Click **Next** .
6. Select the **Daily** option under the **Recurr:** parameter of the **Deployment Schedule** panel.
7. Select the **Deploy anytime according to the above schedule** radio button of the **Time Period** panel.
8. Click **Next** .
9. Click **Assign Device** .
10. Select the target device from the list box, for example the device on which you are currently working.
11. Click **OK** to confirm.
12. Click **Finish** now to confirm all settings and finish this wizard.

The patch job is now defined, it will start checking for patches that are missing on the assigned devices and start downloading these.

Monitoring automated patching

As the patch job automatically executes all tasks, you only must check once in a while that everything is running smoothly.

1. Select the **Patch Management> Patch Jobs> Your Patch Job** node in the left tree hierarchy.

> The right pane shows in the upper half a recap of your patch job definitions:

- **Patch Job Filters** : the following lines display the type and severity of the patches included in the patch job.
- **Patch in the following product** : Displays the list of products for which patches are included in the job.
- **Patch Window** : Displays the schedule for the patch job.

2. You can click any of these titles to open the **Patch/Service Pack Distribution Wizard** and make modifications to these definitions.
3. Click **Finish** when you are done and all modifications will become applicable immediately and the display will be updated.
4. In the lower part the **Active Patches** tab is preselected and shows the advancement of the job execution for each patch that is part of the job.
5. Select the **Assigned Devices** tab.
6. Select a device, right-click with your mouse button and then select the **Details** option from te pop-up menu.

> The appearing window lists all patches that are currently missing on the selected device for the product, type and severity selected in the patch job and its details and the current patch application status.

Scheduling monthly patch installation

Patch Job Windows are timeframes that you define in which the patch job installs the missing patches on the target devices. You can schedule daily installation windows, weekly or monthly ones or you can switch off the schedule as we have done for our main patch job example. This option defines a window that allows the patch packages to be transferred to the target devices at any time so as to be ready when the time of the patch window arrives. This window allows the installation to start every second Saturday of the months at 1 o'clock in the morning and run its course until all missing patches are installed as no end time will be specified.

1. Select the **Patch Management> Patch Jobs> Your Patch Job** node in the left tree hierarchy.
2. In the right pane click the **Patch Window** link.
3. Select the **Monthly** option under the **Recurr:** parameter of the **Deployment Schedule** panel.
4. In the table that appears to the right-click the **2nd** cell and the last **S** which stands for Saturday.
5. Select the **Deploy only during this time** radio button of the **Time Period** panel.
6. In the now accessible list box select the option **Allow files to be downloaded to devices prior to start time** .
7. Select the *01:00 am* value for the **Start** time.
8. Click **Finish**.

Scheduling weekly patch installation

This window will define a very similar window as the option before, with the difference that the patch installation will occur on a weekly schedule and is limited from Saturday morning to Sunday night, to ensure that the installation will not interfere with the working week.

1. Select the **Patch Management > Patch Jobs > Your Patch Job** node in the left tree hierarchy.
2. In the right pane click the **Patch Window** link.
3. Select the **Weekly** option under the **Recurr:** parameter of the **Deployment Schedule** panel.
4. In the table that appears to the right-click the **M** and the last **S** which stand for *Monday* and *Saturday* , while holding the **CTRL** key.
5. Select the **Deploy only during this time** radio button of the **Time Period** panel.
6. In the now accessible list box select the option **Allow files to be downloaded to devices prior to start time** .
7. Clear the **No End Time. Run Till Completed.** box.
8. Select *01:00 am* value for the **Start:** time and *03:00 am* as the **End:** time.
9. Click **Finish**.

> Be aware, that the last started patch installation will not be interrupted when the specified end time arrives, it will finish installing.

Regularly scanning a device group for missing patches

You can also scan any number of devices simultaneously in one step. To do so, you make use of a *device group* which consists of devices according to certain criteria.

Since new patches are published frequently, you should regularly scan your devices for missing patches. You can automate scanning by defining a schedule.

In this task you learn how to scan immediately and every day at 01:00 AM for patches.

1. Go to **Patch Management > Patch Detection** and click the **Edit > Scan Device Group** menu item.
   The **Assign to Device Group** window displays.
2. Click and select the device group you want to scan for missing patches from the list.

> If you have not yet created a device group yourself, you can select the predefined device group *All Devices* which includes all devices in your network.

3. Click **OK** .
   The window is closed and the **Scheduler** window displays.
4. In the **When do you want this rule to be run on devices?** box select the **Run repeatedly on a schedule** option to define the time to scan the device group for missing patches. To scan every day at 01:00 AM, leave all values in this area as they are, only in the time box next to the **Once daily** list select **01:00** .
5. Below the **When should this schedule end?** question select the **Unlimited** option from the **End after** box.
6. Click **OK** .
   The device group is scanned for missing patches and added to **Scanned Device Groups** under **Patch Detection** .
7. Click **Patch Detection > Scanned Device Groups** .
   In the right window pane you can follow the progress of the scan via the **Status** column.
8. Wait until the status `Scan completed` is displayed.
9. Go to **Patch Management > Patch Detection > Scanned Device Groups > Your Scanned Device Group > Missing Patches** and select an element in the right window pane to check which patches are missing for the device group .

> Patches are combined in different categories, for example, affected product, language or severity. **Count** indicates the number of missing patches on all devices for the selected category.

You successfully scanned a device group and created an up-to-date patch inventory. Additionally the device group is scanned every day according to your schedule.

Deploying a Bulletin to Affected Devices

Patch Management offers two principal ways for fixing patch problems:

- View the **Patch Inventory** with **Missing Patches** and select the patches you want to deploy manually to devices
- From the **Patch Deployment** node start the **Patch/Service Pack Distribution** and select patches/bulletins you want to deploy to all affected devices

In this task, you get to know the second way: You define which bulletins must be fixed in your network and Patch Manager automatically finds all affected devices based on the results of the patch scan. Subsequently, Patch Manager downloads all relevant patches included in the bulletin and deploys them to the devices.

1. Click the **Wizards > Patch/Service Pack Distribution** menu item.
   The **Patch/Service Pack Distribution Wizard** is displayed.
2. Enter a name for the new patch group in the **Add patches to this patch group:** field.

3. From the **Deploy the patches:** drop-down list select **Using a schedule that I define** and click **Next** .
4. Select the **Bulletins Only** radio button and click **Find** .
5. Select the bulletin(s) you want to deploy from the list in the middle.

   By default all available bulletins of affected devices are listed ordered by severity.

   - To view only bulletins of a certain severity, select the respective check box in the **Severity** area and click **Find** .
   - To view only new bulletins, select the **Only new** check box and click **Find** .
6. Select the bulletins to deploy in the list that appears.
7. Click to add them to the list of bulletins to deploy at the bottom.
8. Click **Next** .
   The **Schedule** view displays.

You selected a bulletin you want to deploy to affected devices . Continue with [Scheduling Deployment|Scheduling Deployment#title_schedule_deployment] to define when the bulletin should be deployed.

Scheduling Deployment

With the default schedule, missing patches are deployed immediately. However, deploying several patches to a number of devices can be resource consuming and might decrease the efficiency of your network. In this case, BMC recommends to execute deployments when the network load is low, that is, at night, during lunch break or on the weekend. For this purpose provides a scheduler which allows you to define specific times for deployment.

In this example, you define that all patches are assigned to the devices at 1:00 AM. This means that the patches will be downloaded centrally on the Patch Manager and sent as packages to all devices . After the assignment, there should be a time of 5 hours between 1:00 AM and 6:00 AM to extract all patches from the packages on the devices . If all patches cannot be extracted until 6:00 AM, they are not installed. Instead the installation is postponed to the next night between 1:00 AM and 6:00 AM again. This procedure is repeated until all patches are extracted and ready for installation. With this schedule, you ensure that patches are only deployed at night and do not affect the regular working day.

1. In the **Assignment** tab of the **Schedule** view define when you want the bulletin(s) to be assigned to the respective devices.To assign the bulletin(s), for example, over night, select the **Deferred to** radio button and select **Tomorrow** from the first list and `01:00` from the second drop-down list.
2. Click the **Frequency** tab and define the time for the deployment of the bulletin(s).To allow deployment between 1:00 AM and 6:00 AM, select 01:00 from the **between** drop-down list and 06:00 from the **and** drop-down list in the **Frequency** group box.

3. Click **Finish** .
   The **Confirmation** dialog box appears.
4. Select the **Go to Patch Group** radio button and click **Yes** .
   The dialog closes and in the right window pane the new patch group opens.
5. You can follow progress in the following nodes:
   - To view the status of the patches of the patch group, click the **Patches** tab.
   - To view the affected devices and their patch deployment progress, go to **Assigned Objects > Devices** in the left window pane.

Generating Patch Group Reports

Once devices were scanned for patches or patches were deployed, you can generate patch reports. Patch reports offer you an overview and details of the patch situation for the respective patch group . The Console provides a number of report templates specifically for Patch Management . Additionally, you can also create your own report templates.

In this task, you learn how to generate patch reports based on existing report templates. To do so, proceed as follows:

1. Go to **Patch Management > Patch Deployment** .
2. In the left window pane, select the patch group you want to generate a report for.
3. Go to its **Report Results** subnode.
4. Click **Assign a report to the patch group** .
   The **Assign a Report** dialog displays.
5. In the right window pane, click **Patches** and select the report you want to generate.To get an overview of the patch situation, select **Patch Group Executive Summary** .
6. Click **OK**.
   The **Confirmation** dialog box appears.
7. To immediately generate the report, click **OK**.
   The **Select Generation Formats** dialog displays.
8. Select the respective check boxes for the formats you want to generate.

   > You can generate up to three different formats (XML, HTML, PDF) at the same time.

9. Click **OK**.
   The dialog closes and the reports are generated. In the right window pane the selected formats have the status `Available` .
10. To view the report, select the report and then click **View in the browser window** .
    The **Select Display Format** dialog displays.
11. From the **Available Formats** drop-down list, select the format in which you want to display the report, for example, HTML, and click **OK**.
    A new Browser window or tab opens and displays the report.

You generated a patch report in different formats based on the patches and devices of an existing patch group. With the aid of this report, you can determine which devices need patching or make the results available in your company.

Automatically Downloading Patches

Before being deployed to devices, patches must be available as packages on the **Patch Manager** . When you deploy patches automatically via the **Patch/Service Pack Distribution** two different cases can occur:

- if the selected patches were already downloaded and compiled as packages, they are immediately sent to the target devices for deployment.
- if the selected patches have not been downloaded yet, they are first downloaded by the **Patch Manager** , compiled as packages and then sent to the target devices for deployment.

Therefore, to deploy several patches which require much disk space, downloading can be time consuming and the start of the deployment is put on hold.

The Patch Manager can be configured to automatically download patches based on specific criteria. If there is for instance a new critical patch online, it is immediately downloaded. When you want to deploy it later on, the patch can be sent to all target devices right away without delay.

1. Go to **Patch Management > Patch Manager > Your Patch Manager > Dynamic Downloading** .
2. Click **Create a dynamic downloader** .
   The **Create Dynamic Downloader** dialog displays.
3. In the text box **Name** enter a name for the new dynamic downloader and click **OK** .
   The dialog closes and a new dynamic downloader is created and listed in the right window pane.
4. In the right window pane double-click **Your Dynamic Downloader**.
   The tab **Options** appears.
5. Define the criteria for the patches to be dynamically downloaded:
   a. To only download patches of a certain severity, select the respective check boxes in the **Severity** area.
   b. In the **Products** area click . In the **Add Products** dialog select your product(s) and click **OK** .
   c. In the **Languages** area click . In the **Add Languages** dialog select your language (s) and click **OK** .
6. Ensure that **Estimated Number of Patches to Download** at the top of the right window pane shows at least `1 patch` . If `0 patches` displays, repeat the last step with different criteria.
7. To activate the dynamic downloader , select **Active** from the **Enable Dynamic Downloader** drop-down list.
8. To save the settings of the dynamic downloader , click **Save** .
   A **Confirmation** dialog box appears.

9. To confirm the new settings, click **Yes**.
10. To follow the downloading progress, click the **Status** tab.
    All patches matching the defined criteria are listed and automatically downloaded.

You created, configured and activated a new . Thereby you made sure that important patches are always immediately downloaded and made available for deployment on the devices in your network.

Viewing the Patch Detection dashboard

Patch Detection is a component of Patch Management which scans your devices for patches and displays the results in different categories.

What can I do with patch detection?

With **Patch Detection** you can:

- Select a single device and scan it for patches
- Select a device group and scan all its members for patches
- Schedule scanning to scan the targets regularly at certain times
- View results in four different categories: Installed Patches, Installed Service Packs, Missing Patches and Missing Service Packs
- View a bar chart or pie chart visualizing the scan status
- Select the patches or service packs you want to deploy

Where do I find patch detection in the console?

To view **Patch Detection** go to:

Related topics

- Scanned Device Groups
- Scanned Devices
- Patch Manager

Scanned Device Groups

The following topics provide more information about nodes in Scanned Device Groups:

What can I do in this node?

In this node you can:

- Select a device group and scan all its members for patches
- Schedule scanning to scan the targets regularly at certain times
- View device groups that have already been scanned
- View a bar chart or pie chart visualizing the scan status

The Missing Patches tab of device groups

In this node you can view summaries on the following details regarding the patches that are missing on at least one device of the group, either in the form of an inventory table or in the form of a bar or pie chart:

- By **Affected Products**
- By **Bulletin Name**
- By **CVE**
- By **Installed Service Pack**
- By **Language**
- By **Patch Name**
- By **Product Family**
- By **Reason**
- By **Severity**

Missing Service Packs

In this node you can view summaries on the following details regarding the service packs that are missing on at least one device of the group, either in the form of an inventory table or in the form of a bar or pie chart:

- By **Affected Products**
- By **Installed Service Pack**
- By **Language**
- By **Product Family**
- By **Reason**
- By **Severity**

The Installed Patches tab of device groups

In this node you can view summaries on the following details regarding the patches that are installed on at least one device of the group, either in the form of an inventory table or in the form of a bar or pie chart:

- By **Affected Products**
- By **Bulletin Name**
- By **CVE**
- By **Installed Service Pack**
- By **Language**
- By **Patch Name**
- By **Product Family**
- By **Reason**
- By **Severity**

The Installed Service Packs tab of device groups

In this node you can view summaries on the following details regarding the service packs that are installed on at least one device of the group, either in the form of an inventory table or in the form of a bar or pie chart:

- By **Affected Products**
- By **Installed Service Pack**
- By **Language**
- By **Product Family**
- By **Reason**
- By **Severity**

What can I do in this node?

In this node you can:

- Select a single device and scan it for patches
- Schedule scanning to scan the targets regularly at certain times
- View devices that have already been scanned
- View a bar chart or pie chart visualizing the scan status

Patch Manager

The following topics provide more information about Patch Manager:

- What is a Patch Manager?
- What can I do with a Patch Manager?
- Can any device be a Patch Manager?
- Where do I find a Patch Manager in the console?

- The Patch Configuration node

What is a Patch Manager?

A Patch Manager is a device in your network which manages the patching system.

What can I do with a Patch Manager?

With a Patch Manager you can:

- scan devices in your network for patches
- download patches
- deploy patches on affected devices
- check for new bulletins/ patches
- assess existing bulletins

Can any device be a Patch Manager?

Any device with a supported Windows operating system can be defined as Patch Manager . To be able to deploy patches efficiently across your network, the Patch Manager should have a strong configuration and at least 2GB disk space to store patches. For detailed information regarding the required operating systems refer to the Prerequisites topic.

Where do I find a Patch Manager in the console?

To view the currently device defined as Patch Manager go to:

The Patch Configuration node

What can I do in this node?

In this node you can:

- update the Patch Knowledge Base
- inform yourself about the status of the Patch Knowledge Base
- configure proxy
- configure **Patch Manager** advanced downloading and updating

Managing patch inventory

The following topics are provided:

- What is a Patch Inventory?
- What can I do with a Patch Inventory?
- How can I create a Patch Inventory?

What is a Patch Inventory?

The **Patch Inventory** provides an overview of **Missing Patches** , **Missing Service Packs** , **Installed Patches** and **Installed Service Packs** of a device or device group.

What can I do with a Patch Inventory?

With a **Patch Inventory** you can:

- Assess patches and service packs that are already installed or are missing
- Select the patches or service packs you want to deploy
- Sort patches or service packs by different criteria like severity, product name or product family
- Create reports to visualize the patching situation of your network

How can I create a Patch Inventory?

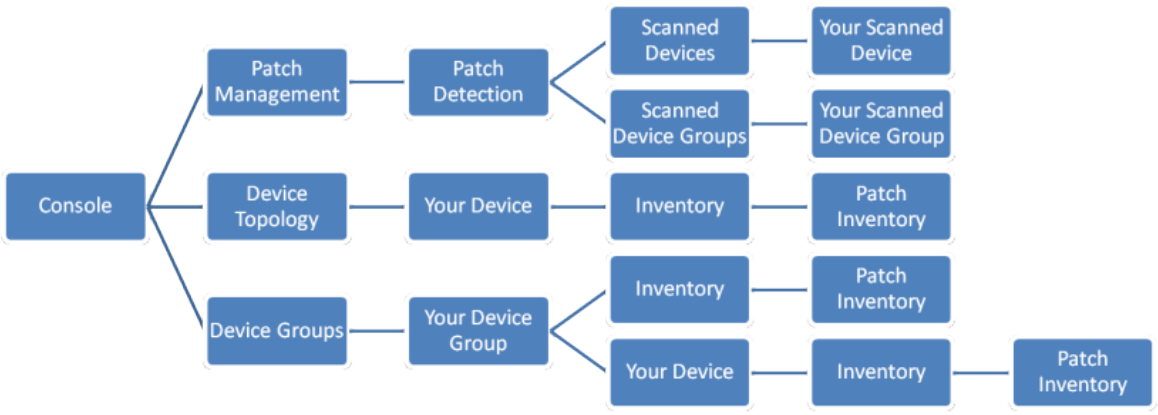
Before you can view the **Patch Inventory** of a device you must scan it for patches. After scanning with **Patch Detection** the **Patch Inventory** is automatically uploaded and available.

Is a Patch Inventory always up-to-date?

A **Patch Inventory** displays the results from the last scan. To ensure that a **Patch Inventory** is up-to-date, configure **Patch Detection** to regularly scan for patches.

Where do I find a Patch Inventory in the console?

To view the **Patch Inventory** of a device or device group go to:



Related topics

- Patch Inventory Nodes

Patch Inventory Nodes

The following paragraphs provide more information about patch inventory nodes:

- Missing Patches and Service Packs
- The Installed Patches tab of devices
- The Installed Service Packs tab of devices

Missing Patches and Service Packs

In the respective tabs, you can view the following information about missing patches and service packs:

- View and order all missing patches and service packs of the selected device
- hide bulletins
- select patches/service packs and deploy them to the devices
- add patches and service packs to a patch group
- see the time of the last scan and Patch Knowledge Base update
- scan the device for patches

The Installed Patches tab of devices

In this node you can:

- view and order all patches installed on the selected device
- see the time of the last scan and Patch Knowledge Base update
- scan the device for patches

The Installed Service Packs tab of devices

In this node you can:

- view and order all service packs installed on the selected device
- see the time of the last scan and Patch Knowledge Base update
- scan the device for patches

Working with patch groups

A **Patch Group** is a container with all necessary information to deploy one or several patches to one or more target devices/device groups.

The following topics are provided:

- What can I do with a Patch Group?
- Should I create one Patch Group with all patches or split patches into different Patch Groups?
- Where do I find a Patch Group in the console?
- Related topics

What can I do with a Patch Group?

With a **Patch Group** you can:

- deploy patches to devices and device groups
- assign devices and device groups on which you want to deploy patches
- define actions to be executed before and after deployment (for example, displaying a dialog, rebooting after installation)
- define a schedule for patch deployment
- generate and view reports on the **Patch Group**

Should I create one Patch Group with all patches or split patches into different Patch Groups?

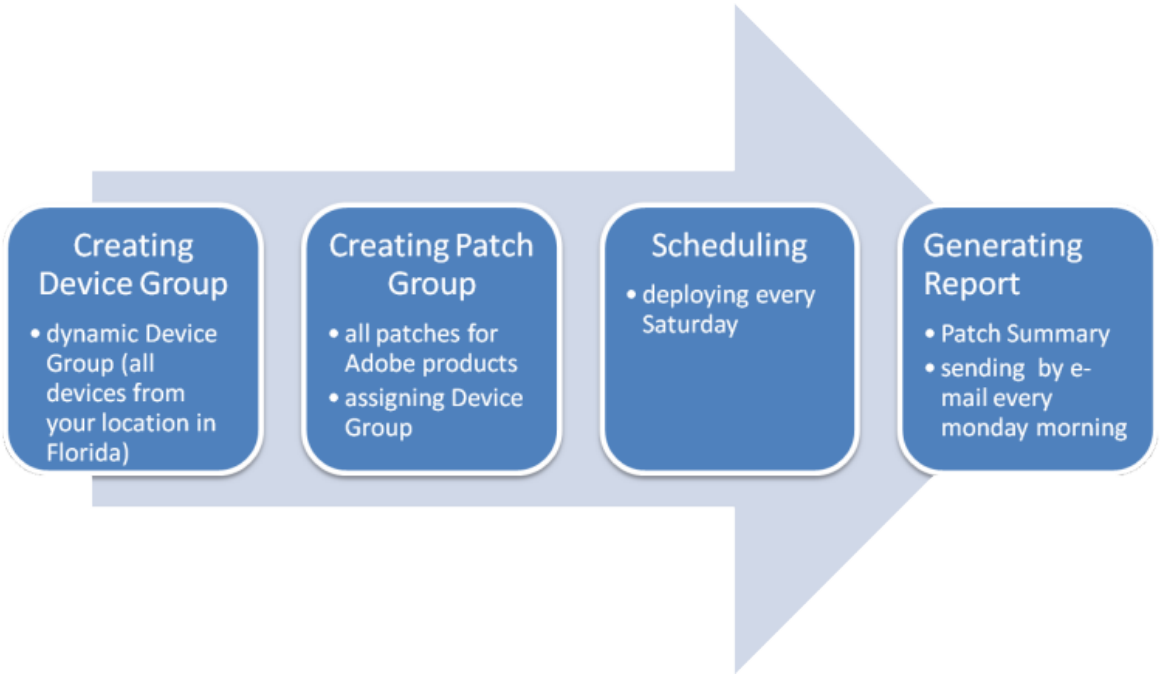
If you have a limited number of patches that must be deployed to all devices in your network, it might be most efficient creating one patch group, add all your patches to the group and assign the predefined device group *All Devices* .

Thus you ensure that all devices in your network have the included patches installed.

If you have many patches from different vendors and BCM agents in different geographical locations, it might be most efficient to split patches into different groups.

Following you can see a fictitious example of a global company which has a location in Florida and wants to ensure that all Adobe products at that location are up to date. This example demonstrates a possible way of using patch groups effectively.

The process could be as following:



- **Creating Device Group** : dynamic device group including all devices from your location in Florida.
- **Creating Patch Group** : includes all patches for Adobe products and is therefore called ***Adobe Patches*** . Assign the dynamic device group with devices from Florida.
- **Scheduling** : Define a schedule to deploy the patches of the patch group every Saturday when the network load is low. All patches are deployed to the devices next Saturday. Due to this schedule the Patch Manager checks the devices from Florida every Saturday: if a device has the patches already installed, no patches are deployed and the Patch Manager continues checking. If there is a new device detected which is missing the patches, the respective patches are immediately deployed.
- **Generating Report** : generate the predefined report **Patch Group Executive Summary** every Monday morning and have it sent it by email to your account and other employees in your company who require a report.

All your Adobe products that are installed on the devices in Florida are automatically patched and a report is generated and distributed providing an overview of the current patching situation.

Where do I find a Patch Group in the console?

To view all your existing patch groups go to:

To define **Global Settings** for patch groups go to:

To view predefined reports assigned to patch groups go to:

Related topics

- Managing preinstallation parameters
- Managing installation parameters
- Managing reboot options
- Managing patches of a patch group

Managing preinstallation parameters

This tab defines the behavior of the patching system prior to the actual patch installation on the target device. The default values for these parameters can be defined per user in the respective tab of the **Patch Deployment** section of the **Preferences** window.

The following topics provide more information about preinstallation parameters:

Available parameters

Parameter	Description
Information Window	This option defines if a pop-up menu appears, of the target device, informing the remote user that patches will now be installed and applied on his computer.
Message to Display	This is a free text box in which you can enter the message to be displayed on the screen of the target device. If no text is entered here a default message (The system is about to apply the security update.) will be displayed. This message is localized in all console languages. If you enter your own text here it will not be localized and will appear as entered on all operating system languages.
Allow User to Extend Countdown Timer	Check this box if the user can extend the countdown timer before the patch installation will automatically start.
Initial Countdown (sec)	This text box defines in seconds the time before the information window that displays is auto-validated to allow the patch installation to proceed. To deactivate the option 0 must be set.
Timer Incrementation Value (min)	This value in minutes defines the interval by which the countdown timer is incremented each time the user decides to extend it, if he was allowed to do so by the preceding option.
Timer Maximum Extension Value (min)	This value defines the maximum interval the countdown timer can be extended. If for example the initial value is 2 minutes, the user can each time extend it by 2 minutes as well, and this value is set to 5 minutes, the user can extend the countdown once, 2 min initial 2*2 min extension makes 6 minutes which is higher than the defined 5 minutes.

Modifying the preinstallation parameters

To modify the values of the preinstallation parameters proceed as follows:

1. Double-click any line of the table in the right window frame.
   The **Properties** window appears.
2. Make the required modifications in the available parameters.
3. Click **OK** to confirm the modifications and to close the window.

You modified the parameters that define the behavior of the patching system before the actual patch installation.

Managing installation parameters

The **Installation** tab allows you to configure the parameters for the patch installation procedure of the patch group. The following topics provide more information about installation parameters:

- Available parameters for patch installation

- Modifying the installation parameters

Available parameters for patch installation

Field	Description
Quiet Mode	This option displays if the installation of the patch group's patches is to be executed without the remote user being aware of it. Otherwise the default dialog boxes concerned with patch installation appears. By default this value is set to *Yes* .
Stop On Error	With this option you can define if the installation of patches is to continue even if one of the patches of the group has failed to install. By default this option is set to `true` , continue the installation.
Lock mouse and keyboard on client device	Defines if the mouse and keyboard on the target device are blocked during the patch installation, that is, the user logged on to the local device may not execute any other operations during the installation.
Locking Message	Enter into this box the message to be displayed on the screen of the target device to inform the user what is happening on his device. If no text is entered here a default message appears.
Force Installation	This option allows you to force the installation of a patch group again even if it was already installed. This can be useful, if for example a problem occurred in the network or a device crashed during the installation.
Patch Group Options	In this section you need to define the type of installation for the patch. If the patch to install is not applicable to any of the Microsoft Office products select **No Specific Office Install Options** from the drop-down list. Otherwise, you have the following options for Microsoft Office patches:
Administrative Installation	This option should be used if Microsoft Office was installed via an administrative installation. For this option to work the path to the location of the Microsoft Office DVD or share must be entered into the following text box together with a valid user name and password.
Full File Installation	This installation option is for a complete install for Microsoft Office without any DVD being required.
Mixed Installation	For the mixed installation the path to the location of the Microsoft Office DVD or share might be necessary. Enter it into the following text box together with a valid user name and password.
Path	Enter into this box the location of the Microsoft Office Installation source. This can be a local path, for example, `C:/patchex/MS/office/office2010` or it can be a network share, in the form of *[IpAddress]**[SHARE]**MSOFFICE2010* , for example, *FD43-0-0-0-8C84-4BAD-D413-DD68.ipv6-literal.net**CDSERVER**MSOFFICE2010* . You can also enter the path in the following format: *[IpAddress]**[SHARE]**MSOFFICE2010* , for example, *192.155.1.24**CDSERVER**MSOFFICE2010* .
User	If the source location is on a device/share that requires identification you must enter here a user name with which it can be accessed. Otherwise you can leave the text box empty.
Password	If identification is required enter here the password for the specified login.
Confirm Password	Re-enter the password for confirmation.
Patch Job Options	In this section you can define additional options specific to patch jobs.
Retry Attempts	The number of installation retries before the patch is shown as failed in the Console. Updating the ConfigFiles reinitializes this parameter to 0 and the installation process starts again.

Modifying the installation parameters

To modify the values of the installation parameters, proceed as follows:

1. Double-click any line of the table in the right window frame.
   The **Properties** window appears.
2. Make the required modifications in the available parameters.
3. Click **OK** to confirm the modifications and to close the window.

You modified the parameters that define the actual installation procedure of the patch group.

Managing reboot options

In the **Reboot** tab, you can define the parameter settings for a safe restart of the target devices after the patch group installation. This tab is only of interest if in the preceding tab **Installation** the option **Reboot after deployment** was chosen for the **Reboot Type** . If the option **No reboot** was selected, this table will be empty. When safe restart is selected, a pop-up window appears on the target screen, informing the user of the impending restart and providing him with the restart options defined in this tab.

The default values for these parameters can be defined per user in the respective tab of the **Patch Deployment** section of the **Preferences** window.

The following topics provide more information about reboot options:

- Available parameters for patch reboot
- Modifying the reboot parameters
- Modifying the pop-up window logos

Available parameters for patch reboot

Field	Description	
Reboot Type	This field displays if a reboot is previewed after the installation of the last patch package of the patch group. Possible values are `No reboot` and `Reboot after deployment` . Be aware that if you do not reboot after installation when a reboot is expected by one of the patches installed, this patch will still be seen as missing even if you force a scan after install by the following option. If no user is logged on to the target device the reboot will be automatically launched. If there is an open session that is locked the reboot mechanism will wait until the session is unlocked before displaying the respective window and launching the reboot.	
Shutdown After Reboot	Check this box, if the device is to be shut down after the required reboot after the patch installation is completed.	
Display Reboot Dialog	Check this box if a pop-up window is to be displayed on the target screen informing the local user of the imminent reboot of his device.	
	Customize Reboot Message	This field contains the title of the window which will be displayed on the screen of the remote device before the device is shut down,

Field	Description	
		for example, *Maintenance Shutdown* .
Shutdown Initiated by User	Here the user can be specified that initiated the reboot of the device, such as for example *Admin* or *Patch Administrator* , and so on. This information will be displayed in the reboot pop-up menu previously defined.	
Enable End-User Interaction	The following fields are only applicable for this option:	
	Allow User to Cancel Reboot	Specifies if the user can definitely cancel the reboot of the concerned device.
Reboot Directly after Disconnecting	This option defines if the user can decide to immediately reboot the device, without awaiting the end of the specified countdown.	
Force reboot if Session is Locked	This option defines if the reboot is to be executed even if the session is locked. By default this option is deactivated, that is, the reboot will wait until the session becomes unlocked.	
Allow User to Extend Countdown Timer	This option defines if the user can extend the time before the device is rebooted.	
Initial Countdown Timer (min)	The value in this field indicates the waiting time in minutes between the pop-up menu first displays and the actual initialization of the reboot of the device. The default value is *2* minutes.	
Countdown Timer Increment (min)	This value in minutes defines the interval by which the countdown timer is incremented each time the user decides to extend it, if he was allowed to do so by the preceding option. The default increment time is *2* minutes.	
Countdown Timer Maximum (min)	This value defines the maximum interval the countdown timer can be extended. If for example the initial value is 2 minutes, the user can each time extend it by *2* minutes as well, and this value is set to *5* minutes, the user can extend the countdown once, *2* min initial *2*2* min extension makes *6* minutes which is higher than the defined 5 minutes. The default value of this option is *5* minutes.	
Only Reboot if Requested by Patch	This option defines if the device is always rebooted after a patch installation or only if a patch specifically requests it. By default this option is activated. If this option is deactivated a reboot occurs if at least one patch successfully installed, independent if it requires a reboot. If this parameter is activated a reboot occurs only if at least one patch of a patch group or a patch job installed successfully and at least one of the successfully installed patches requires a reboot. If none of them do so, the device is not rebooted. No reboot occurs in either case if all patch installations of the group or job fail.	
Reboot after Logoff	This option defines that the reboot of the device is effected only once the user has logged off the device.	

Modifying the reboot parameters

To modify the values of the restart parameters, proceed as follows:

1. Double-click any line of the table in the right window frame.
   The **Properties** window appears.
2. Make the required modifications in the available parameters.
3. Click **OK** to confirm the modifications and to close the window.

You modified the parameters that define the restart of the remote device after a patch installation.

Modifying the pop-up window logos

If thus configured, a pop-up window appears on the remote device after the patch installation has finished and before the restart is launched, providing a number of options as defined in the restart parameters. You can also modify the logos of this window to those used by your organization, or any others. To do so, proceed as follows:

1. Prepare the following images, and ensure they are all there, all five of them are needed. The images must be in `.bmp` format.
   - TinySized.bmp - 574 x 379 pixel
   - SmallSized.bmp - 574 x 455 pixel
   - MediumSized.bmp - 574 x 509 pixel
   - FullSized.bmp - 574 x 572 pixel
   - RebootAfterLogOut.bmp - 574 x 274 pixel
2. Copy the images to the following directory: `<InstallDir>/master/data/core/res` .
3. Then you need to also copy the images to directory `<InstallDir>/client/data/core/res` on all client devices.
   Once these images are saved to this location, they will be used in the safe restart pop-up windows when they are displayed on the target screens.

You have successfully modified the logos of the pop-up window that displays on the remote device after a patch installation to inform the user of the required restart.

Managing patches of a patch group

The **Patches** tab provides the list of all patch packages which are included in the patch group, those currently being downloaded and those that are already available. In the line above the table, you can follow the progress of the currently effected downloads, the value in parenthesis indicates the amount remaining to be downloaded.

> **Note:**
>
> This tab is only displayed if you have a valid Software Distribution license.

The following topics provide more information about managing patches of a patch group:

- Adding patches

Adding patches

You can add other patch packages to the patch group. When you add one or more packages, the operational rule about the installation of the patch packages will automatically be created under a specific *Premium Patches* folder under the main **Operational Rules** , which will include all the necessary steps to install the added packages. Also the installation schedule (immediate installation once only) will be directly created for the added patch package bypassing the default schedule defined in the user preferences. If currently no devices are affected by this patch package, the operational rule will not be created. This will only happen once a device becomes affected by the patch package. To add a patch package to a patch group, proceed as follows:

1. Select the **Patches** tab of the patch group to which you want to add a new patch package.
2. Click **Edit > Add Patch** .
   The **Patch Selection** dialog box opens on the screen. It displays the list of available patch packages sorted by bulletins and service packs in its display window.
3. Select the desired package and click **OK** to add it to the patch group and close the window.
   If one or more of the selected patches were replaced by newer versions, a **Superseded Patches** window appears, for each superseded patch.
4. In this window you can define if only individual patches are to be replaced by their newer version, by clicking **Yes** / **No** in each appearing window, or you can define once for all patches to be superseded by clicking **Yes to all** / **No to all** .

You have now added a further patch package that will be installed on the target devices once the patch group is executed.

Downloading selected patches

If a patch download has failed for a patch group, the download can be retried by proceeding as follows:

1. Select the failed download in the table, which is to be retried.
2. Click **Edit > Download Selected Patch(es)** or .
3. The patch download will be started directly.

You have now manually downloaded a patch package of which the automatic download failed.

Changing the patch manager

It is possible to change the patch manager for a failed patch download or a download still being executed. To do so, proceed as follows:

1. Select the failed download in the table, for which the patch manager is to be changed.

2. Click **Edit > Change Patch Manager** .
   The **Change Patch Manager** window displays on the screen, providing the list of all available patch managers.
3. Select the patch manager to use from now on for this patch from the list and then click **OK** to confirm.
4. The patch manager will immediately be changed and the patch to be download will be reinitialised directly.

You defined another device as the patch manager to download a specific patch.

Displaying affected products

To display the products which are affected by the patch added to the patch group, proceed as follows:

1. Select the package, for which the list of devices are to be displayed, in the table of the **Patches** tab.
2. Click **Edit > Display Product List** .
   The **Product List** window will appear on the screen displaying the names of all products impacted by this patch.
3. Click **Close** to close the window.

You displayed the list of all products that are affected by a patch that is part of the patch group.

Managing patch jobs

A **Patch Job** is a container with all necessary information to deploy one or several patches to one or more target devices/device groups in a completely automatic way.

- What can I do with a Patch Job?
- Why select a Patch Job instead of a Patch Group?
- Should I create one Patch Job with all patches or split patches into different Patch Jobs?
- Where do I find a Patch Job in the console?
- Related topics

What can I do with a Patch Job?

With a **Patch Job** you can:

- Deploy patches to devices and device groups
- Assign devices and device groups on which you want to deploy patches
- Define actions to be executed before and after deployment (for example, displaying a dialog, rebooting after installation)
- Define a schedule for patch deployment
- Generate and view reports on the **Patch Job**

Why select a Patch Job instead of a Patch Group?

A **Patch Job** allows you to define you patching process in such a way that you only must monitor the results but never must manually interfere in its execution. When defining the **Patch Job** , you specify all required elements such as the severity of the patches to apply, which types of patches to apply, that is, only security patches or all of them, and the product for which these patches are to be applied, for example, for the operating system, one or several Microsoft Office products, or a single specific application. Then you define the device population on which these patches are to be applied and the execution schedule for these. Now, whenever a new patch becomes available that fits all the defined requirements, it will automatically be downloaded, added to the **Patch Job** , transferred to the target devices according to the defined schedule and installed - without any manual interference.

Should I create one Patch Job with all patches or split patches into different Patch Jobs?

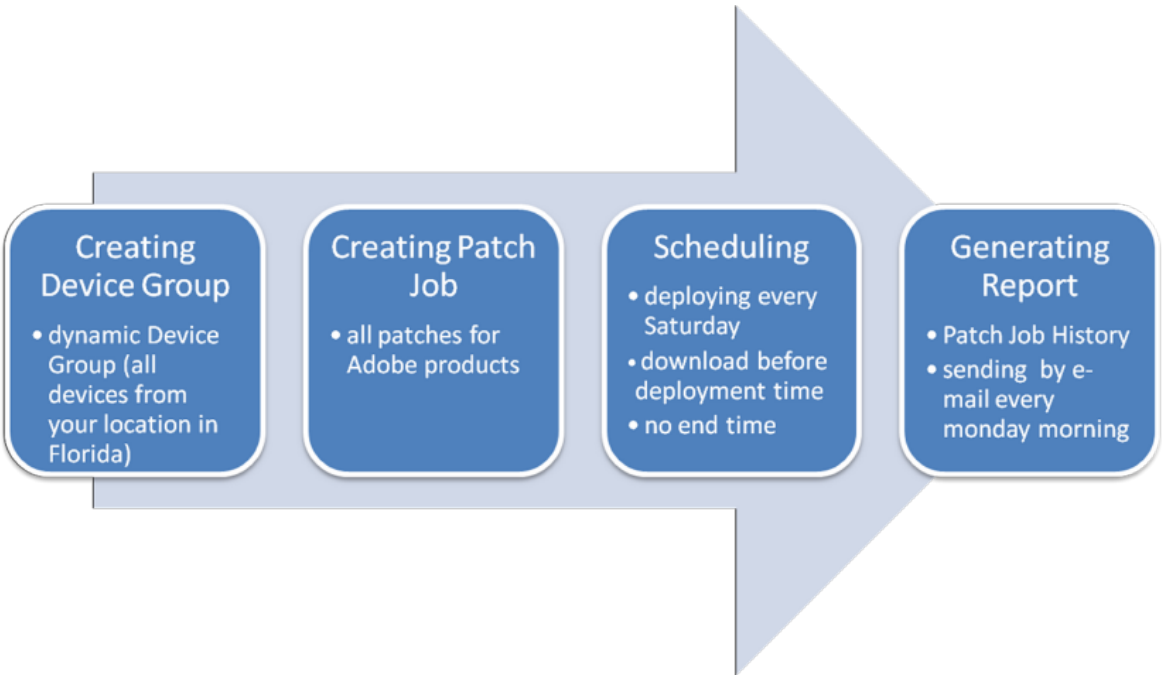
If you have a limited number of patches that must be deployed to all devices in your network, it might be most efficient creating one patch group, add all your patches to the group and assign the predefined device group *All Devices* .

Thus you ensure that all devices in your network have the included patches installed.

If you have many patches from different vendors and BCM agents in different geographical locations, it might be most efficient to split patches into different jobs.

Following you can see a fictitious example of a global company, which has a location in Florida and wants to ensure that all Adobe products at that location are up to date. This example demonstrates a possible way of using patch jobs effectively.

The process could be as following:



- **Creating Device Group** : dynamic device group including all devices from your location in Florida.
- **Creating Patch Job** : includes all patches for Adobe products and is therefore called ***Adobe Patches*** . Assign the dynamic device group with devices from Florida.
- **Scheduling** : Define a schedule to deploy the patches of the patch group every Saturday, when the network load is low. All patches are deployed to the devices next Saturday. Due to this schedule, the Patch Manager checks the devices from Florida every Saturday: if a device has the patches already installed, no patches are deployed and the Patch Manager continues checking. If there is a new device detected which is missing the patches, the respective patches are immediately downloaded and deployed.
- **Generating Report** : Generate the predefined report *Patch Job History* every Monday morning and have it sent it by email to your account and other employees in your company who require a report.

All your Adobe products that are installed on the devices in Florida are automatically patched and a report is generated and distributed providing an overview of the current patching situation.

Where do I find a Patch Job in the console?

To view all your existing patch jobs go to:

To define **Global Settings** for patch jobs go to:

To view predefined reports assigned to patch jobs go to:

Related topics

- The Patch Job node
- Evaluating a patch job
- The Active Patches tab of a patch job
- The Assigned Devices tab of a patch job
- The Assigned Device Groups tab of a patch job
- The Options tab of a patch job
- The History tab of a patch job

The Patch Job node

The view of a patch job provides some general information about the selected job and information about the job's progress.

Parameter	Description
Patch Job Filters	The total size of the patch package.
Patch in the following product	This section lists all products which is patched by the job.
Patch Window	This section displays the schedule conditions for the patch application, such as start end end date and the allowed transfer time to the targets.
Pie Chart	The pie chart shows a graphical representation of the current status of the patch job execution. For more details see The Active Patches tab of a patch job .
Filter on the last (days):	Via this dropdown list you can limit the displayed data to a more recent timeframe by selecting the corresponding option.
Last Deployment:	The date and time at which the patch job tried to install or successfully installed a patch on a device.
Last Evaluation	Displays the date and time at which the patch job was last evaluated.

Note:

> The section titles shown in blue are also links that provide you the possibility to open the **Patch/Service Pack Distribution Wizard** on the respective window to modify the selections.

Further information about this patch job displays via its following tabs:

- The Active Patches tab of a patch job
- The Assigned Devices tab of a patch job
- The Assigned Device Groups tab of a patch job
- The Deployment Options tab of a patch job
- The Office Installation tab of a patch job
- The History tab of a patch job

Evaluating a patch job

At any moment and from any location under a patch job you can evaluate its progress:

1. Select the device in the table.
2. Click **Evaluate Now** .

The progress of the patch job is immediately be evaluated, the status is updated on the screen and the **Last Evaluation:** box is updated with the respective date and time.

The Active Patches tab of a patch job

This tab shows the progress of the patching process that is executed by the selected patch job. It provides the following information.

Parameter	Description
Patch Name	The name of the executable file contained in the security patch.
Bulletin	The name of the bulletin if one exists for this patch.
Status	The overall installation status of the patch executive file, that is, the least favorable status of all devices is displayed. This means that if even on only one of all the assigned devices the installation failed, the overall status is displayed as failed. The possible values are: • **Patch inventory not yet uploaded** : The agent is waiting to establish the patch inventory of the device that is required to determine which patches are missing and must be installed. • **Execution Pending** : The patch job is installing the patch on all devices on which it is missing. • **Installed** : The patch file was successfully installed on all devices. • **Installation failed** : The patch could not be installed on at least one of the devices.
Installed Devices	This column shows the relation between the number of devices that have already successfully installed the patch versus the total number of devices on which the patch is missing.

Parameter	Description
Failed	The number of patches that failed to install.
Severity	The importance of the patch. This is not necessarily the same severity as that of the individual bulletins contained in the patch. If a bulletin is classified as *Unrated* , it is often due to the fact that it contains several executable files with different severity ratings.
CVE ID	The CVE identification of the patch if it has one.
Size	The total size of the patch package.
Product Family	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.

Viewing the devices assigned to a specific patch

To view all devices on which a specific patch is missing and scheduled or already installed, proceed as follows:

1. Select the patch executable in the table in the right window pane.
2. Click **Properties** .
   The **Devices assigned to <patch name>** appears.

Parameter	Description
Device Name	This column lists all devices that are assigned to this patch job.
Status	The patch installation status of the device. Possible values are: • **Patch inventory not yet uploaded** : The agent is waiting to establish the patch inventory of the device that is required to determine which patches are missing and must be installed. • **Executing** : The patch job is executing and installing the required patches one after the other. • **Installed** : All missing patches were successfully installed. • **Installation failed** : At least one of the required patches could not be installed on the device. • **Not applicable** : The patches of this patch job are not applicable to the device, that is, they are not missing on the device.
Assignment	This column lists all devices that are assigned to this patch job.
Last Attempt	The date and time at which the patch job last tried to install the patch.
# of Attempts	The number of attempts that were required to install the patch or that were made before the installation was finally abandoned.
Error	The error message connected to the reason why the patch installation failed.

3. Click **Close** to close the window.

The Assigned Devices tab of a patch job

This tab lists all devices that are assigned to the patch job together with the following information.

Note:

Be aware, that this table columns represent the global evaluation of the patch job, however, if you do not have read access on all devices assigned to this job, the number of devices shown in the detailed views can differ from the information shown here.

You can filter the table according to the following criteria:

- **Filter by Patch Status** : To limit the displayed list to the devices of a certain patch installation status, select the desired value from this list.
- **Filter by Device Group** : To limit the list of devices to the members of a specific group or display only those devices that are no member of any group, select the desired value from this list.

Parameter	Description
Device Name	This column lists all devices that are assigned to this patch job.
IP Address	The IP address of the device.
Status	The patch installation status of the device. Possible values are: • **Patch inventory not yet uploaded** : The agent is waiting to establish the patch inventory of the device that is required to determine which patches are missing and must be installed. • **Executing** : The patch job is executing and installing the required patches one after the other. • **Installed** : All missing patches were successfully installed. • **Installation failed** : At least one of the required patches could not be installed on the device. • **Not applicable** : The patches of this patch job are not applicable to the device, that is, they are not missing on the device.
Inherited from Group	This column shows if the assignment was made directly or via a group, in which case the name of the device group is displayed in the field.
Installed Devices	This column shows the relation between the number of devices that have already successfully installed the patch versus the total number of devices on which the patch is missing.
Failed	The number of patches that failed to install.
Patch Knowledge Base Version	The version number of the patch knowledge base that was used for the patch process of the respective device.
Last Update	The date and time at which the patch inventory was last updated on the device to check if all its patches are up to date.

Related topics

- Displaying the patch job log file
- Viewing patch job details

Displaying the patch job log file

For more detailed information about the patch job executed on a specific device, you can display the device's patch job log file.

1. Click **View Log File** .
   The **Patch Job Log File** window displays on the screen, displaying the complete log file.
2. To view specific parts of the log file you can use the filter options on top of the window to reduce the amount of information shown.
3. Click **Close** to close the window again.

Viewing patch job details

1. Select the device in the table.
2. Click **Details** .

The **Patch Details for the Device** window appears and displays the list of all patches that are required by the device and which are dealt with by the currently selected patch job. It provides the following information about these patches:

Parameter	Description
Patch Name	The name of the executable file contained in the security patch.
Bulletin Name	The name of the bulletin if one exists for this patch.
Language	The language in which the patch is installed.
Status	The current status of the patch installation. If the installation failed an error message is displayed as to the reason of the failure.
Size	The total size of the patch package.
Assignment	The date and time of the assignment between the patch package and the device, that is, when the patch job is evaluated or when a device uploaded a new patch inventory.
Last Attempt	The date and time at which the patch job last tried to install the patch.
• 1. of Attempts*	The number of attempts that were required to install the patch or that were made before the installation was finally abandoned.

The Assigned Device Groups tab of a patch job

This view displays the list of all device groups that are assigned to the patch job.

Double-clicking an entry opens the **Assigned Devices** tab filtered down to the members of the respective group.

The Options tab of a patch job

This tab displays a recap of the options defined for this patch job:

Parameter	Description
Display an information window prior to installation	Defines if a pop-up window appears on the screen of the target device, informing the remote user that patches are now installed and applied on his computer.
Install using Quiet mode	Defines that the patch installation is to be executed without the remote user's being aware of it. If you uncheck this box the default dialog boxes concerned with patch installation appears on the screen. Be aware, however, that not all patches necessarily interact with the user.
Stop On Error	Defines that the patch installation is to continue even if one of the patches of the group has failed to install.
Lock mouse and keyboard on client device	Defines if the mouse and keyboard on the target device are blocked during the patch installation, that is, the user logged on to the local device may not execute any other operations during the installation.
Reboot after installation	Defines if a reboot is previewed after the installation of the last patch package of the patch job. Be aware that if you do not reboot after installation when a reboot is expected by one of the patches installed, this patch is still seen as missing even if you force a scan after install by the option below. If no user is logged on to the target device the reboot is automatically launched. If there is an open session that is locked the reboot mechanism waits until the session is unlocked before displaying the respective window and launching the reboot.

Note:

Clicking the blue link above the parameter list will open the patch wizard on the corresponding page to edit these options.

This section includes:

Editing patch jobs

It is possible to edit the patch job definitions on the tabs of a patch job.

1. Select a line in the right window pane.
2. Click **Edit Patch Job** .
   The **Patch/Service Pack Distribution Wizard** displays on the screen displaying the wizard page corresponding to the tab on which it was called.
3. Make the required modifications in the page(s).
4. Click **Finish** to confirm and apply the modifications.

The modifications will be taken into account immediately and applied to all future patch and service pack installations.

The History tab of a patch job

The **History** tab provides the same information aboutce in tabular and once in graphical format: It shows the installation progress of the patches to be installed and the final installation result for a customizable number of days past.

To modify the number of days for which the information and graphics are shown, select the desired number from the **Show past (days):** drop-down list.

The table displays the following detailed information:

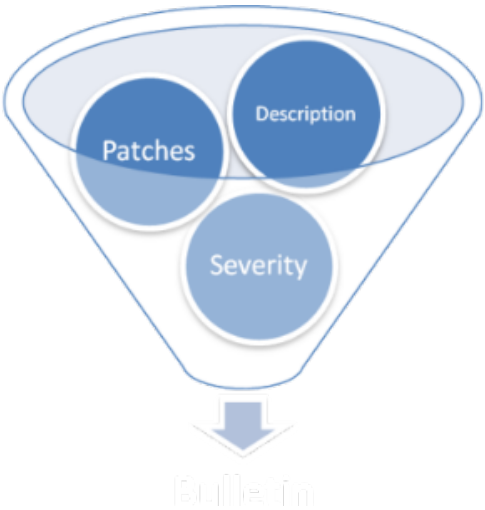
Parameter	Description
Evaluation Time	The date and time at which the patch job progress was evaluated.
Installed	The number of patches that were installed. Be aware that his number may be higher than the number of missing patches. This is due to the fact that if an application is missing several patches only the latest patch is actually installed and applied, as they normally contain all previous patches as well. However, the count in this case considers that not only this latest patch was installed but all the missing ones before as well.
Pending	The number of patches waiting to be installed.
Critical Pending	The number of critical patches waiting to be installed.
Failed	The number of patches that failed to install.
Number of devices	The number of devices on which the patches were installed. Once all patches are installed the last number should be the same as the number of the assigned devices.

Managing bulletins

A bulletin is a file published by a software manufacturer about a security issue or vulnerability in one of its products.

A bulletin contains:

- a description of the problem with origin, severity and possible solutions
- links for patches



What can I do with a Bulletin?

After getting an idea of the objective of the bulletin in the description, you can deploy it on devices in your network which are affected by it. All patches from the bulletin are downloaded and installed on the respective devices.

Are some Bulletins more important than others?

Each bulletin has a certain severity indicating the urgency of the contained patches. Severity is represented by a coloured flag:

- Critical
- Important
- Moderate
- Low
- Unrated

If a bulletin is classified as `Unrated` , it is due to the fact that it contains several patches with different severity ratings.

Missing patches with the status `Critical` should be fixed immediately, whereas `Low` indicates the lowest severity.

What does the icon next to a Bulletin stand for?

Each bulletin has an icon next to it to indicate its current status:

- green: All patches of the bulletin were downloaded successfully.
- yellow: At least one patch of the bulletin was downloaded successfully, but there are still patches that have not been downloaded yet.
- red: The download of the patches failed.
- gray: No patch of the bulletin was downloaded yet.

How can I ensure that I always have the latest Bulletins?

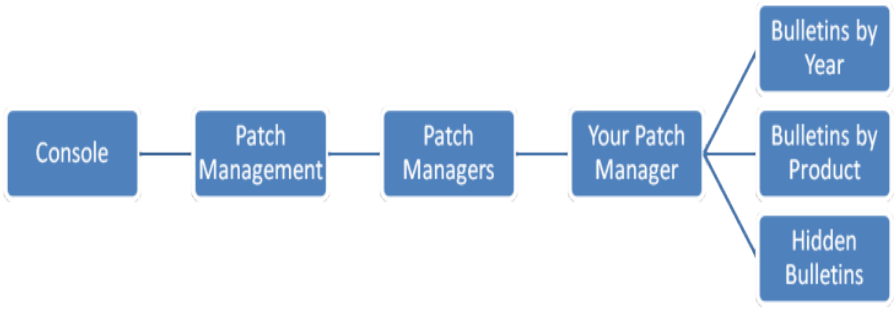
Patch Management regularly checks for new bulletins to ensure that no important patches are missed. Your only task is to deploy these bulletins.

Whenever Patch Management detected a new bulletin, this is visualized by the icon next to the bulletin.

Where do I find Bulletins in the console?

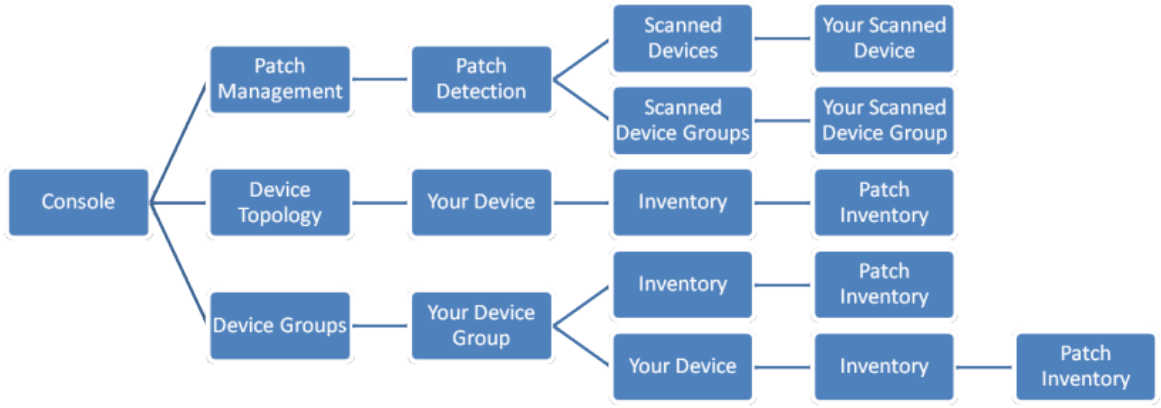
In the Console you find bulletins in different places.

To view all available bulletins go to:



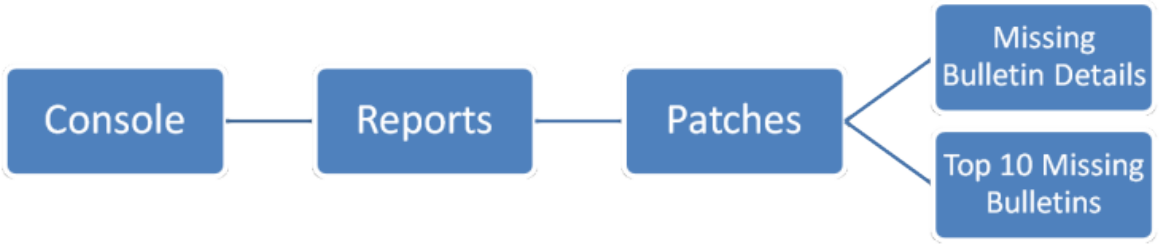
- **Patch Management > Patch Manager > Your Patch Manager > Bulletins by Year**
- **Patch Management > Patch Manager > Your Patch Manager > Bulletins by Product**
- **Patch Management > Patch Manager > Your Patch Manager > Hidden Bulletins**

To view which bulletin belongs to a patch go to **Missing Patches** or **Installed Patches** of the following nodes:



- **Patch Management > Patch Detection > Scanned Devices > Your Scanned Device**
- **Patch Management > Patch Detection > Scanned Device Groups > Your Scanned Device Group**
- **Device Topology > Your Device > Patch Inventory**
- **Device Groups**

To create predefined reports based on bulletins go to:



Related topics

- Bulletins by Year
- Bulletins by Product
- Hidden Bulletins
- All Bulletins
- Downloaded Bulletins
- General Bulletin Information
- Patches of a Bulletin
- Devices affected by a patch
- Products affected by a patch

What can I do in this node?

In this node you can:

- view all available bulletins
- view downloaded bulletins
- select bulletins and deploy them to affected
- hide bulletins
- filter bulletins by:
  - severity
  - time frame
  - status (only new, only affected devices)
  - content

Bulletins by Product

The following topics provide more information about bulletins by product:

- What can I do in this node?

- What is a Device Count?
- Hiding product bulletins

What can I do in this node?

In this node you can:

- view all available product families with their corresponding bulletins
- view downloaded bulletins
- select bulletins and deploy them to affected devices
- hide individual bulletins or all bulletins from a product family

What is a Device Count?

In the overview of all available product families you see a column called **Device Count** . **Device Count** indicates the number of devices in your network affected by bulletins of the product family. If the **Device Count** of a product family is ***0*** , no device is affected by the respective bulletins.

Hiding product bulletins

Bulletins can be hidden individually or they may be hidden by product, that is, all bulletins of a specific product are hidden. In this case the product itself will disappear from the list of **Bulletins by Product** . To hide all bulletins and the product from this view and add it to the **Hidden Bulletins** table proceed as follows. In the table of the **Hidden Bulletins** the bulletins will appear individually and not classified by the product name. Be aware that hidden bulletins cannot be fixed. To hide only some of the product's bulletins select the respective product and proceed from this view. Contrary to the hiding of vulnerabilities, bulletins are always hidden for all users of the console and not per individual administrator.

1. Select the product family to hide in the right window pane.
2. Click **Edit > Hide Product Bulletins**  .
   A message window appears. In this free text box you can enter comments as to why the product bulletins are hidden.
3. Click **OK** to confirm the message and close the window.

The elements will now disappear from the **Hidden Bulletins** tab and be displayed in the **Hidden Bulletins**.

Hidden Bulletins

The following topics provide more information about hiding bulletins:

- What can I do in this node?
- What happens when I hide a bulletin?
- Why should I hide bulletins?
- Unhiding bulletins

What can I do in this node?

In this node you can:

- view and order hidden bulletin
- unhide bulletins

What happens when I hide a bulletin?

When you hide a bulletin it can no longer be deployed and isn't displayed anymore in the following views:

- **Patch/Service Pack Distribution Wizard**
- results of **Patch Detection**
- **Patch Inventory** of devices and device groups
- **Patch Selection** dialog when adding a patch to a patch group
- **Bulletins by Year**
- **Bulletins by Product**

Why should I hide bulletins?

By default when you want to deploy a bulletin all available bulletins can be listed. However some bulletins might be irrelevant to your company and should not be displayed at all.

A policy in your company specifies that only bulletins with a severity of at least Moderate should be deployed for Microsoft products. Therefore you hide all Microsoft bulletins with a severity of Low so that they are no longer available for deployment.

Unhiding bulletins

To remove a bulletin from the **Hidden Bulletins** and make it reappear in the regular bulletin tabs proceed as follows. The elements will reappear directly in the bulletin tabs again.

1. Select the bulletins to unhide in the **Hidden Bulletins** tab in the right window pane.
2. Click **Edit > Unhide Bulletin** .

The bulletins will be taken off the list and be displayed again in the bulletin tabs when selected the next time.

All Bulletins

All Bulletins

This tab provides the list of all available bulletins according to their year of publication with a number of filter options to limit the list for specific requirements.

Note:

When this view is opened for the first time, it is empty.

What can I do in this tab?

In this tab you can:

- Filter the list of available bulletins according to specific criteria
- Select one or more bulletins and have them fixed.
- Move one or more bulletins to the list of hidden bulletins.

Which filter criteria are available?

You can filter the bulletins according to one or a combination of several of the following criteria:

Note:

To start the filtering, click **Sort**.

Parameter	Description
Start Date	Select in this drop down box the starting date of the bulletins to be displayed.
End Date	Select in this drop down box the last publication date for which to display the bulletins.
Start Severity	Select the lowest severity for the displayed bulletins.
End Severity	Select the highest severity for the displayed bulletins. If the bulletins of only one severity are to be displayed both severity fields must display the same severity value.
Contains	Enter any type of string which should be contained either in the **Bulletin Name** or in the **Title** field. The field is case insensitive.
Affected Devices	Check this box to limit the list to the bulletins which affect at least one device in the whole network.

Hiding Bulletins

To hide a bulletin from this view and add it to the **Hidden Bulletins** table proceed as follows. Bulletins are always hidden for all users of the console and not per individual administrator.

1. Select the bulletins to hide in one of the bulletin tabs in the right window pane.
2. Click **Edit > Hide Bulletin** .
   A message window appears. In this free text box you can enter comments as to why the bulletin is hidden.
3. Click **OK** to confirm the message and close the window.

The elements will now disappear from the bulletin tab and be displayed in the **Hidden Bulletins** .

Downloaded Bulletins

The **Downloaded Bulletins** tab shows the list of bulletins that you have worked with in any way, that is, for which at least one patch executable has already been downloaded.

What can I do in this tab?

In this tab you can:

- Filter the list of downloaded bulletins according to specific criteria
- Select one or more bulletins and have them fixed.
- Move one or more bulletins to the list of hidden bulletins.

Which filter criteria are available?

You can filter the bulletins according to one or a combination of several of the following criteria:

> **Note:**
>
> To start the filtering click **Sort** .

Parameter	Description
Start Date	Select in this drop down box the starting date of the bulletins to be displayed.
End Date	Select in this drop down box the last publication date for which to display the bulletins.
Start Severity	Select the lowest severity for the displayed bulletins.
End Severity	Select the highest severity for the displayed bulletins. If the bulletins of only one severity are to be displayed both severity fields must display the same severity value.
Contains	Enter any type of string which should be contained either in the **Bulletin Name** or in the **Title** field. The field is case insensitive.
Affected Devices	Check this box to limit the list to the bulletins which affect at least one device in the whole network.

Hiding Bulletins

To hide a bulletin from this view and add it to the **Hidden Bulletins** table proceed as follows. Bulletins are always hidden for all users of the console and not per individual administrator.

1. Select the bulletins to hide in one of the bulletin tabs in the right window pane.
2. Click **Edit > Hide Bulletin** .
   A message window appears. In this free text box you can enter comments as to why the bulletin is hidden.
3. Click **OK** to confirm the message and close the window.

The elements will now disappear from the bulletin tab and be displayed in the **Hidden Bulletins** .

General Bulletin Information

As the name indicates, the **General** tab provides the general information about the individual security bulletin:

Parameter	Description
Bulletin Name	The name of the bulletin as defined by the concerned application's manufacturer, for example, for Microsoft products the scheme is ms<year of publication>-<running bulletin number>.
Title	The title of the bulletin indicating in general the security vulnerability it will remedy or the name of the concerned application.
Date Posted	The date the bulletin was first posted by the application's manufacturer.
Summary	The Summary field provides a longer textual explanation on the security vulnerability and how it is closed.

This section also includes:

Opening the Microsoft bulletin web page

If the selected bulletin concerns a Microsoft product, it is possible to directly establish a connection with the respective bulletin's page of the Microsoft website to find more information about the individual security bulletin. To do so, proceed as follows:

1. Select the desired Microsoft bulletin in the left window pane and display the **General** tab in the right pane.
2. Click **Edit > Open Microsoft Bulletin Web Page** .

Internet Explorer or otherwise your installed browser will open on your screen and display the page of the selected security bulletin.

Editing the bulletin

To display details about a patch, proceed as follows:

1. Select the patch in the right window pane.
2. Click **Edit > Properties** .
   The **Properties** window appears, displaying all available information about the patch, including a hyperlink to the CVE webpage if it exists.
3. Click **Close** to close the window.

Patches of a Bulletin

A patch can consist of one or more executable files to be installed. One or more of these files might be applicable to different operating systems and thus not be installed on all of them.

The **Patches** tab provides the following information:

Parameter	Description
Patch Name	The name of the executable file contained in the security patch.
Severity	The importance of the security vulnerability and patch, which is represented by a colored flag. This is not necessarily the same severity as that of the bulletin. If a bulletin is classified as Unrated, it is often due to the fact that it contains several executable files with different severity ratings.
Device Count	The number of devices that need this patch to be installed. Be aware that this number is not the total number of concerned devices in the network but the number of devices which the administrator has read and/or write access to.
Status	The current status of the patch.
Size	The fields of this column display the approximate size of the patch file in MB.
Details	This field provides some more detailed information about why a patch download has failed.
CVE ID	The CVE identification concerning the patch as a hyperlink and leads you directly to the respective web page.
Knowledge Base Article	The number of the respective Microsoft Knowledge Base article of the patch if it is a Microsoft patch, otherwise this field remains empty.
Superseded By	Displays if a new version of this patch exists and the name of such a patch.
Information	This field can contain an additional textual description of the vulnerability and the remedy effected by the patch.
Last Downloaded URL	This field displays the complete URL to the patch.

Devices affected by a patch

The **Affected Devices** tab lists the devices which are impacted by this security patch. In the beginning, this list will be empty, it will only be filled in, once the patch operational rule was executed on the target group or devices.

The tab provides the following information:

Parameter	Description
Device Name	This column lists the names of all devices found in the network on which the operational rule was executed for which this patch is applicable, that is, on which it is not yet installed.
Operating System	Displays the name of the operating system which is installed on the respective device.
Operating System Language	Displays the language of the operating system installed on the respective device.

Products affected by a patch

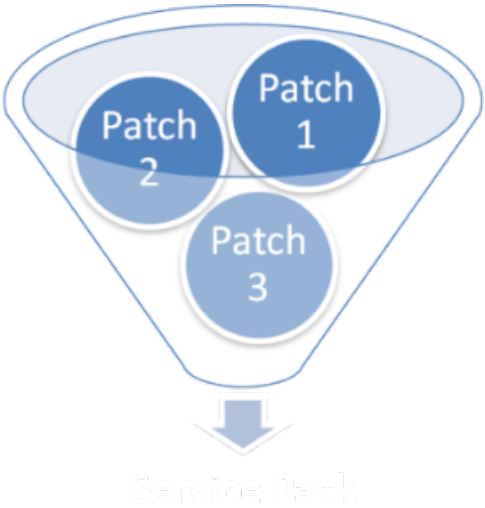
The **Affected Products** tab lists all products which are concerned by this patch, that is, for which security problems are being resolved with this patch. This tab is intended as a reference for easier decision if a patch or one of its executables must be applied for certain clients or if it is not really necessary.

The tab provides the following information about the concerned software products:

Parameter	Description
Patch Name	The name of the executable file contained in the security patch.
Product Name	This field displays the name of the product for which a service pack is available. To the left of the product name you see the bulletin icon, which is color-coded to indicate its *working* status:
Product Family Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Service Pack	Displays the full name of the service pack including the product version, such as Windows XP Service Pack 1.

Managing service packs

A service pack is a collection of updates, patches or enhancements to a software program delivered in the form of a single installable package.



- What can I do with a Service Pack?
- What does the SP1, SP2, SP3, and so on stand for?
- What does the icon next to a Service Pack stand for?

What can I do with a Service Pack?

You can deploy a service pack to devices affected by it. All files from the service pack are downloaded and installed on the respective devices .

What does the SP1, SP2, SP3, and so on stand for?

In a software life cycle several service packs can be released to fix problems and also add new features. Service packs are usually numbered to indicate the version. SP1 (=Service Pack 1) is the first service pack for a software program. For Microsoft XP Professional there are already three service packs available (SP1 - SP3).

What does the icon next to a Service Pack stand for?

Each service pack has an icon next to it to indicate its current status:

-  green: The service pack was downloaded successfully.
-  yellow: At least one file of the service pack was downloaded successfully, but there are still files that haven't been downloaded yet.
-  red: The download of the service pack failed.
-  gray: No file of the service pack was downloaded yet.

For more information, see Service packs by product.

Service Packs by Product

The following topics provide more information about Service Packs by Product:

- What can I do in this node?
- What is a Device Count?
- Displaying affected devices
- Downloading the Language Details of a Patch

What can I do in this node?

In this node you can:

- view all service pack families ordered by name
- view the number of devices affected by a service pack

What is a Device Count?

In the overview of all available product families you see a column called **Device Count** . **Device Count** indicates the number of devices in your network affected by service packs of the product family. If the **Device Count** of a product family is ***0***, no device is affected by the respective service packs.

Displaying affected devices

To display the devices which are affected by a specific patch, proceed as follows:

1. Select the patch package, for which the list of devices is to be displayed, in the table of the **Patches** tab.
2. Click **Edit > Display Affected Devices**  .
   The **Affected Devices List** window appears displaying all devices.
3. Click **Close** to close the window.

You displayed the list of all devices that are affected by a specific patch of the patch group.

Downloading the Language Details of a Patch

To display the list of languages in which the service pack was downloaded proceed as follows:

1. Click **Edit > Display Affected Devices** .
   The **Downloaded Language Details** window appears. It displays the list of all languages in which the service pack was downloaded and the download/publication status of each.
2. Click **Close** to close the window.

Managing dynamic downloader

A **Dynamic Downloader** is a component of Patch Management to automatically download specific patches or service packs.

- What can I do with a Dynamic Downloader?
- How can I find out how many patches match my criteria?
- Where can I follow the download progress?
- Where do I find a Dynamic Downloader in the console?

What can I do with a Dynamic Downloader?

With a **Dynamic Downloader** you can automatically download patches and service packs by defining specific criteria:

- Severity
- Product Family
- Language
- time
- Affected Devices
- Product Name

If a new bulletin is detected which complies with the criteria of an activated **Dynamic Downloader** , it is immediately downloaded.

Microsoft Office is frequently used in your company. Your employers are from different nations and Microsoft Office is installed in English, German and Spanish. To ensure efficiency you always want to have the latest patches and service packs installed. You define a **Dynamic Downloader** for Microsoft Office so that patches and service are available in the three required languages without any delay. After the download you add them to the existing patch group ***Microsoft Office*** . According to the defined schedule the new patches and service packs are deployed to the affected devices in your network.

How can I find out how many patches match my criteria?

At the top of the **Options** tab of a **Dynamic Downloader** there is a message **Estimated Number of Patches to Download** . The text next to it indicates the number of patches that match your criteria, for example, `15 patches` . If `0 patches` displays, modify your criteria until the desired number of patches is shown.

Where can I follow the download progress?

You can follow the download progress in two nodes:

- To follow the current download progress and the status of all patches of a specific dynamic downloader , go to **Patch Management > Patch Manager > Your Patch Manager > Dynamic Downloader > Your Dynamic Downloader** and click the **Status** tab.
- To follow the download progress of all dynamic downloaders, go to **Patch Management > Patch Manager > Your Patch Manager > Downloads in Progress** . Once a patch or service pack is downloaded, it disappears from this node.

Where do I find a Dynamic Downloader in the console?

To view all your existing **Dynamic Downloader** s go to:

For more information about dynamic downloading, see Dynamic downloading.

Dynamic Downloading

The following topics provide more information about dynamic downloading:

- What can I do in this node?
- Dynamic download options
- Status of a dynamic download
- Downloads in progress

> **Note**
>
> Dynamic downloading option is not available for BMC Client Management OnDemand.

What can I do in this node?

In this node you can create, delete and order **Dynamic Downloader**.

Dynamic download options

In this tab you can specify the criteria according to which the downloader will recover the patches or service packs from the Internet. It provides a number of different criteria, such as the patch severity or the publication date or time. You can filter the patches or service packs by only one option or you can use all available options together to find very specific patches or service packs.

> **Note:**
>
> Don't forget to check the **Enable Dynamic Downloader** box, to activate the dynamic downloader. If this box is not checked no patches will be downloaded for the criteria you defined.

Status of a dynamic download

This tab provides information about the patches concerned by the dynamic downloader. It displays the list of all patches or service packs that match the criteria defined for this dynamic download and the current download status of each matching patch.

Adding downloaded patches to a patch group

Once patches are downloaded they can directly be added to existing patch groups from this view. Be aware, that this option is only available if at least one patch group exists. To do so, proceed as follows:

1. Select one or more successfully downloaded patch(es) in the downloader status table.
2. Click **Edit > Add to Patch Group**  .
   The **Patch Groups** window appears providing the list of all existing patch groups.
3. Select the group to which the patch(es) is/are to be added and click the **OK** button.

The selected patch(es) will be added directly to the group.

Downloading failed patches again

If for example a patch download has failed during a dynamic download, it is possible to request another download try for this individual patch. To do so, proceed as follows:

1. Select the failed patch in the table of the right window pane.
2. Click **Edit > Download Again**  .

The download of the patch will be restarted immediately.

Downloads in progress

In this node you can:

- follow progress of patches or service packs that are currently being downloaded or waiting to be downloaded
- remove patches or service packs if the downloaded has not yet started

Once the download is finished, the entry disappears from the list.

Locally accessing patch management

The **Patch Management** node of the **Agent Configuration** provides access to the patch and service pack situation of the device. If you do not have a license for this feature this node will not be present in the console. The **Patch Management** information displays in the following tabs:

- Locally accessing installed and required patches
- Locally accessing installed and required service packs
- Status before and after installation

Locally accessing installed and required patches

The following topics guide you about installed and required patches (local access):

- Installed patches (local access)
- Required patches (local access)

Installed patches (local access)

The **Installed Patches** tab displays the list of all patches which are already installed on the selected device. It provides the following information about these patches:

Parameter	Description
Patch Name	This field displays the name of the patch as provided by the product manufacturer.
Product Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Bulletin Name	The name of the bulletin as defined by the product's manufacturer, for example, for Microsoft products the scheme is `msyear of publication-[running bulletin number` .
Language	The language of the patch that is used, that is, the language of the operating system or the application for which the patch was installed.

Required patches (local access)

The **Required Patches** tab displays the list of all patches which are currently missing on the selected device. It provides the following information about these patches:

Parameter	Description
Patch Name	This field displays the name of the patch as provided by the product manufacturer.
	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.

Parameter	Description
Product Name	
Bulletin Name	The name of the bulletin as defined by the product's manufacturer, for example, for Microsoft products the scheme is `msyear of publication-running bulletin number` .
Language	The language of the patch that is needed, that is, the language of the operating system or the application requiring the patch.

Locally accessing installed and required service packs

The following topics provide more information about installed and required service packs (local access):

Installed service packs (local access)

The **Installed Service Packs** tab displays the list of all service packs which are already installed on the selected device. It provides the following information about these service packs:

Parameter	Description
Service Pack Name	The name of the service pack that contains the bulletins and patches that were applied to the respective product.
Product Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Language	The language of the service pack that is used, that is, the language of the operating system or the application for which the patch was installed.

Required service packs (local access)

The **Required Service Packs** tab displays the list of all service packs which are currently missing on the selected device. It provides the following information about these service packs:

Parameter	Description
Service Pack Name	The name of the service pack that contains the bulletins and patches to be applied to the respective product.
Product Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Language	The language of the service pack that is needed, that is, the language of the operating system or the application requiring the patch.

Status before and after installation

The following topics provide more information about the tabs:

- Status before Installation
- Status after Installation

Status before Installation

The **Status before Installation** tab displays the list of all patch executables which are missing and which will be installed on the device via the patch group the device is a member of.

The tab provides the following information about the patches:

Parameter	Description
Patch Name	This field displays the name of the patch as provided by the product manufacturer.
Product Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Language	The language of the patch that is needed, that is, the language of the operating system or the application requiring the patch.
Status	The current status of the patch. This can be either `Requested` or `Received` to indicate that the patch was requested for download or was successfully downloaded to the device. Once all patches have the status `Received` the installation will start and the situation will be displayed in the next tab **Status after Installation** .

Status after Installation

The **Status after Installation** tab displays the list of all patch executables which are being installed on the device via the patch group the device is a member of and provides the final information about the patch installation.

The tab provides the following information about the patches:

Parameter	Description
Patch Name	This field displays the name of the patch as provided by the product manufacturer.
Product Name	This field displays the full name of the software product family, such as Windows XP Home Edition or Adobe.
Language	The language of the patch that is needed, that is, the language of the operating system or the application requiring the patch.
Status	The current status of the patch. This can be either `Requested` or `Received` to indicate that the patch was requested for download or was successfully downloaded to the device. Once all patches have the status `Received` the installation will start and the situation will be displayed in the next tab **Status after Installation** .

Patch Service Pack Distribution Wizard

What Does this wizard?

This wizard guides you through the complete patch deployment process. It provides you with the following types of deployment:

- Automated Deployment Process
- Semi-automatic or Manual Deployment Process

Where can I access this wizard?

The **Patch/Service Pack Distribution Wizard** can be launched from different locations in the CM console and depending on this location it will provide different options. The wizard can be launched from the following locations:

- the **Patch/Service Pack Distribution** option of the main **Wizards** menu, accessible from any location in the console
- the **Edit> Fix** icon, available in different locations under the **Patch Management** node and the patch inventory of devices and device groups

The following topics are provided:

- Automated Deployment Process
- Semi-automatic or Manual Deployment Process
- Activation - Patch Distribution Wizard

Automated Deployment Process

With this type of deployment, you define a patch job once for a specific type of patch or service pack. It will be applicable for a specific type of target group and every time a patch or service pack becomes available or a new device is included into the group, the necessary patches will be automatically deployed without manual interference.

Related topics

- Automated Deployment Type
- Patch Criteria
- Deployment Options
- Office Options
- How to Deploy
- Assigned Devices for patch jobs

Automated Deployment Type

Patch management allows you to configure two different types of deployment:

- completely automated deployment via patch jobs
- manual deployment via patch groups.

In this first window you must define which type to use.

1. Leave the **Patch Job** radio button selected if you wan to create a completely automated patch deployment.

Then you must define the following options:

1.
   - Enter the name for the new patch job into the **Add patches to this patch job:** field.

> **Note:**
>
> If this job already exists, the patches and targets you select via this wizard will be added to the existing job, and any modifications you make will be applied also to the existing targets.

- Specify via the **Deployment Options** drop-down list to use the patch options defined in the **Preferences** or to freely configure them (**Let me configure them**)

2. To create a more manually oriented patch group select the **Patch Group** radio button.

> This option is not available if the wizard is called from under the **Patch Jobs** node.

3. Click **Next** .

Patch Criteria

In this window, you must define the criteria according to which the patches are downloaded and added to the patch job. You can choose to use only one criterion, two or all three of them.

1. Check all boxes under the **Severity** heading, for which the patches are to be included.
2. Check all boxes under the **Type** heading, for which the patches are to be included.
3. Select the corresponding radio button under the **Product Name** heading, if patches for all products or only for one or more specific products are to be included.
   If you selected the limited product option, you need now to check the boxes for all products in the now accessible list of products.

> This also means, that if a new product becomes available, for example, *Windows 8* , it will not automatically be added to the list of products to patch.

> With BCM 12.6, you can distribute patches to specific products from a product family, rather than distribute it to the entire product family. This enhancement comes as part of upgrading the patch management system in BCM, which is provided by Shavlik Protect 9.2.
> For example, Adobe is represented as
> - Acrobat
> - Reader
> - AIR
> - After Effects
> - Bridge

- Creative Cloud
- Digital Editions
- Distiller
- Dreamweaver
- Elements
- Fireworks
- Flash Builder
- Flash Professional
- Illustrator
- InDesign
- Shockwave
- Adobe Photoshop

4. Click **Next**.

Deployment Options

This window will only be displayed if you selected to configure your patch options differently than those defined in the **Preferences** .

Here you have the same three tabs, in which you can define the general options for the deployment of the patches/service packs:

- **Preinstallation**
- **Installation**
- **Reboot**

For more information about the parameters of the tabs, refer to the The Patch Group Tab topic.

1. Make the desired changes in the respective tabs.
2. Click **Next** .

Office Options

This window will only be displayed if you selected to include patches for Microsoft Office in your patch job. Here you must provide some specific information about the Microsoft Office products.

1. From the **Product Name** list select the Office product.

You can select more than one product by holding the CTRL key during the selection.

Note:

Be aware however, that the products you select at the same time must have their information stored in the same location, that is, the required information must be accessible via the same path.

2. Click **Add** .
   The **Path Configuration** window displays.
3. Enter the required information for the selected products into the respective boxes.
4. Click **OK** to confirm the data.
   The products are now added to the list of products to patch with the specified information.
5. If the data is already available in another patch job you can also directly copy the information:
   a. Click **Copy from Patch Job** .
      The **Select a Patch Job** windowdisplays.
   b. Select the patch job containing the information from one of the available lists.
   c. Click **OK** .
      The information is automatically copied and added to the current patch job, overwriting any information that might were entered previously for matching products.
6. Click **Next** .

How to Deploy

In this window you can schedule the interval and time at which the patch job is executed. For this you have several options.

1. Under the **Deployment Schedule** you must define the execution interval, for which you have the following choices:
   - **Monthly** : This option allows you to execute the patch job on "the first, second, third, fourth, last Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday of the month".

1. For this you must select the day of the week (**S** = **Sunday** , **M** = **Monday** , etc.) on which it is to be executed.
2. and you must define on which of the 4 available times this day occurs to execute, for example, on the first, second, third or fourth of the month.
   - **Weekly** : This option allows you to execute the patch job every week for a given set of days. Selecting this option will make the day's selection panel available to give you the opportunity to specify which day(s) of the week the patch job will be executed.

1. For this you must select the day of the week (**S** = **Sunday** , **M** = **Monday** , etc.)
   - **Daily** : With this option the patch job will be executed dayly and no further definitions are required in this section.
2. Under the **Time Period** section you must define the time of execution:

- You can either select to execute whenever the downloaded patches become available, in which case you must select the **Deploy anytime according to the above schedule** radio button.
- Or you can select to execute at very specific times or timeframes, in which case you must select the **Deploy only during this time** radio button and specify the following:

1. In the first drop-down list you must define the transfer schedule for the patches to the concerned devices:
   - they can be transferred at the beginning of the specified start time to limit the network load to the defined patch times.
   - they can be transferred to the devices as soon as they are available to be ready for immediate installation when the start time arrives.
2. Select the **Start:** and **End:** time during which the patches of the patch job are to be installed. If the patch execution is to be finished in any case check the **No End Time. Run Till Completed.** box instead of defining one.

> **Note:**
>
> Be aware that any individual patch for which the installation was started will be finished even if the **End:** Time has arrived.

3. Click **Next** .

Assigned Devices for patch jobs

In this step the target devices and device groups are selected. To add devices or groups select the respective buttons on top of the list box. A patch group can contain device groups and individual devices at the same time.

To assign a device or device group to the patch group proceed as follows:

1. Click **Assign a device group to a SCAP job** or **Assign a device to a SCAP job** / on top of the list box.
   The **Assign Target Devices or Groups** pop-up windows appears, displaying all available devices or groups..
2. Select the desired device or device group from the window.
3. Click **OK** to confirm the assignment and close the window.
4. The selected targets will be added to the list
5. Click **Finish** to confirm all choices and to start the download and patching process.

Semi-automatic or Manual Deployment Process

This type allows you to either deploy patches according to your predefined settings or you can specifically define settings for a deployment.

Related topics

- Patch Deployment Type
- Bulletins - Patches - Service Packs
- Patch Manager - Deployment Process
- Patch Group - Deployment Process
- Patch Group Configuration
- Assigned Devices for patch groups
- Download Options
- Patch Languages
- Pre-installation Parameters
- Installation Parameters
- Reboot Options
- Schedule - Deployment Process
- Task- Deployment Process
- Fix Selection
- Mail - Deployment Process

Patch Deployment Type

In the first window of the patch deployment wizard, you must decide to run an automatic deployment, that is, use the default values defined for deployments for your current deployment, or to configure this deployment with specific parameters.

1. Click the **Let me configure the rules for a customized deployment** radio button and then click **Next** to continue and configure the desired values as required.
    - Leave the **Select the type of deployment you would like to perform.** radio button selected for automatic deployment.
    - You can specify a name for the new patch group to be created by entering it in the **Add patches to this patch group:** field.
    - To define a specific deployment schedule select the **Using a schedule that I define** option in the **Deploy the patches:** drop-down list.
2. Click **Next** to continue.

Bulletins - Patches - Service Packs

This first window, **Bulletins - Patches - Service Packs** , is always empty when opened. To display bulletins/service packs you must first make a selection in the boxes previously displayed the list box. Following you can see the list of sorting options that are available in this window, options can be used individually or be combined. Click **Sort** to apply your filters and display the list. If no filters are selected all available bulletins/service packs of the current year will be displayed, sorted by their severity. Double-clicking a bulletin will open its **Properties** window displaying the available information about it.

Bulletins

To patch the target devices via bulletins proceed as follows:

1. a. Check the **Bulletins Only** radio button.
   b. Select the options according to which the bulletins to be displayed are to be filtered.
   c. From the displayed bulletins select one or more and click **Add** to add their patches.
   d. If the bulletins are on different pages of the view repeat step 3 until all bulletins are added.
   e. Click **Next** to continue with the next step. **Service Packs**

To patch the target devices via service packs proceed as follows:

1. a. Check the **Service Packs Only** radio button.
   b. Select the options according to which the service packs to be displayed are to be filtered.
   c. From the displayed service packs select one or more and click **Add** to add their patches.
   d. If the service packs are on different pages of the view repeat step 3 until all service packs are added.
   e. Click **Next** to continue with the next step.

Patch Manager - Deployment Process

In the step, the Patch Manager , which is to manage the patching process for the selected patches, must be defined. This window appears the currently defined Patch Manager device, by default this is the master.

1. Select the desired device to be used as *Your Patch Manager* .
   a. To use another device as the patch manager select **Add Patch Manager** on top of the list box.
      The **Add a new Patch Manager** pop-up window displays displaying all devices that can be used as a *Patch Manager* .
   b. Select the device to be used from one of the list boxes.
   c. Click **OK** to confirm and close the window.
      The device will replace the existing Patch Manager and its configuration parameter will be updated accordingly.
   d. Select the new *Patch Manager* from the list.
2. Click **Next** to continue with the next step.

Patch Group - Deployment Process

In this step of the wizard, the patch group must be defined via which the patching of the target devices is to be done. For this you have two choices:

1. First you must decide if an existing patch group is used or a new one to be created:
   - **Create a new patch group**

- **Use existing patch group** If you select this option, the following box becomes accessible displaying the list of existing patch groups. Select the group to which the patches packages are to be added.

2. Check the **Send Email** if an email is to be sent.

> Via this check box, you can define if an email is to be sent to the security personnel regarding the fixing of the selected patches. If an email is sent no task can be created or used.
> Make sure that you have filled in the respective information regarding your mail system in the following locations, otherwise the wizard cannot send an email:
> - the **Email** tab of the **System Variables**
> - the **Email** tab of the **Preferences** window
> - the email address in the account information for the sender in the administrator‘s tab.

3. Check the **Task** option, if a task is to be created for this patch group execution.

> This option is available for all types of wizards and allows you to create a specific task for the operation defined by the wizard. This option will not be available if the option **Send Email** is activated.

4. Check the **Use Existing Task** box, if the currently defined patch application is to be assigned to an already existing task.
   The drop-down box to the right will become available and display the list of all existing tasks of type Patch Distribution, that do not yet have a patch distribution assigned.
5. Select the desired task.

> This option is dimmed if no tasks of type patch distribution exist

6. Click **Next** to continue.

Patch Group Configuration

This window is only available if you selected to create a new patch group. To do so:

1. Enter the name of the patch group to create in the **Name** field.
2. Enter the name of the directory if the new group is to be created in a specific directory. By default it is created directly under the **Patch Groups** node.
3. Click **Next** to continue with the next step.

Assigned Devices for patch groups

In this step, the target devices and device groups are selected. If you chose to use an existing patch group, this list box displays the devices and groups which are already assigned to the patch group. Otherwise it is empty. To add devices or groups, select the respective buttons on top of the list box. A patch group can contain device groups and individual devices at the same time.

To assign a device or device group to the patch group, proceed as follows:

1. Click **Assign a device group to a SCAP job** or **Assign a device to a SCAP job** / on top of the list box.
   The **Assign Target Devices or Groups** pop-up windows appears, displaying all available devices or groups.
2. Select the desired device or device group from the window.
3. Click **OK** to confirm the assignment and close the window.
4. The selected targets will be added to the list
5. Click **Next** to continue with the next step.

Download Options

This step allows you to limit the patches to be downloaded and applied to certain severities and to force the download of patches which are currently not required.

1. Clear the severities for which the patches of the selected bulletin(s) are not to be downloaded.
2. Define the filter according to which the patches to be downloaded are selected based on affected devices.
3. Click **Next** to continue with the next step.

Patch Languages

In this window of the wizard, you can select for which languages the patch is to be downloaded, that is, the operating system languages of the devices in your network. If the patch group contains affected devices the languages required for these devices are preselected.

1. Click **Next** . Now, before continuing with the next step, an pop-up window appears, displaying the list of patches to be downloaded together with the language it is downloaded in, its size and availability. If a patch does not exist for the required language and thus cannot be downloaded, it is shown with a red x instead of the green check mark in the **Availability** column.
2. To make modifications in the list of patches to download click **Cancel** , this will return you to the **Patch Languages** window, where you can make modifications to your language selection.
3. Click **OK** to confirm the list and continue with the next step.If in the list of selected patches, either in the first wizard window or via the inventory list selection you have selected a patch that was replaced with a more recent patch than the selected one, the **Superseded Patches** window appears. It lists all patches in the inventory which have more recent versions. You

have the choice here to either just continue, then the initial patch and the superseding patch will be installed or you can cancel and restart the fixing process by selecting the more recent patch version.

Pre-installation Parameters

The pre-installation parameters define the user interaction of the patching process before launching the patch installation. You can define via these parameters if the user is provided with any type of information or choices regarding the patch installation.

1. Check the **Information Window** box if a message is to be displayed to the user.
2. Enter the text of the message into the **Message to Display** box. Be aware that this message will not be localized, it displays for all operating system languages in the language that it is defined here. You can also leave this text box empty, in this case the default message (*Security updates are being deployed. When you log off, your system will reboot and the security updates will be installed.*) will be displayed which is localised in all console languages.
3. Check the **Allow User to Extend Countdown Timer** box, if the user is to have the possibility of postponing the patch installation.
4. Enter the extension values in the following text boxes.
5. If an operational rule is to be executed before installing the patches enter it here, by clicking **Browse** and selecting it in the appearing window.
6. Click **Next** to continue.

Installation Parameters

In this step of the wizard the behavior of the patch group will be configured. If the group already existed, the values defined for that group will be displayed in the window and you can make any necessary changes. If the group was newly created the window shows the default values defined in the **Preferences** .

1. Mark the boxes of the options to apply differently than defined by default.
2. Click **Next** to continue.

Reboot Options

The **Reboot Options** box provides the parameter settings for a safe restart of the target devices after the patch group installation. These parameters are only of interest if **Reboot after deployment** option is chosen for the **Reboot Type** . When safe restart is selected, a pop-up window appears on the target screen informing the user of the impending restart and providing him with the options defined in this box.

If the group already existed, the values defined for that group displays in the window and you can make any necessary changes. If the group was newly created, the window shows the default values defined in the **Preferences** .

1. Mark the boxes of the options to apply differently than defined by default.

2. Click **Next** to continue.

Schedule - Deployment Process

This step of the wizard concerns the scheduling of the patch installation on the targets. Same as with the configuration and restart options in the last window, this dialog box appears either the predefined schedule of an existing group or the default schedule for a new group.

1. Define the date and time at which the assignment of the patch group to the targets is to be effected in the **Select Patch Group Assignment Date** box.
2. Define the date and time at which the actual installation of the patches contained in the patch group is to take place in the **Select Patch Installation Date** box.
3. Now, if not task or email was requested, click **Finish** to confirm all choices and to start the download and patch package creation process, otherwise click **Next** to proceed to the definition for the connected task or email to be sent.

Task- Deployment Process

This optional step of the wizard allows you to directly create a task for the patch application defined via this wizard or to assign it to an already existing task. This option is only available if you checked the corresponding box in the first window of the wizard.

1. Define all parameters for the task that is to follow this patch group.
2. Click **Finish** to confirm all choices and to start the download and patch package creation process.

Fix Selection

This window of the wizard defines which type of the wizard is to be executed. The window offers you the following different options:
Fix Selection

In this box, you define which of the available patching options you want to apply for fixing the selected vulnerabilities. Depending on the location from where the wizard was launched, this either applied to the selected patch or all patches of the bulletin.

1.
   - **Download Patches** This wizard allows you to download several selected patches at the same time and automatically create the patch packages, which are required for vulnerable devices or device groups, and publish them to the master.
   - **Download and Apply Patches** This wizard allows you to download several selected patches at the same time and automatically create the patch packages, which are required for vulnerable devices or device groups, publish them to the master and deploy them to the target devices and groups. **Send Email**

Via this check box you can define if an email is to be sent to the security personnel regarding the fixing of the selected patches. If an email is sent no task can be created or used.

Ensure that you have filled in the respective information regarding your mail system in the following locations, otherwise the wizard cannot send an email:

1.
   - the **Email** tab of the **System Variables**
   - the **Email** tab of the **Preferences** window
   - the email address in the account information for the sender in the administrator‘s tab. **Task**

This option is available for all types of wizards and allows you to create a specific task for the operation defined by the wizard. This option will not be available if the option **Send Email** is activated. **Use Existing Task**

Check this box, if the currently defined patch application is to be assigned to an already existing task. The drop-down box to the right will become available and display the list of all existing tasks of type Patch Distribution that do not yet have a patch distribution assigned. Select the desired task. This option is dimmed if no tasks of type patch distribution exist.

Click **Next** to continue.

Mail - Deployment Process

This optional wizard window will only be displayed if you chose to send an email to the members of your organisation concerned with the fixing of patches.

1. Enter all information required for the email into the respective boxes.
2. Click **Finish** to start the download and patch package creation process and to send the email.

Activation - Patch Distribution Wizard

The last option provided by the patch wizard is to directly activate patch group and thus start the patching process. If you do not directly activate, you must go to the respective patch group in the console and manually activate it at the desired time. To directly go to the patch group selected or created in the wizard after the window has closed, check the **Go to Patch Group** box.

Instead of moving the console focus to the patch group, you can also go directly to the task if an existing one was selected or a new one created. For this check the box **Go to Task** .

To directly activate the group click **Yes** , otherwise click **No** . Click **Cancel** to abandon the patch download and application process you just defined.

Managing peripheral devices

Data leakage or privacy breaches can cripple your organization. Yet many companies focus on external threats while forgetting to protect against internal risks, such as those that arise from the proliferation of removable devices.

Peripheral Device Management protects your business through effective device management and lockdown of unauthorized devices, such as USB drives, cell phones, portable hard drives, and music players:

- Block use of prohibited external devices
- Understand and manage all removable devices on your network
- Manage inbound and outbound communication from all endpoints

Related topics

- Creating your first device rule
- Monitoring local events
- Monitoring the results on the master

Creating your first device rule

Windows Device Management in the BMC Client Management is concerned with peripheral devices and allows you to control the usage of these as well as the connected movement of data, especially all data that leaves the company. This is done by enabling or disabling specific peripheral devices in your network, for example, USB storage, printers, modems, and so on.

> **Note:**
>
> The Windows Device Management functionality is, as its name indicates, only applicable to Windows, version 2003 and later.

> **Note:**
>
> It is strongly recommended to only create one single rule per peripheral device class. Multiple rules might contradict each other and thus result in not applying the desired rules in the network. It is however possible to have different rules for the different peripheral classes, for example, one rule for all USB storage devices, one rule for all CD/DVD burners, another one for all modems, and so on.

Prerequisites

To execute the examples provided in this section we assume that:

- you have different USB storage devices available.
- a browser is installed on your master.

Device Management Procedures

The device management procedures explain the different elements of Windows device management and guide you through the generation, monitoring and interpretation of the generated events and data. This is done via the following steps:

- Configuring Windows Devices for Device Management.
- Controlling the Data via USB Storage Devices.
- Device Control Event Monitoring

Controlling the data via USB Storage Devices

In this example we will create an operational rule which controls the USB storage devices. That means we will define which storage units are allowed to connect to the network devices via USB and refusing all others. The rule will therefore have the following steps:

- **Reset Device Management Rule** to make all previous USB storage device rules invalid.
- **Create Device Management Rule** allowing the respective device.
- **Create Device Management Rule** forbidding all other USB storage devices.

1. Click **Wizards > Operational Rule Creation** .
   The **Operational Rule Creation Wizard** displays on the screen with its first window.

   > **Note:**
   >
   > The left pane of the wizard window appears all available steps of this wizard.

2. Enter *USB Storage Device Control* (or any other desired name) into the **Name** box.
3. Leave all other parameters as they are, because neither packages will be distributed nor dependencies are required for this rule.
4. Click **Next >** to continue.
   The **Steps** window displays.
5. Select **Add Step** on top of the list box.
   The **Select a Step** pop-up windows appears.
6. Expand the item **Windows Device Management** and select step **Reset Device Management Rule** .

   > A rule defining the management of a specify device class should always use the **Reset Device Management Rule** as its first step. This is to make sure there are no other rules that are already assigned or used and that might interfere with this new rule.

7. Click **Add** .
8. Leave all values as they are, because the **USB Storage Devices** is already preselected in the **Class Type** box.
9. Click **OK** to confirm and add this step to the list of **Selected Objects**.
10. Select step **Create Device Management Rule**.
11. Click **Add** .
    The **Properties** dialog box appears. The **USB Storage Devices** option is already preselected.
12. Check the box **Enable**. This will allow the usage of the defined USB storage.
13. In the **Filter Type** box select **Exact Match**.
14. Into the **Filter** box enter the exact name of the USB storage to allow.

> If the name is not correct, the storage will not be recognized when it is connected.
> If you are not sure about the exact name see Option (c) now to find out.
> To allow all USB keys of a specific manufacturer or type see Option (b) now.

15. Click **OK** to confirm and add this step to the list of **Selected Objects**.
16. Select step **Create Device Management Rule** again.
17. Click **Add** .
    The **Properties** dialog box appears. **USB Storage Devices** is already preselected.
18. Leave the **Enable** box clear unselected. This will prohibit the usage of all other USB storages.
19. In the **Filter Type** box select **Pattern** .
20. Into the **Filter** box enter the wildcard character asterisks (*).
21. Click **OK** to confirm and add this step.

> When creating a list of conditions always start with the most restrictive condition and work your way down to the most general. A step prohibiting or allowing „the rest" or „all others" should always be the last in the rule.

22. Click **OK** again to confirm the list of steps for the operational rule and close the window.
23. Click **Finish** to confirm the settings of the new operational rule.
    A confirmation window appears which allows you to directly continue with the **Operational Rule Distribution Wizard**.
24. Click **Yes** to continue directly with the distribution of the new rule.
    The **Operational Rule Distribution Wizard** displays on the screen.

> **Note:**
>
> The **Name** box is inaccessible because the operational rule to distribute is already preselected, that is, the one we just created.

25. Leave all options as they are and click **Next>** to continue.
26. Select **Assign Device Group** on top of the list box in the new window.
    The **Assign to Device Group** pop-up window appears.
27. Select the group *All Devices*.
28. Click **OK** to confirm and close the window.
    The device group will be added to the list window.
29. Click **Finish** to confirm all choices and launch the assignment and configuration process.
30. The last option provided by the wizard is to go directly to one of the objects, that is, the operational rule or the task, if one was created. for our example we will directly activate the rule and change to focus to it, therefore check the **Go to Operational Rule** box and click Yes, to directly activate the rule.
    The device group will be added to the table in the right pane with a status `Activated`.

To follow the assignment process select the ensuing *All Devices* subnode and follow the status in the right window pane for the group members.

Related topics

- Allowing all devices of a specific manufacturer
- Correcting device name

Allowing all devices of a specific manufacturer

Instead of limiting the usage to one specific USB key, you can also limit the usage to all keys of a specific manufacturer, for example to those that your company provided to all those employees needing to exchange data. For this, proceed as follows:

1. In the **Properties** dialog box enter the following values:
2. In the **Filter Type** box select **Pattern**.
3. Into the **Filter** box enter the part name of the USB key that is common to all keys of the manufacturer preceded if necessary and/or followed by the asterisks (*) wildcard character, for example, ***Cruzer***.

   > This will allow all USB storages whose name includes `Cruzer` to be used on the managed devices.

4. Proceed with Point 14 (page 11) of the general procedure.

Correcting device name

When specifically allowing or forbidding the usage of a certain device peripheral the correct name under which the device will be registered in the **Device Manager** must be used. You can find the correct name thus:

1. Connect the device peripheral in question to a device.
2. Open the **Computer Management** window.
3. Open the **Computer Management (local)>System>Device Manager** node in the left window pane.
   In the right window pane the local device will now be displayed with all its parameters.
4. Open the node **Disk Drives**.
5. Copy the name that you find here for the desired peripheral exactly to the **Filter** box of the step.

Monitoring local events

Events can be monitored locally and centrally once the data is uploaded to the CM database, and they can be monitored individually for single device or for all the members of the group. This section provides information on monitoring local events.

After the status for the device group members displays `Executed`, the rule is received on the target and the specified peripheral device control is activated. You can now monitor what is happening concerning device management locally on each of the devices of your group. For this some device management activities need to be carried out on one of the devices, that is, the master.

Once some power management activities are carried out on one of the devices you can monitor these as follows locally:

1. Open the node **Device Topology> Master> Agent Configuration> Module Configuration> Windows Device Management**.

   > This node displays in its first tab the configuration parameter concerning the event logging which was activated via the first operational rule.

2. Select the next tab, **Rule List** .

   > Here you can see the list of all steps of the device rules that are assigned to the currently selected device. In our example there is only one rule yet, consisting of two steps. The first step, the rule reset step, will never appear in this list.

3. Now select the tab **Events**.

   > As we have activated event logging, every time a USB storage is connected to the device an event is logged in this table.

4. Connect the USB storage device to the master that was admitted in the second step. Execute some operations on it, copying, creating, deleting, and so on.
5. Now connect another USB storage device to the master.

> The master will recognise the new hardware, it displays in the Windows Device Manager window but not in the Windows Explorer, because it is unusable. Depending on the operating systems of the master, an error message might appear in the SysTray that an error occurred with the newly found device.

6. In addition an event is logged by the "/> agent and displayed in the tab.

For information about monitoring events centrally, see Monitoring the results on the master.

Monitoring the results on the master

Up to now, the event data is only available locally on the agent. However, to be able to print reports on this topic and to view them in the console these events must be specifically uploaded to the master and its database. This is done via an operational rule:

> **Note:**
>
> By default, these events are configured to be uploaded every 24 hours, that is, at midnight to the master database. If the agent is not running at this time the events will be uploaded at agent startup. If this schedule does not correspond to your requirements you can assign it a different schedule. Information about how to do so, you can see in the Configuration Management topic.

1. Go to the **Operational Rules** top node in the left window pane.
2. Click **Create Operational Rule** .
   The **Properties** dialog box appears.
3. Enter *Upload Resource Management Events* into the **Name** box and then click **OK**.
   The new operational rule is added to the list of members in the right pane.
4. Double-click the operational rule.

> In the now displayed **General** tab, you can review the basic information of the operational rule.

5. Go to the **Steps** tab.

6. Click **Add Step** to add the first step.
   The **Select a Step** pop-up window appears. It displays the list of available steps in its **Available Steps** box.
7. Double-click the **Event Log Manager** folder.
8. Select the step **Upload Events** and click **Add** .
   The **Properties** dialog box appears.
9. In the **Model Name** box select the **Windows Devices** value and leave all other boxes as they are.
10. Click **OK** to confirm the parameters and **OK** again to confirm the new step.
    The operational rule is now configured and must be assigned to the target, that is, the group *All Devices* .
11. Go to the **Assigned Objects > Assigned Device Groups** node in the left window pane under your newly created operational rule.
12. Select **Assign Device Group** .
    A confirmation window appears.
13. Click **Yes** , to activate the operational rule automatically.
    The **Select a Device Group** pop-up window appears.
14. Select the group *All Devices* from the list.
15. Click **OK** to confirm the assignment.
16. Follow the execution of the operational rule under the assigned group.

    > Once the status is `Executed` for all members of the all data is uploaded.

17. To verify this go to the **Alerts and Events** node of the master.

    > This node displays the list of all events registered by the event log models for the selected device group.

18. To display the device management events instead of the default software distribution events select **Windows Devices** from the **Model Name** drop-down list.
19. Click **Find**.
    The following table will now display all events that were uploaded and are continued to be uploaded.

Now all data is uploaded and ready and reports can be generated.

Managing devices remotely

The BMC Client Management is an advanced systems management software that provides a reliable way to monitor all systems on a network. It isolates the exact point of failure when issues occur and makes it possible for network and system difficulties to be resolved quickly.

The Remote Manager of BMC Client Management includes accessing remote services such as network applications, transferring files among servers and workstations, administering servers, and viewing or taking control of distributed desktops to help users with issues. Through the **Remote Control** node you can directly access any of the managed devices within your system.

The Remote Manager of BMC Client Management provides a reliable way to monitor all systems on a network. It isolates the exact point of failure when issues occur and makes it possible for network and system difficulties to be resolved quickly. It includes accessing remote services such as network applications, transferring files among servers and workstations, administering servers, and viewing or taking control of distributed desktops to help users with issues. Through the **Remote Control** node you can directly access any of the managed devices within your system, however, you must ensure that you have the corresponding login information and access rights.

The Remote Manager provides its operations via the following nodes for individual devices and device groups:

- **Direct Access**
- **Remote Control**
  - Remotely controlling a device through the BCM Java Console
  - Remotely controlling a device through a web browser

This section includes following topics:

Remote Manager Licenses

Contrary to the other BMC Client Management modules, the Remote Manager requires two different licenses:

1. **Direct Access**
   This license allows the administrator to use the **Direct Access** functionality to directly access remote devices. This license also includes the **File Transfer** functionality.
2. **Remote Control**
   This license is required for remotely accessing and controlling the devices.

Remote Manager capabilities and access rights

To be able to directly and remotely access devices an administrator needs specific capabilities and access rights for the different functionalities.

Remote Control through the BCM Java Console

- **Remote Control** node: **Remote Control - View** .
- The capability **Remote Control - Manage** is required to access remote devices and take over control of these.
- The capability **File Transfer - Manage** is required if you also intend to transfer files to and from the remote devices during a remote control session.

Remote Control through a web browser

- Remote Control from a supported browser.
- The capability **Remote Control - Manage** is required to access remote devices and take over control of these.
- The capability **Send and Request** information is available to and from the remote device during a remote control session.
- The capability **File Transfer - Manage** is not available to and from the remote devices during a remote control session.

Direct Access

- **Direct Access** node: **Direct Access - View** .
- The capability **Direct Access - Manage** is required to access remote devices and execute any type of operation on their file systems, registry, services or processes.
- The capability **File Transfer - Manage** is required if you also intend to transfer files to and from the remote devices during a direct access session.

For more information about managing devices remotely, see the following topics:

- Remote management overview through the BCM Java Console
- Remotely controlling a device through the BCM Java Console
- Remotely controlling a device through a web browser
- Directly accessing a device
- Certificate installation on systems

Remote management overview through the BCM Java Console

The Remote Manager of BMC Client Management includes accessing remote services such as network applications, transferring files among servers and workstations, administering servers, and viewing or taking control of distributed desktops to help users with problems. Through the Remote Control node you can directly access any of the managed devices within your system, however, you need to ensure that you have the corresponding login information and access rights.

To be able to establish a connection you might be required to have the login information of the managed device, that is, the login name and its corresponding password, as well as the agent access rights, which are defined through the agent's user interface. This setting is defined via the **System Variables**.

On the side of the client, the agent icon in the systray, which normally is blue and oscillates green, when the agent is busy, turns yellow , to indicate to the user that the client was taken over via remote control.

Once the remote control connection is established, the target screen appears in the full console window. By default the icon bar is externalized from the console window and displays as a separate panel next to the maximized console window. You can change this setting by clicking the Maximize icon to return to the usual console display.

You can take over the control of a remote device from the Search , Device Groups and Device Topology location.

> **Attention**
>
> If you are using NAT configurations the devices can only be accessed via **Remote Control** if agent tunneling is activated.

Remotely controlling a device through the BCM Java Console

The Remote Manager of BMC Client Management includes accessing remote services such as network applications, transferring files among servers and workstations, administering servers, and viewing or taking control of distributed desktops to help users with problems. Through the Remote Control node you can directly access any of the managed devices within your system, however, you need to ensure that you have the corresponding login information and access rights.

To be able to establish a connection you might be required to have the login information of the managed device, that is, the login name and its corresponding password, as well as the agent access rights, which are defined through the agent's user interface. This setting is defined via the **System Variables** .

On the side of the client, the agent icon in the systray, which normally is blue and oscillates green, when the agent is busy, turns yellow , to indicate to the user that the client was taken over via remote control.

Once the remote control connection is established, the target screen appears in the full console window. By default the icon bar is externalized from the console window and displays as a separate panel next to the maximized console window. You can change this setting by clicking the Maximise icon to return to the usual console display.

You can take over the control of a remote device from the **Search** , **Device Groups** and **Device Topology** location.

Note:

If you are using NAT configurations the devices can only be accessed via **Remote Control** if agent tunneling is activated.

The following paragraphs lead you through your first steps when remotely controlling devices in your network.

You can take over the control of a remote device from the **Search** , **Device Groups** and **Device Topology** location. Following topics provide more information about remotely controlling a device:

- Establishing a remote control session
- Switching between remote control sessions
- Launching a new task
- Transferring files between devices via remote control
- Disconnecting from a remote control session
- Maximizing the remote screen
- Copying and pasting in a Remote Control session
- Sending an CTRL+ALT+DEL command
- Modifying the active remote control properties

Establishing a remote control session

To establish a connection with the selected client proceed as follows. It is possible from any point at which a device is selected to establish a remote control session with it.

Note:

Before you connect, however, ensure that you have the corresponding permissions to establish the connection.

1. Select a device in the left window pane under the **Device Topology** node, or the relay.
2. Select the **Remote Control** node of the device.
   An identification window appears, in which you must provide a valid login and password for the remote device.
3. Provide a valid login and password for the remote device.
4. Click **Edit > Remote Control** .
   The **Connection Status** appears. After the connection is correctly established, the screen of the target client displays in the right window pane.

You can now execute any required functions or manipulation on the target computer or take over the mouse cursor to help the local user.

Note:

If you have the remote device in your view, you will see, that the CM icon in the systray, which normally is blue and oscillates green when the agent is busy, has turned yellow , to indicate that the client was taken over via remote control.

Note:

To display the list of all devices that you are currently remotely controlling and to switch from one to another, click the button at the bottom left. The **The list of active remote control connections allows you to switch between connections by double-clicking.** window appears, listing all currently open remote control sessions. Double-click an entry to switch to the session. Click **Close** to close the window.

Switching between remote control sessions

It is possible to have more than one remote control session established. To switch between these sessions, proceed as follows:

1. Click **Active Remote Connections** in the bottom left hand corner of the status bar.
   The **List of Active Remote Connections** window appears. It displays the list of all currently established remote control connections.
2. Double-click the desired connection.
   The focus of the console window will move to the selected remote control connection.

Note:

The window will not close upon selection, it will remain open next to your console window until you actively close it by clicking **Close.**

Launching a new task

It is possible to remotely launch a new process. To do so, proceed as follows:

1. Select **Edit > New Task (Run...)** .
   The **Run Process** window opens on the screen.
2. In the `Program Path` field enter the complete path on the remote client to be launched.
3. In the `Program Attributes` field enter any possibly necessary attributes with which the process is to be started.
4. Click **OK** to confirm the new process and close the window.

Transferring files between devices via remote control

You can also retrieve the test.txt file from the remote device and save it on your local device.

1. Select **File Transfer** .
   The **File Transfer** window opens on the screen. This window allows you to copy files from the local to the remove device and vice versa.
2. Find the source file, that is, the test.txt file to be copied in the tree hierarchy of the remote device and select it.
3. Select the target directory, that is, *c:/temp* on your local device.
4. Click the arrow between the two boxes to start the transfer.

> The transfer can be stopped and thus the file copy being cancelled by clicking **Cancel the current transfer** .

5. Select **Close** at the bottom of the window when all required files were transferred.
6. You can delete the test.txt file on the remote device in the same way as you would do on your local device.

Disconnecting from a remote control session

To end a remote control connection with a remote client, proceed as follows:

1. Click **Disconnect** .
   A confirmation windowdisplays.
2. Click **Yes** to continue.

The connection will be interrupted and the image of the remote screen appears from your right window pane.

> **Note:**
>
> If you leave the **Remote Control** node for another node in the console, a confirmation window pops up on the screen. Through this window you can either disconnect the remote control session or specify to keep it running.

Maximizing the remote screen

The size of the remote screen displayed on your local computer can be toggled between normal screen and maximized. Normal screen indicating only the right window pane of the console window and maximized being the right and left pane. To toggle the screen, proceed as follows:

1. Establish a connection with the remote client as previously explained.
2. Click **Edit > Maximize** .

The screen display will toggle to the respective other display size within your console window.

Copying and pasting in a Remote Control session

It is possible to exchange data between the remotely controlled client and the host controlling it. This copy and paste function works in the same way as the regular Windows function. This function works in both directions from the controlling to the controlled device and vice versa. To do so, proceed as follows:

1. Start the file Explorer on the remote device
2. Open a text editor and create a new file. Save it under c:/temp as test.txt.
3. Open Notepad, for example, type some text, select it and then copy it to your local clipboard using CTRL + C keyboard shortcut.
4. In the Remote Control console window open the test.txt file on the remote device.
5. Now place the cursor at the end of the test.txt file and use the CTRL + V keyboard shortcut to copy the content to the file.
6. Save it.

The contents of the source clipboard are copied to the target device.

Sending an CTRL+ALT+DEL command

Be aware, that depending on the operating system of the remote client sending an CTRL+ALT+DEL does not have the same result. On Windows XP the Task Manager displays, on Windows NT the security window appears, and so on. To send this command, proceed as follows:

1. Establish a connection with the remote client as previously explained.
2. Click **Edit > Send CTRL+ALT+DEL** .

Modifying the active remote control properties

It is also possible to modify some remote control connection parameters during an active connection. To do so, proceed as follows:

1. Select **Properties** .
   The properties **Properties** window appears.
2. Make the required modifications in the available parameters.
3. Click **OK** to confirm the modifications and to close the window.

Remotely controlling a device through a web browser

In addition to the classic remote control feature through the BCM console, 12.6 release enables administrators to remote control devices through a web browser. This browser-based technology to remote control devices does not require you to run the BCM java console on the device.

This BMC Client Management video (5 mins 37 secs) describes how to remotely control devices through a web browser.

This topic covers the following topics:

Browser and OS compatibility

Browsers:

- Firefox latest version
- Chrome latest version
- Microsoft Edge latest version
- Internet Explorer 11
- Safari latest version

OS:

Only devices running on these OSes and installed with a BMC Client Management agent can be remote controlled.

- Microsoft Windows
- macOS

Why choose browser-based remote control over the classic BCM console view

- No need to install the BCM java console on your device
- Remote control in full screen
- Easily open and manage several remote control sessions in a single browser at the same time

Before you begin

- You must have access to a BCM java console

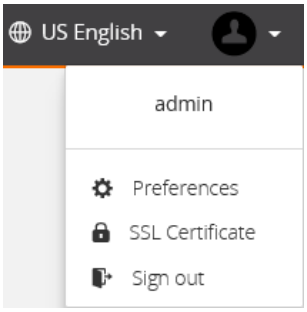
- URL to access BCM server. Contact a BCM administrator.
- Enable capability for remote access
- Request credentials for remote access

Enable capability for remote access

1. On the BCM console, click **Global Settings** > **Administrators**.
2. Click and ***administrator*** (must not be admin), and click **Security Profile**.
3. In the **Capabilities** tab, ensure that the **Remote Control** capabilities are enabled.

Installing an SSL certificate

An SSL certificate installed on the controlling device improves the performance of operations when you use the browser-based console. You should install the certificate authority on your system.



To install SSL certificates:

- Windows devices: Remote devices can be controlled even without an SSL certificate installed on the device.
- macOS devices: Remote devices cannot be controlled without an SSL certificate installed on the device.

For more information, see Certificate installation on systems.

Choosing the user interface locale

To change the locale:

1. In the browser window, enter the URL of the web console, https://*<IPAddressMaster>*:<MasterHttpPort>/webconsole.
2. At the top of the web page, under **Change Language**, select the locale in which you want to interact with the user interface and view instructions.

> ⚠ US English is the default language. The browser cache saves the language preference for future sessions.

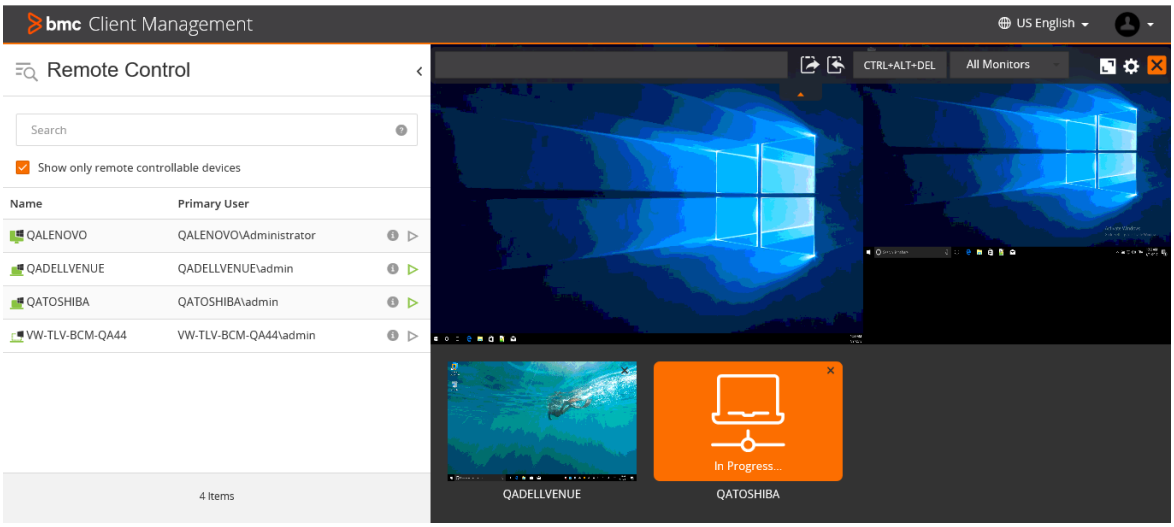
Establishing a remote control session

Only online devices that are running Windows or macOS and running a BCM agent can be remote controlled.

1. In the browser window, enter the URL, **https://*<IPAddressMaster>*:**<MasterHttpPort>**/webconsole**.
   Where *<IPAddressMaster>* is the IP address of the master server or the hostname of the server.
   If you face issues connecting to the master server, check your network connection. If issues persist, contact the BCM administrator.
2. Enter the admin credential.
3. If you are searching for specific devices, try one of the following:
   a. Enter ***** to get a list of all the available devices.
   b. Search using the following attributes: device name, user name, or OS name or a combination of these attributes.
   c. Search using a boolean combination of the above attributes.
   For example, the search phrase ***admin and windows*** return a list of devices with user name *admin* that are running *Windows* OS.
   d. Search a specific field expression. For example, ***name::admin***.
4. To start a remote control session, either double-click a device or Click ▷ next to a device. It is possible to remote control multiple devices at a time.
5. To switch between multiple remote control sessions, click a device thumbnail to switch to that remote control session.

To know more about the search syntax, hover the computer pointing device over the icon in the ? search box.

If you refresh the browser (F5), a dialog gives you the option to leave the page, which means that all open remote control sessions are lost or the option to stay on the page.



To hide the left page that displays device information, on the left pane, click 

To know more about the OS, IP address, and MAC address of a device, hover over the  icon.

Recognize device icons:

 Online physical devices

 Online virtual devices

 Offline physical devices

 Offline virtual devices

Configuring settings

Set preferences for remote control sessions - color depth, lock mouse and keyboard and so on. Preferences can be set at an administrator-level or for individual remote sessions.

- Defining pagination limits on the browser-based console
- Configuring administrator-level settings
- Customizing connection settings for an individual remote control session

Defining pagination limits on the browser-based console

Define the number of remote devices that can be displayed on a single electronic page.

1. On the BCM java console, at the top right corner, click **Preferences**.

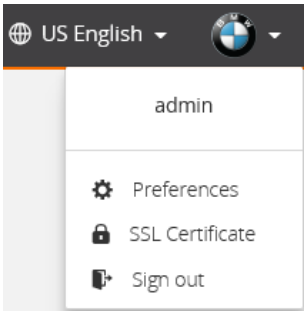
2. On the **Preferences** window, click **Tables**.
3. Under **Paging Settings**, in the **Table Rows per Page**, enter a value that represents the number of rows displayed on a single page.

The search results for devices extend to multiple pages depending upon the value set in **Table Rows per Page** field. For example, if you set the **Table Rows per Page** value to 50 and search results fetch 60 devices, 10 devices are displayed on the second page.

Configuring administrator-level settings

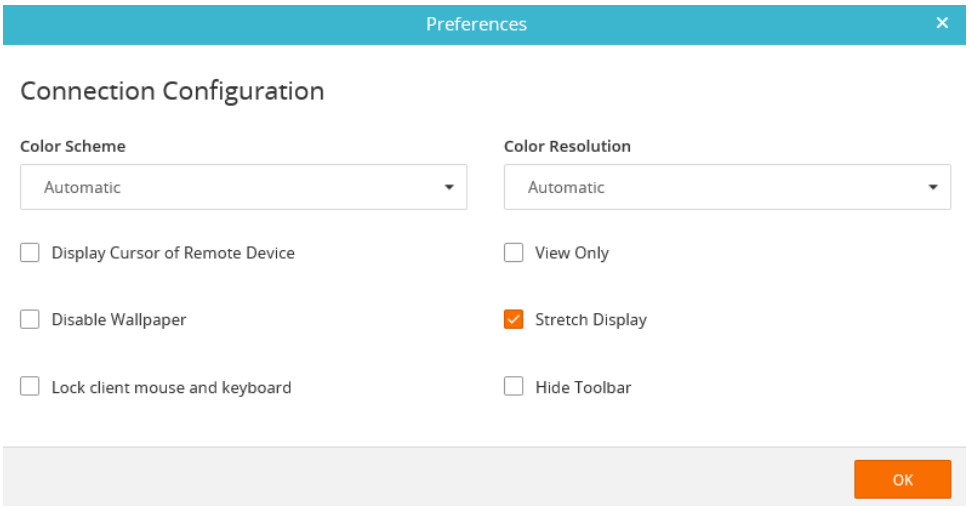
To configure connection settings at an administrator-level, for all the remote control sessions, follow these steps:

1. On the remote control browser, top right corner, click the administrator profile > **Preferences**



2. On the **Preferences** window, set the connection settings.

Preferences	Description
Color Scheme	Select the color scheme: Monochrome, Color, or Automatic.
Color Resolution	Select the depth of the color or the bit depth.
Display Cursor of Remote Device	Enable this option if you want to view the cursor of the remote device.
View Only	Enable this option to disable any action on the remote device.
Disable Wallpaper	Enable this option to disable the remote device's wallpaper. This option is not available if the View Only mode is enabled.
Stretch Display	Stretches the remote screen to the host screen.
Lock client mouse and keyboard	Disables the remote device's mouse and keyboard. This option is not available if the View Only mode is enabled.
Hide Toolbar	Enable this option if the toolbar should not be viewable on the host screen.



3. Click **OK**.

Customizing connection settings for an individual remote control session

As an administrator, you can customize connection settings for each remote control session.

1. After you start a remote control session, click **Configure the connection**.
2. On the **Connection Configuration** window, set the following settings.

Setting	Description
Color Scheme	Select the color scheme: Monochrome, Color, or Automatic
Color Resolution	Select the depth
Display Cursor of Remote Device	Enable this option if you want to view the cursor of the remote device
View Only	Enable this option to disable any action on the remote device
Disable Wallpaper	Enable this option to disable the remote device's wallpaper
Stretch Display	Stretches the remote screen to the host screen
Lock client mouse and keyboard	Disables the remote device's mouse and keyboard

3. Click **OK**.

Extending the remote-controlled device to multiple monitors

> The **All Monitors** setting is only seen on the toolbar when there are multiple monitors available for selection. Otherwise, the setting is not visible on the toolbar.

Somtimes, you might want to view all the monitors together on your device to perform some checks on the remotely controlled device. In other situations, you might just want to work on a single monitor connected to the remotely controlled device.

To view other monitors connected to the remotely controlled device:

- On the toolbar, in the **All Monitors** drop-down list, you can select a specific monitor or select **All Monitors**.
  For example, if there are 2 monitors, if you select the second monitor, only the second monitor is displayed on your device. If **All Monitors** is selected, all monitors connected to the remotely controlled devices are displayed on your screen at the same time.

Switching to a full-screen mode

After starting a remote control session, you can switch the remote control screen into full-screen mode.

You can switch to a full-screen mode in one the following ways:

- Double click the device thumbnail that appears when you start a remote control session.
- Click 

To view in default view, press the Esc key or click 

Sending information to a remote controlled device

After starting a remote control session, an administrator might want to copy information from a host device to a remote controlled device.

> Only text can be sent to or requested from a remote controlled device.
>
> Files cannot be transferred to or from a remote controlled device.

To send information to the remote controlled device:

1. Start a remote control session.
2. In the **Preferences** menu, if the **Hide Toolbar settings** is enabled, click  to view the toolbar.
3. Copy information to the clipboard of the host device.
4. In the remote controlled device, place the cursor in the text box and enter **Control + V**.
5. Click **Send** 
   This action copies that information into the clipboard of the remote device.
6. On the remote controlled device, open a text editor or a similar application and enter **Control + V** to paste that information.

Requesting information from a remote controlled device

An administrator might want to request information from a remote controlled device to a host device. Information requested could be log data to troubleshoot issues or configuration information or some other information from the remote controlled devices.

To request information from the remote controlled device:

1. Start a remote control session.
2. In the **Preferences** menu, if the **Hide Toolbar settings** is enabled, click  to view the toolbar.
3. Copy information to the clipboard of the remote device.
4. In the remote controlled device, place the cursor in the text box and click **Request** 
5. This action copies that information from the remote device into the clipboard of the host device.
6. Copy the information available in the text box then paste it in a text editor.

Feature comparison between Browser-based remote control and BCM Java console

You can compare the functionality provided by both the Browser-based console and the classic Java console. You can choose between one of these modes based on the features you want to leverage while remote controlling devices.

Feature	Browser-based remote control	Classic java console
File Transfer	✗	✓
Sending and requesting information	✓	✓
Unicode key mapping	✓	✓
Hardware key mapping	✗	✓
Run a new process	✗	✓
Reboot the remote device	✗	✓
Full-Screen mode	✓	✗
Stretch Mode	✓	✗
Multiple monitors	✓	✓
View-Only mode	✓	✓

Logging in to the BCM browser-based console using Remedy SSO credentials

If Remedy SSO server is enabled and integrated with BCM, the Remedy administrator can log into the BCM browser-based console using Remedy credentials.

For more information see,

- Managing Remedy SSO parameters
- Integrating with BMC Remedy Single Sign-On

Related topics

Remotely controlling a device through the BCM Java Console

Directly accessing a device

Directly accessing a device

In some situations, administrators find it convenient to work on a single device at a time. Moreover, some features (for example, remote file explorer) require a large amount of data that does not need to be stored in the database. It is therefore necessary to have key emergency features available from the console that do not use scheduling or cascading.

Remote Manager is a real-time configuration tool that provides the administrator with direct read and write access to the directories and files and the registry and services of a remote computer via the **Direct Access** node of the console.

To be able to establish a connection you might be required to have the login information of the managed device, that is, the login name and its corresponding password, as well as the agent access rights, which are defined through the agent's user interface. This setting is defined via the **System Variables**.

Be aware, that you can only access devices with NAT configurations via this functionality if the agent tunneling is activated.

The following tools are available for direct access on a device:

- File System:
  The File System function is very similar to Windows Explorer as it allows you not only to view a device's complete directory structure with its files but also to manipulate them, that is, to copy, move, rename and delete directories as well as files. It also allows you to edit individual text files within the privacy restrictions set up by the user/administrator of the managed device.
- Registry:
  The Registry function allows you to directly access the Microsoft Registry and make changes there. You can add, modify or delete keys here as well all connected values.

- Services:
  Through the Services function you can start or stop services on remote Windows devices and configure startup options. You cannot stop or restart the CM agent from here.
- Process Management:
  The Process Management allows you to access information about programs and processes running on the remote managed devices, thus providing you with the possibility to monitor key indicators of your computer's performance. You can quickly see the status of the programs that are running and end programs that have stopped responding. Here you can start and end processes and configure preferences for this view.
- Windows Events:
  Via the Windows Events you can view and follow all events logged by the system on Windows devices.
- File Transfer:
  This function allows you to transfer files between the local and the remote device, it is the same one used by Remote Control.
- Check Connection:
  This function checks if the device is contactable.
- Reboot:
  This function allows you to remotely reboot the device.
- Shut down:
  Allows to remotely shut down the device.
- Wake up:
  This function wakes the remote device up, either from a sleep/hibernation state or from being shut down.

The following paragraphs lead you through your first steps when directly accessing devices in your network.

You can directly access a remote device from the **Search** , **Device Groups** and **Device Topology** location.

- Transferring files between devices via direct access
- Checking connection
- Rebooting a remote device
- Shutting down a remote device
- Waking up a device
- Managing File System
- Managing Registry
- Managing Services
- Managing processes
- Managing Windows events

Transferring files between devices via direct access

You can also retrieve the test.txt file from the remote device and save it on your local device.

1. Select **File Transfer** .
   The **File Transfer** window opens on the screen. This window allows you to copy files from the local to the remove device and vice versa.
2. Find the source file, that is, the test.txt file to be copied in the tree hierarchy of the remote device and select it.
3. Select the target directory, that is, *c:/temp* on your local device.
4. Click the arrow between the two boxes to start the transfer.

> The transfer can be stopped and thus the file copy being cancelled by clicking **Cancel the current transfer** .

5. Select **Close** at the bottom of the window when all required files were transferred.
6. You can delete the test.txt file on the remote device in the same way as you would do on your local device.

Checking connection

This option allows you to verify the connection of the remote device, that is, to see if it is contactable.

1. Select the device.
2. Right-click the mouse button and select the **Check Connection** option from the **Direct Access Tools** pop-up menu.
   A ping is directly sent to the remote device.

The result of the connection verification displays in an Information window.

Rebooting a remote device

1. You can reboot the remote device by clicking **Reboot** .
2. Click **Yes** in the confirmation window to confirm the reboot.

The remote device is now rebooted.

> **Note:**
>
> The console may appear locked, as its left window pane is minimized, however, this is not the case. If you click the **Maximize** button, the left window pane with the tree reappears and you can continue working normally, including remotely controlling other devices.

Shutting down a remote device

The direct access tools also provide you the possibility to completely shut down the selected remote device. To do so, proceed as follows:

1. Select the device.
2. Right-click the mouse button and select the **Shut down** option from the **Direct Access Tools** pop-up menu.
   A confirmation windowdisplays.
3. Click **Yes** to proceed with the shutdown, but be aware that if there is a user working on the remote device he has no way of stopping the shutdown and might loose data in this case.

Then the shutdown order is sent and the remote device is shut down.

Waking up a device

The direct access tools also provide you the possibility to wake up the selected remote device. To do so, proceed as follows:

1. Select the device.
2. Right-click the mouse button and select the **Reboot** option from the **Direct Access Tools** pop-up menu.
   A confirmation window appears.
3. Click **Yes** to proceed with the wake up.

The wake up order is sent immediately to the remote device and executed.

Managing File System

The **File System** node is very similar to Windows Explorer as it allows you not only to view a device's complete directory structure with its files but also to manipulate them, that is, to copy, move, rename and delete directories and files. It also allows you to edit individual text files within the privacy restrictions set up by the user/administrator of the managed device.

It displays the following information about all the directories and files:

Parameter	Description
File Name	The fields in this column list all subdirectories and files contained in the directory or disk.
Size	These fields display the size of the respective file.
Access	This column displays the access rights for the related file or directory. Accesses can be **Read-only**, **Read, Write** , neither or both.
Last Modification Time	This field shows the date and time of the last modification of the respective directory or file, in the default format defined in the user preferences.

The following topics provide information about managing file system:

Adding as managed application

Applications can be managed in via the **Application Monitoring** node. This means, software applications can be monitored when they are used and how often, they can be prohibited from starting and they may be protected, that is, they will heal themselves if they become corrupted in any way. You can add a software directly from this view to the list of managed applications. Only applications of type **Application** or **Browser**, which contain all required information to be managed, can be added. If an application listed in the software inventory does not provide all necessary information, or its type is **MSI** or **Add/Remove Programs**, this option will not be available. To add an application for managing proceed as follows:

1. In the list of applications select the application(s) to be added to the list of managed applications.
2. Select **Edit> Add as Managed Application**  .
   A confirmation window appears.
3. In this window you can define the folder into which the application is to be added. By default it is added directly under the main application list node. To add it to another folder click the icon to the right (...). The **Select Folder** window appears displaying the folder hierarchy. If the desired target folder does not yet exist you can also create new folders. To do so first select the parent folder of the new one and then select click **New Folder** below the hierarchy. The **Properties** dialog box appears. Enter the desired data into the respective text boxes and then click **OK** at the bottom of the window to confirm the new application list folder. Select the target folder and click **OK** to confirm and to close the window.
4. An Information window will now appear in which you can also directly add the selected application to an existing application list. Click **Yes** to do so, **No** to only add the application to the application catalog.
5. If you selected **Yes**, the **Assign an Application List** dialog box appears providing the list of existing application lists.
6. Select the desired application list from one of the lists available in the window.
7. Click **OK** at the bottom of the window to confirm.
8. If the application list is already assigned to a device or group, a Confirmation dialog box appears, in which you can define to directly reactivate the application list for its assigned objects.

Creating directory

You can add directories to the file structure of the managed remote device. To do so, proceed as follows:

1. Select the directory under which the new directory is to be placed.

2. Click **Edit> Create Directory** .
   The **Create a New Directory** pop-up dialog box opens.
3. Enter a name for the new directory then click **OK** to confirm your addition, otherwise click **Cancel**.

Running a file

You can directly execute a program on the remote device. To do so, proceed as follows:

1. Select the executable file to be run in the right window pane.
2. Click **Edit> Run** .
   The **Execution Parameters** pop-up dialog box opens.
3. Either enter the parameters with which the program is to be executed in the **Command Line Parameters** box or, if it does not need any, leave the text box blank
4. Click **OK** to confirm the execution.

Editing a file

Text files with a size smaller than 200KB may be directly edited in the console. To do so, proceed as follows:

1. In the table in the right window pane select the text file to be edited.
2. Select **Edit> Edit File** .
   An **Edit Text File** window opens on the screen with the contents of the file.
3. Make all necessary changes to the file.
4. Click **OK** at the bottom of the window to confirm the modifications and to close the window.

Transferring files between the devices

You can also retrieve the test.txt file from the remote device and save it on your local device.

1. Select **File Transfer** .
   The **File Transfer** window opens on the screen. This window allows you to copy files from the local to the remove device and vice versa.
2. Find the source file, that is, the test.txt file to be copied in the tree hierarchy of the remote device and select it.
3. Select the target directory, that is, *c:/temp* on your local device.
4. Click the arrow between the two boxes to start the transfer.

> The transfer can be stopped and thus the file copy being cancelled by clicking **Cancel the current transfer** .

5. Select **Close** at the bottom of the window when all required files were transferred.
6. You can delete the test.txt file on the remote device in the same way as you would do on your local device.

Managing Registry

The Microsoft Windows operating systems make use of a set of system configuration files referred to as the registry. The registry is a database repository for information about a computer's configuration. It also provides information to the operating systems which during operation continually references the registry for data on profiles for the users, for example, or the programs installed on the computer and the types of documents each can create, property settings for folders and program icons, and what hardware exists on the system and which ports are used.

The registry is organized hierarchically as a tree and is made up of keys and their subkeys and value entries for each.

The right window pane of a registry key displays the following information about the registry values of the currently selected key:

Parameter	Description
Name	The name of the registry value.
Type	The type of the registry value, possible values are String, Binary or DWord.
Data	The actual data of the registry value.

The right window pane only lists the registry values of the keys, the subkeys of the selected key are only listed in the left window pane.

The **Registry** node on the console allows you to execute modifications on keys and values. Take great care when using this tool. If you are not very familiar with the Registry, you can make changes which will prevent the managed device from rebooting!

This section includes following topics:

Creating key

The **Registry** node on the console allows you to create new keys (or subkeys) to be added to one of the Registry key folders. To create a new key, do the following:

1. Select the Registry key folder under which the new key is to be placed.
2. Click **Edit> Create Key** .
   The **Create New Key** pop-up dialog box opens.
3. Enter a name for the new key.
4. Click **OK** to confirm.

Creating value

The **Registry** node on the console allows you to create new values for an existing key in the Registry. Three different types of values can be created:

- String Value
- Binary Value

- DWORD Value

> **Note:**
>
> Take great care when using this tool. If you are not very familiar with the Registry, you can make changes which will prevent the managed device from rebooting!

To create a new value do the following:

1. Select the key for which the new value is to be created.
2. To create the value either click

Edit > Create String Value

Edit > Create Binary Value ,

Edit > Create DWORD Value
The new value will automatically be created under the key and displayed in the table of the right window pane.

1. To name the newly created value, click **Edit > Properties** .
   The **Properties** dialog box appears.
2. Enter the required data.
3. Click **OK** to confirm.

Managing Services

Through the **Services** node you can start or stop services on remote Windows devices and configure startup options. Be aware that you cannot stop or restart the CM agent from here.

The **Services** node contains the following columns in the right pane giving information for each service related to the accessed remote device:

Parameter	Description
Name	The internal name of the particular service, for example, App Mgmt.
Display Name	The long version of the service name, that is, a more explicit name. For the preceding example this would be Application Management. The content of this field can be edited through the **Properties** dialog box.
Description	This field provides a summarized description of the functionality of the service, such as Provides software installation services such as Assign, Publish, and Remove. The content of this field can be edited through the **Properties** dialog box.
Status	The current status of the selected service. Two possible status are available: **Started** and **Stopped** .
Startup Type	The startup type of the selected service. Three startup types exist: **Manual** , **Automatic** and **Disabled** . The content of this field can be edited through the **Properties** dialog box by selecting the desired value from the drop-down box.
	The **Binary Path** field displays the full installation path for the executable file of the service.

Parameter	Description
Binary Path	
Log On As	The account the service uses to log on. Accounts are either LocalSystem, **Administrator** or a Selected User.

Following operations can be performed on the **Services** node:

- Starting a service
- Restarting a service
- Stopping a service
- Modifying service parameters

Starting a service

To start a currently stopped service on the remote device, proceed as follows:

1. Select the service to start in the table in the right window pane.
2. Select **Edit > Start** .

The service will be started directly.

Restarting a service

To restart running service on the remote device, proceed as follows:

1. Select the service to stop in the table in the right window pane.
2. Click **Edit > Restart** .

The service will be restarted immediately.

Stopping a service

To stop a currently running service on the remote device, proceed as follows:

1. Select the service to stop in the table in the right window pane.
2. Click **Edit > Stop** .

The service will be stopped immediately.

Modifying service parameters

To display all properties of a service and modify values, proceed as follows:

1. Click **Edit > Properties** .
   The **Properties** dialog box appears.
2. In this window the display name of the service, its description and the startup type can be modified.
3. To confirm the modification click **OK** at the bottom of the dialog box.

Managing processes

The **Process Management** node displays information about programs and processes running on the remote managed devices, thus providing you with the possibility to monitor key indicators of your computer's performance. You can quickly see the status of the programs that are running and end programs that have stopped responding. You can also assess the activity of running processes using as many as 15 parameters, and see data on CPU and memory usage.

The **Process Management** node provides the following information about the currently running local processes:

Parameter	Description
Name	The name of the executable file of the process.
PID	The Process Identifier is a numerical identifier that uniquely distinguishes a process while it runs.
Owner	The name of the owner of the process
CPU	The percentage of time that a process used the CPU since the last update.
CPU Time	The total processor time in seconds used by a process since it was started.
Memory Usage	The current working set of a process in KB. The current working set is the number of pages currently resident in the memory.
Virtual Memory	The amount of virtual memory or address space committed to a process. Not applicable for Linux RH9.
Threads	The number of threads running in a process. Not applicable for Linux RH9.
Parent Process	Displays the PID of the parent process if the currently selected process is a child. The field is empty if it is not a child process.
Path	The full path to the executable file of the process.

Managing Windows events

Windows NT and later versions provide you the possibility to record information about their activity in a log file. When an event is logged, the event and its message are appended to the Windows Application Event Log file, the date, time, user, and other identifying information. These events can be viewed with the Windows Event Viewer and also in the CM console through this node.

Using the event logs, you can gather information about hardware, software, and system issues and monitor Windows security events.

Windows records at least three kinds of events which are accessible through their subnodes such as:

- Application
- Security
- System

Depending on the operating systems and the installed software you can find more event logs here for IE 7, Microsoft Office, and so on.

The section includes following topics:

- Application log
- Security log
- System log

Application log

The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The developer decides which events to record.

Parameter	Description
Type	The fields in this column display the type of the event, which can be one of the following: **Error** A significant issue, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged. **Warning** An event that is not necessarily significant, but might indicate a possible future issue. For example, when disk space is low, a warning will be logged. **Information** An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
Date	The date and time the event occurred in the default time format.
Source	This field displays the application that caused the event, this can either be the system or a system component, for example, SNMP or EventLog, or any type of application such as an antivirus or a word processing program.
Category Name	This entry defines the severity level of the individual event. This information in the form of a number is mainly used in the security events.
Event	Displays the ID number of the respective event.
User	Displays the name of the user that caused the event, for example, SYSTEM, if the event was caused by the system or one of its components, the login name of the user which was logged on, or N/A if no information is available on the user.

Security log

The security log can record security events such as valid and invalid login attempts, and events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled login auditing, attempts to log on to the system are recorded in the security log.

Parameter	Description
Type	The fields in this column display the type of the event, which can be one of the following: **Audit Success** An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event. **Audit Failure** An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
Date	The date and time the event occurred in the default time format.
Source	

Parameter	Description
	This field displays the origin of the event, this can either be the system or a system component, for example, SNMP or EventLog, or any type of application such as an antivirus or a word processing program.
Category Name	This entry defines the severity level of the individual event. This information in the form of a number is mainly used in the security events.
Event	Displays the ID number of the respective event.
User	Displays the name of the user that caused the event, for example, SYSTEM, if the event was caused by the system or one of its components, the login name of the user which was logged on, or N/A if no information is available on the user.

System log

The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined.

Parameter	Description
Type	The fields in this column display the type of the event, which can be one of the following: **Error** A significant issue, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged. **Warning** An event that is not necessarily significant, but might indicate a possible future issue. For example, when disk space is low, a warning will be logged. **Information** An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
Date	The date and time the event occurred in the default time format.
Source	This field displays the application that caused the event, this can either be the system or a system component, for example, SNMP or EventLog, or any type of application such as an antivirus or a word processing program.
Category Name	This entry defines the severity level of the individual event. This information in the form of a number is mainly used in the security events.
Event	Displays the ID number of the respective event.
User	Displays the name of the user that caused the event, for example, SYSTEM, if the event was caused by the system or one of its components, the login name of the user which was logged on, or N/A if no information is available on the user.

Certificate installation on systems

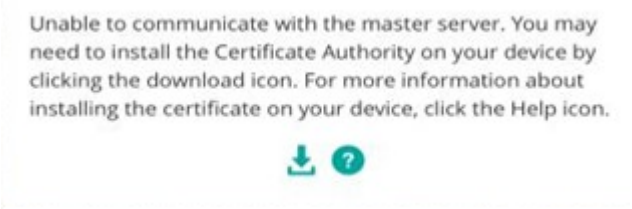
When you try to access a BCM server from a system running macOS, or Windows, it is recommended that a BCM issued certificate is installed on the system. A BCM certificate ensures that system performance is enhanced.

- Certificate installation on macOS systems
- Certificate installation on Windows systems

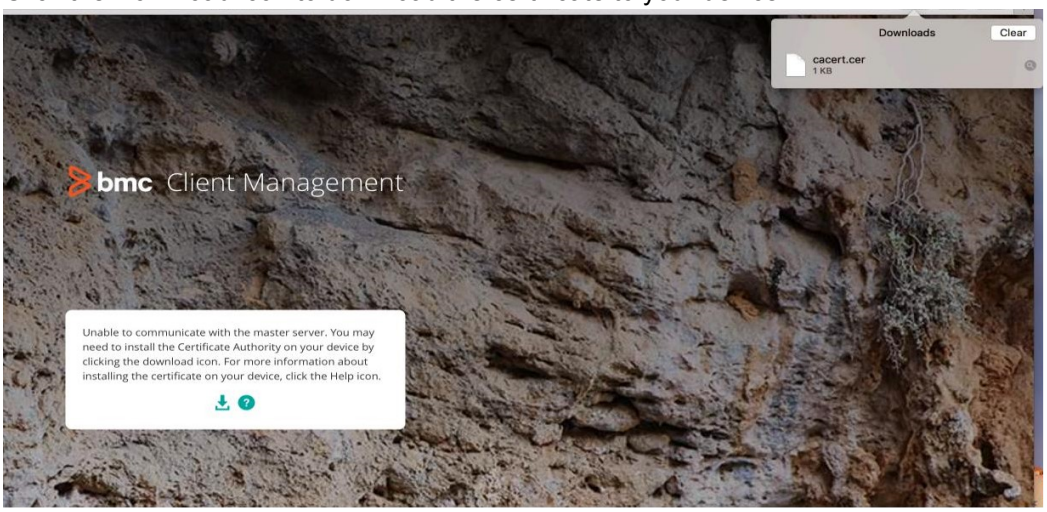
Certificate installation on macOS systems

When you try to access a BCM server from the Safari browser, the Safari browser tries to establish a secure connection with the BCM server. If it does not a certificate from the BCM server, Safari browser blocks access to the server. You need to install a valid certificate from the BCM server.

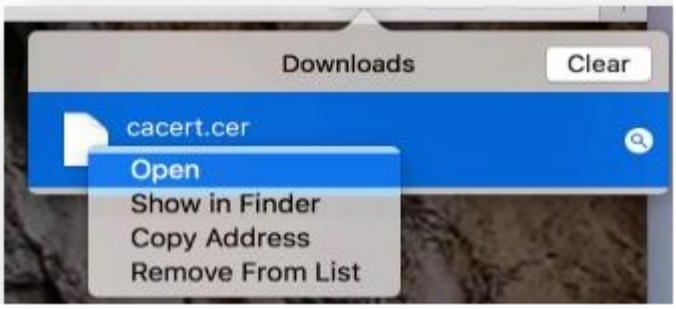
1. When you access the BCM server from a Safari browser, you might see the following message if a trusted certificate is not installed on your device.



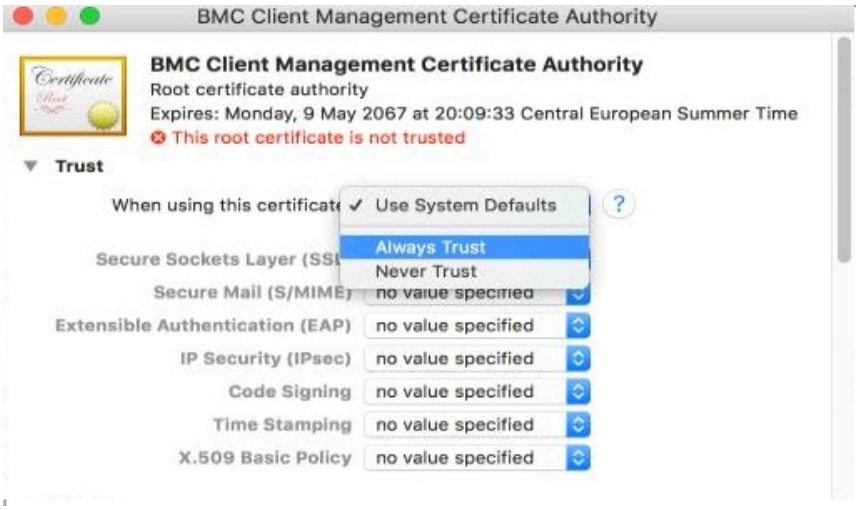
2. Click the Download icon to download the certificate to your device.



3. Right-click the certificate and open it.



4. The **Keychain Access** window manages the certificates on the system. The list displays the BCM Certificate but it needs to be trusted.
5. Right-click **BMC Client Management Certificate Authority** > **Get Info**.
6. In the Certificate information window, for the **When using this certificate** setting, select **Always Trust**. After the certificate is trusted, it is marked as trusted for this account.



7. Refresh the login page and re-login to the browser-based console with your credentials.

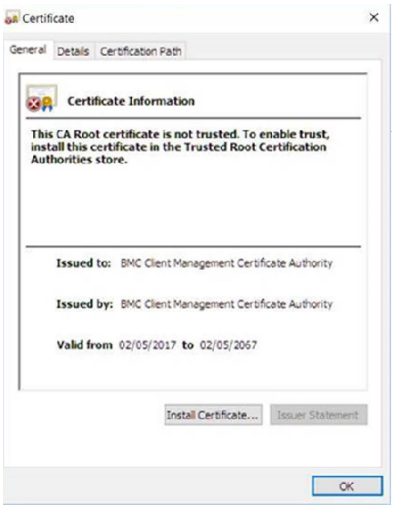
Certificate installation on Windows systems

On Windows systems, ensure that BCM certificate is installed and trusted for secure communication between the BCM server and the system.

- Installing the certificate on the system
- Installing the certificates from a browser

Installing the certificate on the system

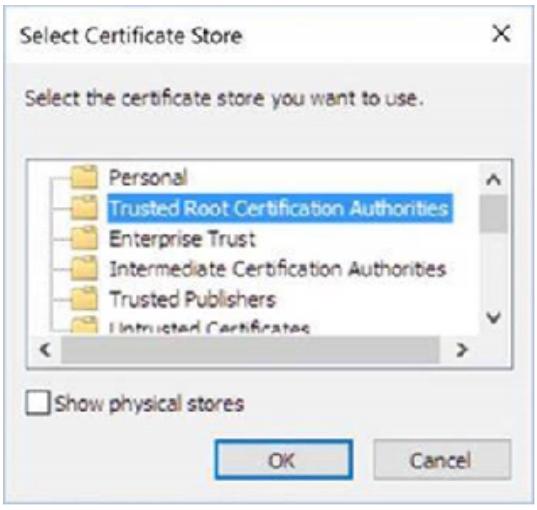
1. On a Windows system, click **Download Certificate**.
2. Click **Install Certificate**.



3. Import the certificate to the local system.

;

4. Click **Next**.
5. On the **Certificate Import Wizard** window, select **Place all certificates in the following store** to specify a location for the certificate.
6. Click **Browse** to select the **Trusted Root Certificate Authorities**.



7. After you install the certificates to your local system, you must restart the browser to load the certificate.

Installing the certificates from a browser

You can directly download the certificate from a browser.

1. On the browser, click **Settings > Manage Certificates**.
2. On the **Trusted Root Certification Authorities** tab, click **Import**.
3. After installation, click **Close**.

Managing Power Management

Organizations looking to implement effective PC infrastructure power savings programs face three hurdles: the limits of voluntary power savings; the difficulty of applying power management policies across distributed infrastructures; and reconciling potential conflicts between power savings and other system management activities.

The BMC Client Management - Power Management uses powerful agent technology to implement power management on client systems. Customers can easily add power management to other services delivered via the CM agent and consolidate policies with their overall system management programs. At a financial level, IT energy costs can thus be cut by US$ 25 to US$ 80 per computer and per year by implementing effective power saving features.

The four steps of power management

BMC Client Management - Power Management is based on the following concepts:

- Each agent can monitor and log system state
- The **Event Log Manager** uploads results to the database
- The console allows for direct access view on events, as well as consolidated results
- Reports show consolidated results as well as evolution

These allow for the following benefits:

- Adapt power management to Windows Vista (power settings inventory and power settings policies)
- Directly measure and report on power consumption, energy costs and C02 emissions

The power management seamlessly integrates with the BMC Client Management baseline features and creates flexible policies that apply to individual user work styles and organizational needs:

- Power management inventory
  The inventory consolidates the current power management settings of each device and provides hardware inventory with power-oriented classification.
- Power management configuration and application
  The power management configuration enforces power management policies with various levels of settings. It controls settings that reduce power to individual components, for example, turning off monitors and hard drives, after a defined unused time period. It also schedules and activates standby/sleep and hibernation modes for whole groups of devices and shuts down unused computers (that is, overnight) as well as schedules their automatic restart (that is, 5 min before the next expected usage).

- End-user awareness
  The power management functionality allows the administrator to schedule and broadcast "green" messages, reminders, etc. Administrators can also measure and publish effective usage time against overall power on time.

Power management components

The power management functionality is composed of the following components on which you can see detailed information in the following topics:

- **Inventory**
  The power management inventory is available for both single devices as well as device groups, and provides three different aspects of power management:
  - It displays detailed information about the system power management hardware resources and capabilities of the remote device,
  - it shows details on the global power management policies, and
  - it provides detailed information about the power schemes/plans that exist on the individual devices.
- **Configuration**
  The power management configuration configures the inventory update and the event logging of the module.
- **Operational Rule Steps**
  The available operational rule steps allow to configure the module as well as the power settings of the managed devices.
- **Reports**
  The functionality provides reports, predefined and delivered with the software as well as the possibility to create further custom reports on all possible aspects of power management.

Related topics

- Power management overview
- Generating the Power Management inventory
- Monitoring the Power Management events
- Power Management reporting
- Defining an upload schedule for Power Management
- Regularly generating (update) the inventory
- Regularly uploading events
- Creating or modifying power scheme
- Changing active power scheme
- Managing Power Management Inventory
- Viewing alerts and events
- Power management step reference

Power management overview

The following topics direct you through the four steps required to configure your system for Power Management, to generate and analyze a first power inventory, monitor its events and report on them.

> **Note:**
>
> The Power Management functionality is *not* applicable to Linux and Mac OS, it is only applicable to Windows, version 2003 and later.

Generating the Power Management inventory

Similar to the **Patch**, the **Power Management** must be generated specifically. This is done via an operational rule executed on your target devices. The first action to take is to create the operational rule, this time manually.

1. Select the **Operational Rules** top node in the left window pane.
2. Click **Edit> Create Operational Rule** .
   The **Properties** dialog box appears.
3. Enter *Power Management Inventory* into the **Name** field and then click **OK**.
   The new operational rule is added to the list of members in the right pane.
4. Double-click the operational rule.
5. Go to the **Steps** tab.
6. Click **Add Step** .
   The **Select a Step** pop-up menu appears.
7. Click the **Power Management** folder and select the **Update Power Management Inventory** step of this group.
8. Click **Add** to add the step to the list of **Selected Objects**.
   The **Properties** dialog box appears displaying the parameters to be defined.
9. Check the remaining options: **Upload after update** , **Force Upload** , **Bypass Transfer Window** .
10. Click **OK** to close the window.
11. Click **OK** to add the step to the operational rule and close the **Select a Step** pop-up menu.
    The operational rule is now created and must be assigned to the target devices, for our example here we will assign it to the group *All Devices* again.
12. Return to the *Power Management Inventory* rule click the **Assigned Objects** and then the **Assigned Group** node.
13. To assign the group select **Assign Device Group** .
    A confirmation window appears.
14. Click **Yes**, to activate the operational rule directly.
    The **Assign to Device Group** pop-up menu appears.

15. Select the *All Devices* group from the list.
16. Click **OK** to add it and close the window.
    If you answered **Yes** to *Would you like to automatically activate the selected items with the default schedule?* (see preceding point 3), the inventory process is started directly!

For more information see Analyzing the Power Management inventory.

Analyzing the Power Management inventory

After the rule has successfully executed, you can take a first look on the inventory on the first device.

1. Open node **All Devices > Your Device > Inventory > Power Management**.

   This node displays its information in three different subnodes.

2. We will for the moment only concern ourselves with the **Global Policies** node.

   This node displays the name of the currently activated power scheme and its parameter values.

   To learn how to change the active power scheme see Option (e).

   To learn how to create new power schemes or modify existing power schemes see Option (d).

Monitoring the Power Management events

Events can be monitored locally and centrally once the data is uploaded to the CM database, and they can be monitored individually for single device or for all the members of the group.

The section includes:

- Monitoring events locally
- Monitoring events on the master

Monitoring events locally

You can monitor what is happening about power management locally on each of the devices of your group. To cause some events to be generated you can for example modify your screen saver settings to a very short time of inactivity, for example, 1 minute. Wait until the screen saver comes on and then unlock your screen again as shown in the screen shot of this example. You can also configure the device to go into Standby modus after 1 minute, wait and then reactivate the device again.

1. Go to the **All Devices > Your Device > Agent Configuration > Module Configuration > Power Management** node.
2. Select the **Events** tab.
   It displays the list of events that occurred on the local device.
3. Refresh the page if it is still empty.
   The following information displays:

Event Date	The date and time at which the power management action, the activation of the screensaver, was executed.
Type	This field displays the type of event that occurred, that is, the screen saver was activated, the device was put in hibernation, and so on.

Monitoring events on the master

Up to now, the event data is only available locally on the agent. However, to be able to print reports on this topic and to view them in the console together with other data, these events must be specifically uploaded to the master and its database. This is done via an operational rule:

> **Note:**
>
> By default, these events are configured to be uploaded every 24 hours, that is, at midnight. If the agent is not running at this time, the events will be uploaded at agent startup.

1. Go to the **Operational Rules** top node in the left window pane.
2. Click **Create Operational Rule** .
   The **Properties** dialog box appears.
3. Enter *Upload Power Management Events* into the **Name** field and then click **OK**.
   The new operational rule is added to the list of members in the right pane. Double-click it.
4. To configure all the steps go to the **Steps** tab.
5. Click **Add Step** to add the first step.
   The **Select a Step** pop-up menu appears. It displays the list of available steps in its **Available Steps** box.
6. Double-click the **Event Log Manager** folder.

7. Select the step **Upload Events** and click **Add** .
   The **Properties** dialog box appears.
8. From the **Model Name** drop-down list select the **Power Management** value and leave all other boxes as they are.
9. Click **OK** to confirm the parameters and **OK** again to confirm the new step.
   The operational rule is now configured and must be assigned to the target, that is, all devices in our test environment.
10. Go to the **Assigned Objects > Assigned Group** node in the left window pane under your newly created operational rule.
11. Select **Assign Device Group** .
    A confirmation window appears. In this window, you can define if the device assignment will be activated according to the default schedule defined in the User Preferences.
12. Click **Yes** , to activate the operational rule automatically.
    The **Assign to Device Group** pop-up menu appears.
13. Select the group *All Devices* from the list.
    The group will be added to the table in the right pane with a status of `Activated`.
14. Select the subnode *All Devices* and follow the execution of the operational rule for the group members.

    > After its status is `Executed` all data are uploaded.

15. To verify this, go to the **Alerts and Events** node of the *All Devices* group.

    > This node displays the list of all events registered by the event log models for the selected device group.

16. In the right pane from the **Model Name** drop-down list, select **Power Management**.
17. In the right pane from the **Model Name** drop-down list, select **Power Management**. Click **Find** .
    The following table displays all events that were uploaded and are continued to be uploaded.

Now all data is uploaded and ready and reports can be generated.

Power Management reporting

The easiest and clearest way to monitor the power management activity is via reporting. The CM console provides a template-based report for this. However, contrary to other modules, there is only one template with a number of different options to display the different aspects of the topic.

- All reports that can be generated with this template according to its different units and groupings can either be shown as a summary for all devices or with the same details displayed for each device that is included in the report.
- The report details can be grouped by Status, **Weekly Hours**, Day, Month, Week or Year
- The units according to which the data can be displayed are Percentage, Hours, Energy, Price and CO2 Emission.
- The reports can be generated for a specific period of time.
- As usual all these reports can be generated and displayed in HTML, PDF and XML format.

The following section will provide some examples of these possibilities, mostly as a summary.

For our examples, we will only create one report which we will modify each time to see the different possibilities. However, you can also create a new report for each example, but this will not be explained specifically. Following topics provide more information about power management reporting:

- Power Management summary report
- Usage per device report
- Distribution by weekly hours report
- Energy costs by weekly hours report
- CO2 emissions by week report

Power Management summary report

We will generate this report via the wizard, which is available from everywhere in the console.

1. Select **WizardsReport Creation** .
   The **Report Creation Wizard** appears. The left pane of the wizard window appears all available steps of this wizard.

   > **Note:**
   >
   > Depending on the selections made in the right window panes, some of these steps will become available/unavailable.

2. Make the following choices in the first wizard window and leave all other values as they are:
   - Enter *Summary* as the name into the **Name** box.
   - Enter *Power Management Summary* as the name into the **Report Title** box.
   - In the **Report Type** box select **Template-based** from the list.
   - In the **Report Template** box select **Power Management Status** from the list.

     > **Note:**

Power management only provides one report which however provides you with several options.

3. Click **Next** to continue.
   The **Options** window appears.

> **Note:**
>
> In the **Options** window, the criteria for the report are defined, for example, if it is to be a summary, if it is generated for a specific period of time, for a specific group, and so on For our example we will first generate the basic report, a status summary.

4. Leave all values as they are and click **Next** to continue.
   The **Publication and Mail** window appears.

> **Note:**
>
> This step allows you to make the generated reports accessible to other associates within your department or company or to send it by mail to specific associates. For this example we will make this a public report and send it to our own e-mail account in PDF format.

5. Enter a name, that is, a title for the report into the **Name** box, for example, *Power Management Summary*.
6. Then check the **Public Report** box.
7. Go down to the second panel and select **Add email** .
   The **Define Mail** dialog box appears on the screen.

> **Note:**
>
> To specify the recipients as direct recipients, copy recipients and blind copy recipients, you proceed in the same way.

8. To enter recipients click **To** / **CC** / **BCC** and the **Select an Address** dialog box appears on the screen.

- To select an administrator or administrator group from the list select the **Select from List** radio button and then select the following recipient(s). You can specify an administrator group as the recipient, in this case the mail will be sent to all members of this group that have a valid e-mail address entered into their general data tab.
- Or you can select the **Select Manually** radio button and enter any valid e-mail address into the following text box. You can also enter more than one address by separating these with a semi-colon, for example, *scotty@enterprise.com; kirk@enterprise.com* .

9. Then enter *Power Management Summary Report* as the **Subject** of the mail.
10. Click **OK** to confirm the mail and add it to the list.
11. Click **Next** to go to the **Assigned Objects** wizard page.

> In this step of the wizard the objects on which the report is to be generated are to be defined. In our example we will assign it to our group *All Devices* for which we generated the power management events.

12. Select **Assign Device Group** .
    The **Assign to Device Group** pop-up menu appears.
13. Select the device group *All Devices* from the window.
14. Click **OK** to confirm the assignment and close the window.
    The device group will be added to the table of assigned device groups.
15. Click **Next** to go to the **Schedule** wizard page.

> The last step in the wizard is the definition of its generation schedule. Our first report we will generate immediately to be able to examine it right away.

16. Select the **Immediately** radio button in the **Execution Date** panel.
17. Then check the **Immediately generate the report** box at the bottom of the window.
18. Click **Finish** to confirm the new report and generate it.
    The **Confirmation** dialog box appears, which allows you to move the focus of the console to the newly created report.
19. Click **Yes** to do so.

For more information, see Analyzing the report.

Analyzing the report

After the report is created and generated it displays in a browser window. To display it, proceed as follows:

The focus of the console was moved to the main view of the newly created report.

1. In this window, select **Edit > View Last Result**  .
   The **Select a Group** pop-up menu appears.
2. Click **OK** to view the report for *All Devices* in HTML format.
3. If the **Confirmation** dialog box appears, click **Yes**.

The newly generated report displays in the window.

The first part of this summary, the introduction provides you with the following information, which will be the same for all different types of reports we will generate:

- A general description of the contents of this report.
- **Time Range** displays the time frame for which the report was generated. If you have not selected a time frame as we did, the dates indicated are the date of the first uploaded event as the start date and the date of the last uploaded event as the end date.
- **Group by** indicates the distribution of the charts, All in this case meaning that all devices are cumulated in one single graph.
- **Unit** indicates in this case that the values provided in the graph are in percent.
- **Number of devices** displays the total number of members of the group that is assigned to the report.
- **Number of devices used for reporting** displays the number of devices that uploaded events usable for this type of report. For the preceding shown example this indicates that only 2 out of the 8 group members show power management actions.

The second part of this report is the summary of all data displayed in the form of a pie chart with the following color explanations.

- The differently colored pie parts represent the different types of events generated.
- The percentage indicates the representation in percent of the respective event (= power state of the device).
- The displayed graph shows that on those two devices someone was working but only 2/3 of the time, for almost 1/3 of the time the screen saver was running, and they were shut down for only 5% of the time.
- It also shows that at all times someone was logged on to both devices.
- In this graph it is not possible to know the active/inactive time distribution between the two devices, for this a report needs to be generated that distinguishes between the devices.

Usage per device report

To display the same report with details on each of the devices of the device group in addition to the group summary, modify the report as follows:

1. Select the report in the left window pane.

> If you want to know more about the general options and possibilities of reports, refer to the Report section.

2. In the right pane select the **Options** tab.

   This tab displays the currently selected report options.

3. To modify these either double-click the table entry or select **Properties** .
   The **Properties** window appears.
4. In this window now check the **Details by Device** option.

   This displays the same information individually for each device of the assigned device group.

5. Click **OK** to confirm and close the window.
   The report is now reconfigured and must be regenerated.
6. Select **Edit > Generate Report** .
   The **Select Generation Formats** window displays.
7. Click **OK** to confirm the preselected choice.
   The report is now generated.
8. Go to the **Report Results > All Devices** node below the report.

   In this view all generated reports are listed in their respective format with their generation status.
   After the status `Available` is displayed the report is ready for display.

9. Select the report entry in the table and click **Edit > View** .
   A new tab or window of the browser is opened displaying this new report.

This report now shows a graph for each device providing data for the report, in this case two. The two graphics above display now - compared to the general summary generated before - the activity /inactivity and usage of the two devices.

Distribution by weekly hours report

The created report can be modified to display more detailed aspects of the defined power management. To do so, proceed as follows:

1. Select the report in the left window pane.

To know more about the general options and possibilities of reports refer to the Report section.

2. In the right pane select the **Options** tab.

   This tab displays the currently selected report options.

3. To modify these either double-click the table entry or select **Properties** .
   The **Properties** window appears.
4. Clear the **Details by Device** option.

   If you leave the option checked, the report will provide the same information but per device, that is, all charts will exists for each device.

5. In the **Group by** drop-down list, select the value **Weekly Hours**.
6. Click **OK** to confirm and close the window.
   The report is now reconfigured and must be regenerated.
7. Click **Edit > View Last Result** .
   The **Select a Group** window opens on the screen.
8. Click **OK** to confirm.
   A new tab or window of the browser is opened displaying this new report.

This report is of course only of interest if your test environment has already run for at least one week to provide data for each day of the week. In our example, the report will only show data for one day, but you will still see, how the report might look.

The report is divided into three different chart types:

1. The first pie chart displays the overall summary, the same as in the first report we generated.
2. The second part consists of a bar chart with one bar for each day of the week. The bars are summarizing the power consumption, that is, the power states of all devices per day.
3. The third part shows a bar chart for each day of the week and each hour of these days and the energy states for these hours.

Note:

If you generated the report by device, the preceding explained parts will be repeated for each of the devices delivering data, that is, having uploaded events to the master database.

Energy costs by weekly hours report

This report displays the energy costs for each of the hours of the week. To define this report, proceed as follows:

1. Select the report in the left window pane.

   > If you want to know more about the general options and possibilities of reports refer to the Report section.

2. In the right pane select the **Options** tab.

   > This tab displays the currently selected report options.

3. To modify these either double-click the table entry or select **Properties** .
   The **Properties** window appears.
4. Make sure that the **Details by Device** option is not selected.

   > If you leave the option checked the report will provide the same information but per device, that is, all charts will exists for each device.

5. In the **Unit** drop-down list select the value **Price**.
6. In the **Device Consumption (Watt)** field enter the medium consumption of a device.

   > The average consumption for a current device is between 300 and 500 watts depending on its equipment.

7. In the **Kilowatt Hour Rate** field enter the price you pay for a kilowatt hour.
   This rate varies depending on your country, for example, 0.19$ as a medium value in the United States.
8. In the **Currency** field list currency, in which the kilowatt rate is entered, for example, *$*.
   The currency will be displayed in the report in this format.
9. Click **OK** to confirm and close the window.
   The report is now reconfigured and must be regenerated.
10. Select **Edit > Generate Report** .
    The **Select Generation Formats** window appears.

11. Click **OK** to confirm the preselected choice.
    The report is now generated.
12. Click **Edit > View Last Result** .
    The **Select a Group** window opens on the screen.
13. Click **OK** to confirm.
    A new tab or window of the browser is opened displaying this new report.

The report is divided into three different chart types:

1. The first bar chart displays the overall cost summary per occurred device state.
2. The second part consists of a bar chart with one bar for each day of the week. The bars are summarising the power costs per power states of all devices per day.
3. The third part shows a bar chart for each day of the week and each hour of these days and the energy costs for these hours.

CO2 emissions by week report

This report displays the CO2 emission per week. To define this report, proceed as follows:

1. Select the report in the left window pane.

   > If you want to know more about the general options and possibilities of reports refer to the Report section.

2. In the right pane select the **Options** tab.

   > This tab displays the currently selected report options.

3. To modify these either double-click the table entry or select **Properties**.
   The **Properties** window appears.
4. Make sure that the **Details by Device** optionis not selected.

   > If you leave the option checked, the report will provide the same information but per device, that is, all charts will exists for each device.

5. In the **Unit** drop-down list, select the value **CO2 Emission (kg)**.
6. In the **Group by** drop-down, list select the value **Week**.
7. Leave the value in the **Device Consumption (Watt)** box.
8. In the **CO2 Emission (g/kWh)** box enter the amount of CO2 that is emitted into the atmosphere in average for a kWh.

> This value also varies according to the countries, in the United States for example it is ~ 520 grams of CO2 per kWh.

9. Click **OK** to confirm and close the window.
   The report is now reconfigured and must be regenerated.
10. Select **Edit > Generate Report** .
    The **Select Generation Formats** window appears.
11. Click **OK** to confirm the preselected choice.
    The report is now generated.
12. Click **Edit > View Last Result** .
    The **Select a Group** window opens on the screen.
13. Click **OK** to confirm.
    A new tab or window of the browser is opened displaying this new report.

This report only has one chart, a bar chart that displays the weekly consumption per device status in their different colors.

Defining an upload schedule for Power Management

To define the upload schedule of the **Power Management** you have two possibilities:

- Modify the default inventory parameters of the **Power Management** module.
- Define a different schedule via an operational rule and assign it to the targets.

The following paragraph explains the first option, because creating a specific schedule has already been detailed in other topics. We will change the basic schedule for all devices not only for one, therefore we will do this via the power management configuration rule that we created before:

1. Open the **Operational Rules** top node in the left window pane.
2. Select the Power Management Configuration rule among its children.
3. Select the **Steps** tab in the right window pane.
4. Select the entry in the table to the right and double-click it.
   The **Properties** window appears. It displays the following parameters which are available for the inventory management:

Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.

Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Log Events	Specifies if the events that are generated are to be logged on the local database.

5. Make the desired modifications, then click **OK** to confirm the modifications and again **OK** to confirm the step.

> If modifications were made to an operational rule it must be reassigned to its targets to notify the local agents of these.

6. Open the **Assigned Objects > Assigned Group** node of the rule.
7. Select the entry in the table to the right.
8. Select **Edit > Reassign Operational Rule** .
   The reassignment process of the operational rule will be launched. You can follow its execution under the following **Assigned Device** node. After the status `Updated` is displayed for all devices, the local agents are aware of the modifications and will from now on manage the inventory upload according to this schedule.

Regularly generating (update) the inventory

When using the automatic activation, a default schedule is assigned to the operational rule: immediate execution, once. In our case we will define a schedule first and then the assignment must be activated.

For our example, it might be useful to run the inventory rule at regular intervals, such as once a week to make sure all devices are still on their assigned power schemes and the users have not modified these. To do so, proceed as follows:

1. After the device group was assigned, go to the **Inventory > Power Management > Assigned Objects > Assigned Group** node.
2. Select the *All Devices* entry in the table in the right window pane.
3. To define the schedule either double-click the table entry or select **Properties** .
   The **Properties** window will open on the screen.
4. First go to the **Validity** tab.

> This tab allows you to define the activation of the execution and its termination.

5. In the **Select Execution Date** box define on when to run the inventory collection.

> In our example we select the **Next Startup** radio button to launch the inventory when the agent is started next.

6. Then go to the following **Termination** box and click **Run Forever**.
7. Now select the **Frequency** tab.
8. Select the **Day of the Week** radio button.

> The check boxes for the individual weekdays become available which are all checked.

9. Clear all boxes apart from **Sunday** to ensure that the devices start their work week with the right scheme.
10. In the **Period** drop-down box to the right select the value **Once daily**.
11. In the following list box select the time at which to execute the inventory collection, for example, *22:00*.

> To modify the minute value just click in the list box with the selected value and change the value, for example, to *22:30*.

12. Click **OK** to confirm the new schedule and close the window.

> The status currently displays `Assignment Paused` , which means you must activate the new schedule.
>
> > **Note:**
> >
> > If the rule was already executed before and the schedule modified afterwards the status displays `Update Paused` .

13. Reselect the *All Devices* entry in the table and then activate it by clicking **Activate Operational Rule** .

> If the rule was already executed it must now be reassigned instead of activated, therefore select **Reassign Operational Rule** .

A confirmation window appears.

14. Click **Yes**.
    The group status will change to `Activated`.
15. To follow the assignment of the group members select the *All Devices* node and follow the different status values in the table to the right.

Regularly uploading events

By default, the events are uploaded to the master database once every day at midnight. If the device is offline at that time, the events are uploaded at agent startup. If this schedule does not fit your requirements you can change it.

When using the automatic activation, a default schedule is assigned to the operational rule: immediate execution, once. For our example we will schedule the upload to take place every morning at 7, just in time for you to generate a daily report about the activities of the last 24 hours.

1. If you cleared the **Default Schedule** option in the first window, the last step of the wizard will be the **Schedule** window.
2. First go to the **Validity** tab.

> This tab allows you to define the activation of the execution and its termination.

3. Go to the following **Termination** box, select the **Run Forever** radio button.
4. Now select the **Frequency** tab.
5. Leave the **By Schedule** and the **Run Every Day** radio buttons selected.
6. In the **Period** drop-down box select the value **Once daily** .
7. In the following list box select the time at which to execute the upload, for example, *07:00.*

> To modify the minute value just click in the list box with the selected value and change the value, for example, to *07:30*.

8. Click **Finish** to confirm the schedule and terminate the wizard.
9. Continue with the general procedure.

Creating or modifying power scheme

Creating new power schemes or modifying existing ones is done via operational rules and its step. The step is the same for both operations:

1. Select **Wizards Operational Rule Creation** .
   The **Operational Rule Creation Wizard** displays on the screen. The left pane of the wizard window appears all available steps of this wizard, in the right part the first window, **Definition** , is shown.
2. Enter *Change Power Scheme* (or any other desired name) into the **Name** field.
3. Leave all other parameters as they are, because neither packages will be distributed nor dependencies are required for this rule.
4. Click **Next >** to continue.
5. Select **Add Step** on top of the list field.
   The **Select a Step** pop-up menu appears.
6. Expand the item **Power Management** and select the step **Create/Modify Power Plan**.
7. Click **Add** to confirm.
   The **Properties** dialog box appears.
8. Enter a name for the new power scheme in the respective field.

   > If you are modifying an existing scheme ensure that you enter the name of the scheme to be modified exactly as it is saved in Windows. Otherwise a new one will be generated.

9. Check the box **Active Power Plan** to make the new scheme the active scheme right away.
10. Enter the following values for testing purposes in the boxes labelled with (AC).

    > This signifies that the parameter applies to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug:

    - **Monitor Off (AC)** : 1 Minute.
    - **Hard Disc Drive Off (AC)** : 2 Minutes
    - **System Suspend (AC)** : 3 Minutes
    - **Hibernate System (AC)** : 5 Minutes
11. Leave all other values as they are.
12. Click **OK** to confirm the step.
13. Click **OK** again to confirm the list of steps for the operational rule and close the window.
14. Click **Finish** to confirm all choices and create the rule.
    A confirmation window appears which allows you to directly continue with the **Operational Rule Distribution Wizard** .
15. Click **Yes** to continue directly with the distribution of the new rule.
16. Leave all options as they are.

    >

> The **Name** field is inaccessible as the operational rule to distribute is already preselected, that is, the one we just created.

17. Click **Next >** to continue.
18. Select **Assign Device Group** on top of the list field.
    A confirmation window appears.
19. Click **Yes** to automatically launch the rule.
    The **Select a Device Group** pop-up menu appears.
20. Select the *Client Devices* group.
21. Click **OK** to confirm and close the window.
    The device group will be added to the list.
22. Click **Finish** to terminate the wizard.
    The last option of the wizard is, as usual, the choice to go directly to one the objects.
23. Check the **Go to Operational Rule** box and click **Yes**, to directly activate the rule.
24. After the operational rule is executed on all devices, you can verify if it works by continued inactivity on all your client devices.

After the operational rule is executed on all devices, you can verify if it works by continued inactivity on all your client devices. After 5 minutes, all devices should be in hibernation.

You can also regenerate a new power inventory by re-executing (reassigning) the respective operational rule to display the active power scheme and its parameters.

Changing active power scheme

The easiest way to change the active power scheme on a group of devices is again by operational rule. Be aware that here you must enter the name exactly as it is defined. To find its correct name go to the **Inventory > Power Management > Power Plans** node. Here you can see all power schemes that exist on the device with their respective parameter settings. Check the entry **Name** for the name to enter in the step parameter.

1. Select **Wizards > Operational Rule Creation** .
   The **Operational Rule Creation Wizard** displays on the screen with its first window, **Definition** . The left pane of the wizard window appears all available steps of this wizard. Depending on the selections made in the right window panes, some of these steps will become available /unavailable.
2. Enter *Change Power Scheme* (or any other desired name) into the **Name** field.
3. Leave all other parameters as they are, because neither packages will be distributed nor dependencies are required for this rule.
4. Click **Next >** to continue.
5. Select **Add Step** on top of the list field.
   The **Select a Step** pop-up menu appears.
6. Open the **Power Management** folder and select the **Define Power Plan** step.

7. Click **Add** to confirm.
   The **Properties** window appears.
8. Enter the name of the scheme to make the active scheme into the **Replacement Power Plan** field.

> Make sure you enter it exactly as it is defined in Windows. You can find the exact name either in the console in the previous inventory, or in the inventory's tab, or in the **Power Scheme** window of Windows.

9. Click **OK** to confirm the parameters and **OK** again to confirm the new step.
10. Click **OK** again to confirm the list of steps for the operational rule and close the window.
11. Click **Finish** to confirm the settings of the new operational rule.
    A confirmation window appears which allows you to directly continue with the **Operational Rule Distribution Wizard**.
12. Click **Yes** to continue directly with the distribution of the new rule.
    The **Operational Rule Distribution Wizard** displays on the screen.

> **Note:**
>
> The **Name** field is inaccessible as the operational rule to distribute is already preselected, that is, the one we just created.

13. Leave all options as they are.
14. Click **Next >** to continue with the **Assigned Targets** window.
15. Select **Assign Device Group** on top of the list field.
    The **Select a Device Group** pop-up menu appears.
16. Select the *Client Devices* group.
17. Click **OK** to confirm and close the window.
    The device group will be added to the list window.
18. Click **Finish** to confirm all choices and launch the assignment and configuration process.

> The last option provided by the wizard is again the choice to go directly to the operational rule.

19. Check the **Go to Operational Rule** box and click **Yes**, to directly activate the rule.

After the operational rule is executed on all devices, you can verify if it properly assigned the new scheme by regenerating the power inventory again. Do so by re-executing (reassigning) the respective operational rule.

Managing Power Management Inventory

The CM agent collects power management specific data in its specific inventory. The collected information is related to the individual properties of the object and contains extensive information. Not all of the collected information is available for individual devices and device groups.

This section includes following topics:

- Power Management of a device
- Power Management inventory for device groups

Power Management of a device

The **Power Management** in the BMC Client Management - Power Management is a type of custom inventory, for which the agent verifies and collects specific device parameters through the operational rule steps on the remote device. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line.

This section includes following topics:

- Power Management Inventory Attributes
- Power capabilities
- Global policies inventory of a device
- Power plans

Power Management Inventory Attributes

The **Attributes** tab of the **Power Management** node of the console displays a list of all power management related objects that are found on the device and uploaded to the master database by the agent. Some of these are settings that can be modified via operational rules, in which case a new inventory must be generated and uploaded to reflect these changes.

Power capabilities

This inventory object displays detailed information about the system power management hardware resources and capabilities of the remote device. This includes information about the presence of hardware features such as power buttons, lid switches, and batteries. Other details returned include information about current power management capabilities and configurations that can change dynamically, such as the minimum sleep state currently supported, which might change as new drivers are introduced into the system, or the presence of the system hibernation file.

The collected parameters are the following:

Parameter	Description
Allows Removal of Power to fixed Disk Devices	Indicates if the system supports allowing the removal of power to fixed disk devices.

Parameter	Description
APM BIOS Power Management Features	Indicates if the system supports APM BIOS power management features.
Batteries Present in the System	Indicates if there are one or more batteries in the system.
Display Brightness	Indicates if the system supports screen dimming capabilities.
Hibernate	Indicates if the local system supports sleep state 4. In this state the system displays to be off. Power consumption is reduced to the lowest level. The system saves the contents of memory to a hibernation file, preserving the state of the operating system, applications, and open documents.
Hibernate File Present	Indicates if the system hibernation file is present.
Lid Switch	Indicates if a lid switch is present. This parameter is only applicable to laptops and notebooks.
Low Power Saving	Indicates if the local system supports sleep state 1. In sleep states 1-3 the system displays to be off. Power consumption is reduced to one of several levels, depending on how the system is to be used. The lower the level of power consumption, the more time it takes the system to return to the working state.
Maximum Power Saving	Indicates if the local system supports sleep state 3.
Medium Power Saving	Indicates if the local system supports sleep state 2.
Power Button	Indicates if a power button is present on the device.
Processor Throttling	Indicates if the system supports processor throttling.
Short-term Batteries	Indicates if the system batteries are short-term. Short-term batteries are used in uninterruptible power supplies (UPS).
Shutdown	Indicates if the local system supports sleep state 5, that is, power off. In this state the system displays to be off. Some components remain powered so the computer can wake from input from the keyboard, LAN, or a USB device. The working context can be restored if it is stored on non-volatile media.
Suspend Button	Indicates if a sleep button is present.
Thermal Zones	Indicates if the system supports thermal zones.
UPS Present	Indicates if there is an uninterruptible power supply (UPS).
Wake Capabilities	Indicates if the system supports wake capabilities.

Global policies inventory of a device

This inventory type displays all policies about the power management feature that were found existing on the device. Policies are predefined settings for specific power management parameters for a specific situation, such as for when the device is plugged in and when the device is running on battery power.

Power plans

This object displays the list of all power schemes that exist on the device with their respective parameter settings. A power scheme is a collection of settings that controls the power usage of your computer. You can use power schemes to reduce the power consumption of individual devices or the entire system. You can configure optional features, such as support for hibernation, the amount of time the system must be idle before turning off the display, or the sleep state used when the system idle timer expires.

Following you can see a list of possible parameters that might appear in this view, however, because the parameters that are available depend on the Windows version of the remote device, not all or more might be listed here, than you will actually see in your inventory:

Parameter	Description
Power Plan Name	The name for the new power plan.
Power Plan Description	A longer textual description of the new power plan, such as after how much time the components is switched off.
Active Power Plan	Defines, if the newly defined power plan is to be activated right away and thus is the default plan.
Idle after (seconds, AC)	The time in seconds that the level of system activity must remain below the idle detection threshold before the system idle timer expires.
Throttle Policy (AC)	The processor dynamic throttling policy to use. The following values are possible: • **None** : No processor performance control is applied. This policy always runs the processor at its highest possible performance level. This policy does not engage processor clock throttling, except in response to thermal events. • **Degrade** : Does not allow the processor to use any high voltage performance states. This policy engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events. • **Constant** : Does not allow the processor to use any high voltage performance states. This policy does not engage processor clock throttling, except in response to thermal events. • **Adaptive** : Attempts to match the performance of the processor to the current demand. This policy uses both high and low voltage and frequency states. This policy lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage. This policy engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events.
Turn off display after (seconds, AC)	Determines whether and when a device's monitor is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the monitor is turned off.
	Determines whether and when a device's hard disk is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the hard disk is turned off.

Parameter	Description
Turn off hard disk after (seconds, AC)	
Minimum Sleep State (before Vista, AC)	The minimum system power state to enter on a system sleep action. The following actions are available for the parameters of this step: • **Do nothing** No power saving actions are executed. • **Sleep** This value puts the device into sleep mode. • **Hibernate** This value puts the device in hibernation. • **Shutdown** This value shuts down the computer to a point that is safe to turn off the power. All file buffers have been flushed to disk, and all running processes have stopped. • **Shutdown and Reset** This value shuts down and restarts the device. • **Shutdown and power off** This value shuts down and turns off the device, if the hardware allows this. • **Warm Eject** The system is entering a sleep mode before it is undocked from the docking station.
Reduced Latency Sleep State (before Vista, AC)	The system power state to enter on a system sleep action when there are outstanding latency requirements. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.
Sleep after (before Vista, seconds, DC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.
Hibernate after (before Vista, seconds, AC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Action at over-throttling (before Vista, AC)	Defines the system power action to initiate in response to a thermal event when processor throttling is unable to adequately reduce the system temperature. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.
Action at idling (before Vista, AC)	Defines the system power action to initiate when the system idle timer expires. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.
	The level of system activity that defines the threshold for idle detection, expressed as a percentage.

Parameter	Description
Idle at (%, before Vista, AC)	
Maximum Sleep State (before Vista, AC)	The maximum system sleep state currently supported. The following system power states are available for the parameters of this step: • **Unspecified** No power saving state is specified. • **Working** The system is fully usable. This state is similar to the **Maximum Performance** with the difference that devices that are not in use can save power by entering a lower power state. • **Low Power Saving**, **Medium Power Saving**, **Maximum Power Saving** The system displays to be off. Power consumption is reduced to one of several levels, depending on how the system is to be used. The lower the level of power consumption, the more time it takes the system to return to the working state. • **Hibernate** The system displays to be off. Power consumption is reduced to the lowest level. The system saves the contents of memory to a hibernation file, preserving the state of the operating system, applications, and open documents. Hibernation is the lowest-powered sleep state. • **Shutdown** The system displays to be off. Some components remain powered so the computer can wake from input from the keyboard, LAN, or a USB device. The working context can be restored if it is stored on non-volatile media. • **Maximum Performance** The system is fully usable.
Optimized for high performance (before Vista, DC)	If this option is activated, the system turns on cooling fans and run the processor at full speed when passive cooling is specified. This causes the operating system to be biased towards using the fan and running the processor at full speed.
Fan throttle tolerance (%, before Vista, DC)	The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event, expressed as a percentage. The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event while the system is operating on AC (utility) power, expressed as a percentage.
Forced throttle (%, before Vista, DC)	The processor throttle level to be imposed by the system, expressed as a percentage.
Lock console on activation (Vista and later, DC)	Determines whether a password is required when a device wakes from sleep. This option may be activated or deactivated. With domain devices this option should be activated and can only be controled via Group Policy.
Power button action (Vista and later, DC)	This parameter specifies the action to take when the device's power button is pressed. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.

Parameter	Description
Sleep button action (Vista and later, DC)	This parameter defines the system power action to initiate when the system sleep button is pressed. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject** .
Start menu button action (Vista and later, DC)	This option specifies whether the computer should **Do nothing** or go to **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**. It is not possible to use an action that is not supported by the device. The default value is, **Sleep** .
Lid close action (Vista and later, DC)	This parameter sets the default action when the lid of a laptop is closed. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject** .
Low battery level (%, Vista and later, AC)	Defines the low level threshold of battery discharge in percentage, by default this is 10%. When the device enters a low-power state, the system notifies the user with either a text prompt alone or a text prompt and an audible alarm. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Low battery level action (Vista and later, DC)** .
Low battery level action (Vista and later, DC)	This parameter defines which of the battery discharge policy settings is used when the battery discharges below the low threshold. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.
Critical battery level (%, Vista and later, AC)	Defines the critical level threshold of battery discharge in percentage, by default this is 3%. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Critical battery level action (Vista and later, DC)** .
Critical battery level action (Vista and later, DC)	This parameter defines which of the battery discharge policy settings is used when the battery discharges below the critical threshold. The possible values are **Do nothing**, **Sleep**, **Hibernate**, **Shutdown**, **Shutdown and Reset**, **Shutdown and power off** or **Warm Eject**.
Minimum processor state (%, AC)	Sets a minimum performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted minimum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. For example a value of 5 % would lengthen the time required to respond to requests and process data while offering substantial power savings. A value of 50 % helps to balance responsiveness and processing performance while offering moderate power savings. A value of 100 % would maximize responsiveness and processing performance while offering no power savings at all.
Maximum processor state (%, Vista and later, AC)	Sets a maximum or peak performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted maximum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. Although reducing the maximum processing power to 50 % or below can cause a significant in reduction in performance and responsiveness, it can also provide significant power savings.
PCI Express Link State Power Management (Vista and later, AC)	Determines the power saving mode to use with Peripheral Component Interconnect (PCI) Express devices connected to the device. Possible values are **Off**, **Moderate power savings** or **Maximum power savings** .

Parameter	Description
Adaptive display (Vista and later, DC)	Specifies whether Windows automatically adjusts when the display is turned off based on mouse and keyboard usage. Check the box to activate.
Sleep after (before Vista, seconds, DC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.
Hibernate after (before Vista, seconds, AC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Allow hybrid sleep (Vista and later, DC)	Specifies whether the device uses the Windows Vista sleep mode rather than the sleep mode used in earlier versions of Windows. The Window Vista hybrid sleep mode puts the device in a low power consumption state until the user resumes using the computer. When running o battery, laptops and Tablet PCs continue to use battery power in the sleep mode, but at a very low rate. If the battery runs low on power while the computer is in sleep mode the current working environment is saved to the hard disk and then the device is shut down completely. This final state is similar to the hibernate mode used with Windows XP. Leave the option unchecked to deactivate it or check to activate it.
Allow Away Mode (Vista and later, DC)	Allows users to keep their system running in case they share resources or perform other tasks for which the user doesn't actually need to operate the computer. When the PC enters **Away mode**, the display is turned off, sound is disabled, and keyboard and mouse input are ignored. **Away mode** is not a real power state. Although the PC appears to be turned off, it actually still runs and consumes power as normal. The latter is why **Away mode** is not recommended unless it's really needed. Once **Away mode** is enabled, any action that would normally put the computer into **Sleep mode** now puts the computer in **Away mode** . Pressing the physical **On/Off** button on the PC exits **Away mode**. **Away mode** can be set by media sharing applications when needed.
Allow sleep states (Vista and later, DC)	Determines whether programs can prevent a device from entering sleep mode. If this option is activated, applications and services with active processes do not prevent the device from entering sleep mode. If deactivated, they do.
Search and indexing power saving modes (Vista and later, DC)	This option allows you to balance indexing activity with power consumption. The possible values for this option are confusingly named after the default power plans, that is, **Power saver**, **Balanced** or **High performance** .
Multimedia when sharing media (Vista and later, DC)	This parameter determines what the device does when a device or another computer plays media from the computer. If you set this option to **Allow the computer to enter Away Mode**, the computer will not enter sleep mode when sharing media with other devices or computers. If you set this option to **Allow the computer to sleep** , the computer can enter sleep mode after an appropriate period of inactivity regardless of whether media is being shared with other computers or devices. If you set this option to **Prevent idling to sleep**, the computer will only enter sleep mode, when sharing media with other devices or computers, if a user puts the computer in sleep mode.

Power Management inventory for device groups

Same as with other types of inventory the power management inventory can also be compiled for the members of a device group. It is divided into the same objects as the inventory for individual devices.

This section includes the following topics:

- Global policies inventory
- Members of power management inventory
- Inventory of power management

Global policies inventory

This inventory type displays all policies about the power management feature that were found existing on the device. Policies are predefined settings for specific power management parameters for a specific situation, such as for when the device is plugged in and when the device is running on battery power.

Members of power management inventory

The **Members** tab of the inventory type displays all attributes found on at least one of the member devices of the group.

Each inventory type lists the different attributes it found and clicking one of these displays the type of the attributes plus some details on this attributes via its tabs.

Inventory of power management

The **Inventory** tab displays the object property information in tabular format:

Parameter	Description
Object Property Name	The fields of this column display the respective values found for the property, for example, the different names of the power schemes available on the different devices.
Count Count	The values in these fields provide the number, how often the property with the name value was found in the group.

Viewing alerts and events

All alerts and events that are generated for the **Power Management** can be viewed locally under the **Event Management** tab of the **Agent Configuration** node of the respective device. The tab displays all events which were logged at agent level and currently stored in the local database. It displays the following information about the individual events:

Parameter	Description
Event Date	The date and time at which the power management action, the activation of the screensaver, was executed.

Parameter	Description
Type	This field displays the type of event that occurred, that is, the screen saver was activated, the device was put in hibernation, and so on.

Power management step reference

This group of parameters collects all power management steps in the Client Management. The steps are applicable to Windows only with one exception, Suspend.

This section includes:

- Create/Modify Advanced Power Plan
- Create/Modify Global Power Policies
- Create/Modify Power Plan
- Delete Power Plan
- Hibernate
- Suspend
- Update Power Management Inventory

Create/Modify Advanced Power Plan

This step allows you to write power plans that are compatible with the older Windows versions as well as Vista and later version schemes. Fields that are not filled in will take the current value on the device. The step contains parameters applicable to all versions, as well as those for before and after Vista versions.

Parameters existing for AC and DC options will be explained only once, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop. All parameters need to be activated first, i.e., the left checkbox must be marked before the step will activate the parameter. Only then can the desired values be entered, selected or marked.

Parameter	Description
Active Power Plan	Defines, if the newly defined power plan is to be activated right away and thus is the default plan.
Power Plan Description	A longer textual description of the new power plan, such as after how much time the components is switched off.
Power Plan Name	The name for the new power plan.
Allow Away Mode (Vista and later, AC)	Allows users to keep their system running in case they share resources or perform other tasks for which the user doesn't actually need to operate the computer. When the PC enters **Away mode**, the display is turned off, sound is disabled, and keyboard and mouse input are ignored. **Away mode** is not a real power state. Although the PC

Parameter	Description
	appears to be turned off, it actually still runs and consumes power as normal. The latter is why **Away mode** is not recommended unless it's really needed. Once **Away mode** is enabled, any action that would normally put the computer into **Sleep mode** now puts the computer in **Away mode**. Pressing the physical **On/Off** button on the PC exits **Away mode**. **Away mode** can be set by media sharing applications when needed.
Allow Away Mode (Vista and later, DC)	Allows users to keep their system running in case they share resources or perform other tasks for which the user doesn't actually need to operate the computer. When the PC enters **Away mode**, the display is turned off, sound is disabled, and keyboard and mouse input are ignored. **Away mode** is not a real power state. Although the PC appears to be turned off, it actually still runs and consumes power as normal. The latter is why **Away mode** is not recommended unless it's really needed. Once **Away mode** is enabled, any action that would normally put the computer into **Sleep mode** now puts the computer in **Away mode**. Pressing the physical **On/Off** button on the PC exits **Away mode**. **Away mode** can be set by media sharing applications when needed.
Allow RTC wake (Vista and later, AC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Allow RTC wake (Vista and later, DC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Allow sleep states (Vista and later, AC)	Determines whether programs can prevent a device from entering sleep mode. If this option is activated, applications and services with active processes do not prevent the device from entering sleep mode. If deactivated, they do.
Allow sleep states (Vista and later, DC)	Determines whether programs can prevent a device from entering sleep mode. If this option is activated, applications and services with active processes do not prevent the device from entering sleep mode. If deactivated, they do.
Low battery level action (Vista and later, AC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Critical battery level action.
Low battery level action (Vista and later, DC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Critical battery level action.
Critical battery level action (Vista and later, AC)	Defines which of the battery discharge policy settings is used when the battery discharges below the critical threshold.
Critical battery level action (Vista and later, DC)	Defines which of the battery discharge policy settings is used when the battery discharges below the critical threshold.

Parameter	Description
Low battery level (%, Vista and later, AC)	Defines the low level threshold of battery discharge in percentage. When the device enters a low-power state, the system notifies the user with either a text prompt alone or a text prompt and an audible alarm. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Low battery level action.
Low battery level (%, Vista and later, DC)	Defines the low level threshold of battery discharge in percentage. When the device enters a low-power state, the system notifies the user with either a text prompt alone or a text prompt and an audible alarm. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Low battery level action.
Critical battery level (%, Vista and later, AC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Critical battery level action**.
Critical battery level (%, Vista and later, DC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Critical battery level action**.
Critical power transition (Vista and later, AC)	Specifies if critical power transition is supported. Critical power transition occurs when battery voltages for the primary batteries decrease to a critically low level that prevents the target device from performing a safe shutdown. Instead of running an On-to-Suspend transition, during which power is shut down in a timely manner, the critical power transition bypasses the usual steps of turning off power to any peripherals or devices by immediately shutting down power to them and applying refresh voltage to the RAM. This preserves the file system and sets the microprocessor into the suspend power state. Recovery from a critical power transition occurs when adequate power is applied to the device. The process of a target device recovering from a critical power transition is equivalent to a warm boot transition.
Critical power transition (Vista and later, DC)	Specifies if critical power transition is supported. Critical power transition occurs when battery voltages for the primary batteries decrease to a critically low level that prevents the target device from performing a safe shutdown. Instead of running an On-to-Suspend transition, during which power is shut down in a timely manner, the critical power transition bypasses the usual steps of turning off power to any peripherals or devices by immediately shutting down power to them and applying refresh voltage to the RAM. This preserves the file system and sets the microprocessor into the suspend power state. Recovery from a critical power transition occurs when adequate power is applied to the device. The process of a target device recovering from a critical power transition is equivalent to a warm boot transition.
Hibernate after (before Vista, seconds, AC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Hibernate after (before Vista, seconds, DC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Sleep after (before Vista, seconds, AC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.

Parameter	Description
Sleep after (before Vista, seconds, DC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.
Fan throttle tolerance (%, before Vista, AC)	The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event, expressed as a percentage. The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event while the system is operating on AC (utility) power, expressed as a percentage.
Fan throttle tolerance (%, before Vista, DC)	The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event, expressed as a percentage. The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event while the system is operating on AC (utility) power, expressed as a percentage.
Forced throttle (%, before Vista, AC)	The processor throttle level to be imposed by the system, expressed as a percentage. The processor throttle level to be imposed by the system while the computer is running on AC (utility) power, expressed as a percentage.
Forced throttle (%, before Vista, DC)	The processor throttle level to be imposed by the system, expressed as a percentage.
Allow hybrid sleep (Vista and later, AC)	Specifies whether the device uses the Windows Vista sleep mode rather than the sleep mode used in earlier versions of Windows. The Window Vista hybrid sleep mode puts the device in a low power consumption state until the user resumes using the computer. When running on battery, laptops and Tablet PCs continue to use battery power in the sleep mode, but at a very low rate. If the battery runs low on power while the computer is in sleep mode the current working environment is saved to the hard disk and then the device is shut down completely. This final state is similar to the hibernate mode used with Windows XP. Leave the option unchecked to deactivate it or check to activate it.
Allow hybrid sleep (Vista and later, DC)	Specifies whether the device uses the Windows Vista sleep mode rather than the sleep mode used in earlier versions of Windows. The Window Vista hybrid sleep mode puts the device in a low power consumption state until the user resumes using the computer. When running o battery, laptops and Tablet PCs continue to use battery power in the sleep mode, but at a very low rate. If the battery runs low on power while the computer is in sleep mode the current working environment is saved to the hard disk and then the device is shut down completely. This final state is similar to the hibernate mode used with Windows XP. Leave the option unchecked to deactivate it or check to activate it.
Hibernate after (seconds, Vista and later, AC)	Puts the device into hibernation mode after the defined number of seconds of inactivity. A value of zero indicates never hibernate.
Hibernate after (seconds, Vista and later, DC)	Puts the device into hibernation mode after the defined number of seconds of inactivity. A value of zero indicates never hibernate.
Action at idling (before Vista, AC)	Defines the system power action to initiate when the system idle timer expires.
	Defines the system power action to initiate when the system idle timer expires.

Parameter	Description
Action at idling (before Vista, DC)	
Idle at (%, before Vista, AC)	The level of system activity that defines the threshold for idle detection, expressed as a percentage.
Idle at (%, before Vista, DC)	The level of system activity that defines the threshold for idle detection, expressed as a percentage.
Idle after (seconds, AC)	The time in seconds that the level of system activity must remain below the idle detection threshold before the system idle timer expires.
Idle after (seconds, DC)	The time in seconds that the level of system activity must remain below the idle detection threshold before the system idle timer expires.
Lid close action (Vista and later, AC)	Sets the default action when the lid of a laptop is closed.
Lid close action (Vista and later, DC)	Sets the default action when the lid of a laptop is closed.
Lock console on activation (Vista and later, AC)	Determines whether a password is required when a device wakes from sleep. This option may be activated or deactivated. With domain devices this option should be activated and can only be controled via Group Policy.
Lock console on activation (Vista and later, DC)	Determines whether a password is required when a device wakes from sleep. This option may be activated or deactivated. With domain devices this option should be activated and can only be controled via Group Policy.
Maximum Sleep State (before Vista, AC)	The maximum system sleep state currently supported.
Maximum Sleep State (before Vista, DC)	The maximum system sleep state currently supported.
Minimum Sleep State (before Vista, AC)	The minimum system power state to enter on a system sleep action.
Minimum Sleep State (before Vista, DC)	The minimum system power state to enter on a system sleep action.

Parameter	Description
Minimum processor state (%, AC)	Sets a minimum performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted minimum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. For example a value of 5 % would lengthen the time required to respond to requests and process data while offering substantial power savings. A value of 50 % helps to balance responsiveness and processing performance while offering moderate power savings. A value of 100 % would maximize responsiveness and processing performance while offering no power savings at all.
Minimum processor state (%, DC)	Sets a minimum performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted minimum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. For example a value of 5 % would lengthen the time required to respond to requests and process data while offering substantial power savings. A value of 50 % helps to balance responsiveness and processing performance while offering moderate power savings. A value of 100 % would maximize responsiveness and processing performance while offering no power savings at all.
Multimedia when sharing media (Vista and later, AC)	Determines what the device does when a device or another computer plays media from the computer. If you set this option to **Allow the computer to enter Away Mode**, the computer does not enter sleep mode when sharing media with other devices or computers. If you set this option to **Allow the computer to sleep**, the computer can enter sleep mode after an appropriate period of inactivity regardless of whether media is being shared with other computers or devices. If you set this option to **Prevent idling to sleep**, the computer only enters sleep mode, when sharing media with other devices or computers, if a user puts the computer in sleep mode.
Multimedia when sharing media (Vista and later, DC)	Determines what the device does when a device or another computer plays media from the computer. If you set this option to **Allow the computer to enter Away Mode**, the computer does not enter sleep mode when sharing media with other devices or computers. If you set this option to **Allow the computer to sleep**, the computer can enter sleep mode after an appropriate period of inactivity regardless of whether media is being shared with other computers or devices. If you set this option to **Prevent idling to sleep**, the computer only enters sleep mode, when sharing media with other devices or computers, if a user puts the computer in sleep mode.
Optimized for high performance (before Vista, AC)	If this option is activated, the system turns on cooling fans and run the processor at full speed when passive cooling is specified. This causes the operating system to be biased towards using the fan and running the processor at full speed.
Optimized for high performance (before Vista, DC)	If this option is activated, the system turns on cooling fans and run the processor at full speed when passive cooling is specified. This causes the operating system to be biased towards using the fan and running the processor at full speed.
Action at over-throttling (before Vista, AC)	Defines the system power action to initiate in response to a thermal event when processor throttling is unable to adequately reduce the system temperature.
Action at over-throttling (before Vista, DC)	Defines the system power action to initiate in response to a thermal event when processor throttling is unable to adequately reduce the system temperature.
PCI Express Link State Power Management (Vista and later, AC)	Determines the power saving mode to use with **Peripheral Component Interconnect (PCI) Express** devices connected to the device. Possible values are **Off, Moderate power savings** or **Maximum power savings**.

Parameter	Description
PCI Express Link State Power Management (Vista and later, DC)	Determines the power saving mode to use with **Peripheral Component Interconnect (PCI) Express** devices connected to the device. Possible values are **Off, Moderate power savings** or **Maximum power savings**.
Power button action (Vista and later, AC)	Specifies the action to take when the device's power button is pressed.
Power button action (Vista and later, DC)	Specifies the action to take when the device's power button is pressed.
Maximum processor state (%, Vista and later, AC)	Sets a maximum or peak performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted maximum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. Although reducing the maximum processing power to 50 % or below can cause a significant in reduction in performance and responsiveness, it can also provide significant power savings.
Maximum processor state (%, Vista and later, DC)	Sets a maximum or peak performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted maximum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. Although reducing the maximum processing power to 50 % or below can cause a significant in reduction in performance and responsiveness, it can also provide significant power savings.
Reduced Latency Sleep State (before Vista, AC)	The system power state to enter on a system sleep action when there are outstanding latency requirements.
Reduced Latency Sleep State (before Vista, DC)	The system power state to enter on a system sleep action when there are outstanding latency requirements.
Search and indexing power saving modes (Vista and later, AC)	Allows you to balance indexing activity with power consumption.
Search and indexing power saving modes (Vista and later, DC)	Allows you to balance indexing activity with power consumption.
	Defines the system power action to initiate when the system sleep button is pressed.

Parameter	Description
Sleep button action (Vista and later, AC)	
Sleep button action (Vista and later, DC)	Defines the system power action to initiate when the system sleep button is pressed.
Sleep mode after idling at (%, Vista and later, AC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Sleep mode after idling at (%, Vista and later, DC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Turn off hard disk after (seconds, AC)	Determines whether and when a device's hard disk is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the hard disk is turned off.
Turn off hard disk after (seconds, DC)	Determines whether and when a device's hard disk is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the hard disk is turned off.
Sleep after (seconds, Vista and later, AC)	Put the device into sleep mode after the defined number of seconds of inactivity. A value of zero indicates never sleep.
Sleep after (seconds, Vista and later, DC)	Put the device into sleep mode after the defined number of seconds of inactivity. A value of zero indicates never sleep.
Throttle Policy (AC)	The processor dynamic throttling policy to use. The following values are possible: • **None** : No processor performance control is applied. This policy always runs the processor at its highest possible performance level. This policy does not engage processor clock throttling, except in response to thermal events. • **Degrade** : Does not allow the processor to use any high voltage performance states. This policy engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events. • **Constant** : Does not allow the processor to use any high voltage performance states. This policy does not engage processor clock throttling, except in response to thermal events.

Parameter	Description
	• **Adaptive** : Attempts to match the performance of the processor to the current demand. This policy uses both high and low voltage and frequency states. This policy lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage. This policy engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events.
Throttle Policy (DC)	The processor dynamic throttling policy to use. The following values are possible: • **None** : No processor performance control is applied. This policy always runs the processor at its highest possible performance level. This policy does not engage processor clock throttling, except in response to thermal events. • **Degrade** : Does not allow the processor to use any high voltage performance states. This policy engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events. • **Constant** : Does not allow the processor to use any high voltage performance states. This policy does not engage processor clock throttling, except in response to thermal events. • **Adaptive** : Attempts to match the performance of the processor to the current demand. This policy uses both high and low voltage and frequency states. This policy lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage. This policy engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events.
USB selective suspend (Vista and later, AC)	Allows a device's port to be suspended when the device is not in use in order to conserve power.
USB selective suspend (Vista and later, DC)	Allows a device's port to be suspended when the device is not in use in order to conserve power.
Start menu button action (Vista and later, AC)	Specifies whether the computer should Do nothing or go to Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power off or Warm eject. It is not possible to use an action that is not supported by the device.
Start menu button action (Vista and later, DC)	Specifies whether the computer should **Do nothing** or go to **Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power off** or **Warm eject**. It is not possible to use an action that is not supported by the device.
Adaptive display (Vista and later, AC)	Specifies whether Windows automatically adjusts when the display is turned off based on mouse and keyboard usage. Check the box to activate.
	Specifies whether Windows automatically adjusts when the display is turned off based on mouse and keyboard usage. Check the box to activate.

Parameter	Description
Adaptive display (Vista and later, DC)	
Turn off display after (seconds, AC)	Determines whether and when a device's monitor is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the monitor is turned off.
Turn off display after (seconds, DC)	Determines whether and when a device's monitor is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the monitor is turned off.

Create/Modify Global Power Policies

This step allows you to write global power policies that are not related to power schemes. This step will not work on Vista and later. A power scheme is a collection of settings that controls the power usage of your computer.

Parameters existing for AC and DC options will be explained only once, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop. All parameters need to be activated first, i.e., the left checkbox must be marked before the step will activate the parameter. Only then can the desired values be entered, selected or marked.

Parameter	Description
Broadcast capacity resolution	Defines the resolution of change in current battery capacity that should cause the system to be notified of a system power state changed event. Check the box to activate it and enter the desired value in the text field.
Enable multiple battery display	Enables or disables multiple battery display in the system power meter.
Require a password on wakeup	Enables or disables requiring password login when the system resumes from standby or hibernate.
Enable systray battery-meter	Enables or disables the battery meter icon in the system tray. When this option is deactivated, the battery meter icon is not displayed on the desktop.
Enable monitor dimming	Enables or disables support for dimming the video display when the system changes from running on AC power to running on battery power.
Enable Wake-on-ring	Enables or disables wake on ring support.
Lid close action (AC)	Defines the system power action to initiate when the system lid switch is closed when running on AC power.
Lid close action (DC)	Defines the system power action to initiate when the system lid switch is closed when running on DC power.

Parameter	Description
Lid open wake (AC)	Defines the maximum power state from which a lid-open event should wake the system when running on AC power.
Lid open wake (DC)	Defines the maximum power state from which a lid-open event should wake the system when running on DC power.
Power button action (AC)	Defines the system power action to initiate when the system power button is pressed when running on AC power.
Power button action (DC)	Defines the system power action to initiate when the system power button is pressed when running on DC power.
Power level 0 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 0 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 0 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 0 policy action	Defines the action to take for this battery discharge policy.
Power level 1 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 1 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 1 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 1 policy action	Defines the action to take for this battery discharge policy.
Power level 2 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 2 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 2 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 2 policy action	Defines the action to take for this battery discharge policy.
Power level 3 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 3 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 3 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.

Parameter	Description
Power level 3 policy action	Defines the action to take for this battery discharge policy.
Sleep button action (AC)	Defines the system power action to initiate when the system sleep button is pressed when running on AC power.
Sleep button action (DC)	Defines the system power action to initiate when the system sleep button is pressed when running on DC power.

Create/Modify Power Plan

This step allows you to create a new power plan. It has parameters to be defined, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop.

Parameter	Description
Active Power Plan	Defines, if the newly defined power plan is to be activated right away and thus is the default plan.
Power Plan Description	A longer textual description of the new power plan, such as after how much time the components is switched off.
Hard Disc Drive Off (AC)	Defines when the hard disk of the device is to be switched off when running on AC power.
Hard Disc Drive Off (DC)	Defines when the hard disk of the device is to be switched off when running on DC power.
Hibernate System (AC)	Defines when the system is put in hibernation when running on AC power.
Hibernate System (DC)	Defines when the system is put in hibernation when running on DC power.
Monitor Off (AC)	Defines when the screen of the device is to be switched off when running on AC power.
Monitor Off (DC)	Defines when the screen of the device is to be switched off when running on DC power.
Power Plan Name	The name for the new power plan.
System Suspend (AC)	Defines when the system is suspended when running on AC power.
System Suspend (DC)	Defines when the system is suspended when running on DC power.

Define Power Plan

This step defines the default power plan which will be used.

Parameter	Description
Replacement Power Plan	Enter into this field the name of the power plan which is to be used by default.

Delete Power Plan

This step deletes an existing power plan and specify the new default plan if appropriate.

Parameter	Description
Power Plan Name to Delete	Enter the name of the power plan to be deleted.
Replacement Power Plan	Enter into this field the name of the power plan which is to be used by default.

Hibernate

This step allows you to immediately put the target device in hibernation.

Parameter	Description
Force	Check this box to force the device to go in hibernation, even if there is activity on the device.

Suspend

This step allows you to immediately put the target device in stand-by mode. It is applicable to Windows and MacOS devices.

Parameter	Description
Force	Check this box to force the device to go in suspend mode, even if there is activity on the device. This parameter is only applicable to Windows devices.

Update Power Management Inventory

This step launches an update of the power management inventory of the device. It is applicable to Windows only.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.

Managing diagnostic tools

The **Diagnostic Tool** provides the CM administrator with checks and verifications to investigate if something does not seem to work correctly and some general sanity checks. It also provides automatic repair operations where possible.

The diagnostics can be used for the following situations:

- Work load evaluation on the master server via its work and file store queues
- Database integrity verification via master agent, device agent and assignment diagnostics.

The CM **Diagnostic Tool** diagnoses problems on:

- The master
- A client
- Operational rules (assignment problems).

The diagnostics tool is accessible in its own node under the **Global Settings** . Under this node you can execute diagnostics on individual device or device groups and find the results of these in their respective subnodes.

Related topics

- Launching a diagnostic
- Viewing device diagnostic results
- Viewing device group diagnostic results
- Canceling a running diagnostic
- Deleting diagnostic results
- Repairing corrupted data in the database
- Filtering for specific diagnostic results
- Filtering for specific status values
- Importing new diagnostic scripts

Launching a diagnostic

If you are launching a diagnostic for the first time on a device or a device group proceed as follows:

If you are relaunching the diagnostic, start at step 3 of the procedure.

1. Select the **Devices** / **Device Groups** node in the left tree hierarchy.
2. Right-click the selected node in the left tree hierarchy.
   A pop-up menu appears.
3. Select the **Add Device** / **Add Device Group** / option.

   > If the device/group is already listed under the node you can (re-)launch a diagnostic by simply clicking **Launch Diagnostic** from the drop-down menu to the right above the table.

   The **Select a Device Group** window appears.
4. Select the desired device/device group and click **OK**.
   The **User Accounts Used for Diagnostic** window appears.

5. Here you can enter or modify user accounts to access the device(s) by clicking **Add** or **Modify**.
   A **Properties** window appears.
6. Enter the login name and corresponding password in the respective text boxes and re-enter the password for confirmation or modify the existing values.
7. To view the passwords clear the **Hide Passwords** check box. Both password boxes will now be displayed in clear text format.
8. To confirm the new user account click **OK** at the bottom of the window.
9. The account will be added to the list in the **User Accounts Used for Diagnostic** window.
10. Repeat the previous steps to add more authentications if necessary.
11. Click **OK** to confirm all authentications and launch the diagnostics.
    An information window appears informing you that the diagnostic was launched.
12. Click **Close** to close the window.

The diagnostic is started directly. A node will appear for the device/device group under the **Global Settings > Diagnostic Tool > Device Groups** / **Devices** nodes in which you can follow the progress of the diagnostic tests.

Viewing device diagnostic results

The subnodes of the individual devices provide detailed information about the diagnostic results. These are displayed via the following tabs:

- Results
- WorkQueue
- FileStoreQueue

Results

The tab shows the overall results of the last diagnostics run on the device. The page is divided into two parts:

- A summary of all tests executed in the upper part.
- Details on the results found by the selected test in the lower part of the view.

Diagnostic Summary

This panel shows an overview of all diagnostics that were executed on the device as well as their results. You can filter the display via the **Diagnostic Status** field, located above the table by selecting **Errors Only** to only show those test for which the result was in error or **Details** to show result details.

The following table shows the following information about all executed tests:

Parameter	Description
Test Type	This column lists all diagnostics that were executed on the device.

Parameter	Description
Status	These fields show if the diagnostics were executed successfully or if they failed.
Last Modification Date	Displays the date and time at which the selected object was modified for the last time; for folders this field remains empty.

Selecting a line will show details on the entry in the following panel.

Diagnostics Details

After you selected a specific test in the upper part of the view the following table will show more detailed information about the results found by your selected test:

Parameter	Description
Description	This column lists all test that were run by the diagnostic.
Details	This field explains the result of the individual executed test.
Solution	This column shows if a solution is available for the problem and, if yes, explains it. The field is always emtpy for successfully executed tests.

WorkQueue

This tab is only available for the master. It shows all operations that the master has currently in his queue for execution, requested either by an agent or specifically by the console.

It is divided into the following two parts:

- Work Queue load
- List of operations

Work Queue load

The pie chart in this upper part of the tab displays the different types of operations that are currently in the work queue of the master, such as identity uploads, patches to install, inventories to generate, and so on. The graph is automatically updated according to the user settings defined in the **Preferences** and thus allows you to follow the progress of time- and resource-consuming processes. This tab is provided to ensure that your master is not becoming overloaded.

List of operations

The table in the lower part of the pane displays the list of operations together with the following information:

Parameter	Description
RequestTime	The date and time that the object to transfer was created on the originating device. This is the same information as that of the **Name** field part but in standard date and time format of *DD MMM YYYY - hh:mm:ss* .
ObjectTypeName	This field displays the type of the object, such as *CustomInventory, Autodiscovery* or *Timer* .
Object Name	

Parameter	Description
	This field shows a character string made up of several components which identifies the origin of the data. The components are the following:n- the name of the device which created the object connected with an underscore (*) ton- the name of the module, which, it is sending, connected again with an underscore (*) ton- the time the object was created in seconds since 1970, another underscore plusn- a random number. This number is added to ensure that even if two objects are received at the same time are uniquely identifiable. nFor example: *scotty_CustomInventory_157896472_1853* , here the device with the name *scotty* sends up its custom inventory data.
OperationName	The name of the operation to be executed on the objects.
Parameter	Any parameter that is needed by the operation for its execution.

FileStoreQueue

This tab is only available for the master. It shows the list of all files that were uploaded to the master for handling.

It is divided into the following two parts:

- File Store Queue load
- Oldest file by priority

File Store Queue load

The upper part of the view displays information about the contents of the file store queue via a bar chart, that is it show a bar per file type and the number of files of this type is represented in the hieght of the bar. The graph is automatically updated according to the user settings defined in the **Preferences** and thus allows you to follow the progress of time and resource consuming processes. This tab is provided to ensure that your master is not becoming overloaded, that is, in a perfect environment this tab should always be empty.

Oldest file by priority

The table in the lower part of the view displays the oldest file for each of the possible priorities together with the following information:

Parameter	Description
QueueId	The unique identifier of the file given to it by the database.
FileType	The type of the file, for example, *Identity, OperationalRuleStatus* or *Package*. The type is based on the source module of the file. The modules used by modules such as *Inventory, Packages, Operational Rules, Rollout, Identity* , etc.
SourceDevice	Shows the name of the machine on which the file was created plus its port number, for example, *scotty:1610*.
FirstRelay	The name of the first relay if the transfer channel is **Data**, that is, the data is being sent to a client. If the object is defined **Notification**, this field is empty, as the way to the managed device is known to the master and thus does not need to be stored.
FilePath	The path to the file where it is located on the master.
FileLabel	The label is based on the source module of the file, for example, the name of the step of an operational rule, or the package name used on the client for an package.

Parameter	Description
FileName	This field displays the physical name of the file.
FileChecksum	The checksum of the file.
Priority	This value is only used by the asset discovery module when integrating inventories of remote devices. The default value of 100 is lowered to 500 if an inventory to be integrated arrives before the identity of the device.
FileInfo	Information that is passed on by the files.
AdditionalInfo	Any additional information that might be passed on, for example, additional parameters that are passed on by file type.
FileTypePriority	The priority order in which the files are handled. Most files have a priority of 0 (low). If a file has priority 1 (high), it is handled first.

Viewing device group diagnostic results

The subnodes of the individual device groups provide detailed information about the diagnostic results. These are displayed via the following tabs:

- Status
- Summary

Status

This view shows the list of all diagnostic tests that are currently running or were already terminated on the member devices of the group. It can be filtered to reduce the list either by **Execution Status** or by **Diagnostic Result** . The table provides the following details on the tests:

Parameter	Description
Name	The name of the device on which the diagnostics were executed.
Status	Displays the progress of the diagnostic execution.
Diagnostic Result	These fields show if the diagnostics were executed successfully or if they failed.
Description	This column lists all test that were run by the diagnostic.
Create Time	The date and time at which the object was originally created.
Last Modification Date	Displays the date and time at which the selected object was modified for the last time; for folders this field remains empty.

Right-clicking an entry allows you to go to the selected entry by selecting the **Go To** item of the appearing pop-up menu or by double-clicking the entry. The focus of the console will be moved to the selected device under the **Devices** node.

This section includes following topics:

- Changing the update manager
- Checking for available updates
- Local update manager status

- Updating the components

Changing the update manager

f you need to define another device as the **Update Manager** , proceed as follows:

1. Click **Change Update Manager** .
   The **Change Update Manager** window displays.
2. Select the new **Update Manager** from one of the available lists.
3. Click **OK**.

The selected device is now the new **Update Manager**. The focus of the console moves to the **Update Manager** view of the device. There you can ensure that it is up to date by checking for later versions and if required updating the components.

Checking for available updates

To verify if updates are available for one or more of the components, proceed as follows:

1. Click **Check for Update** .

A verification is launched via the Internet to check for available updates.

- If none are found only the **Last Verification** date box above the table is updated with the date and time of this operation.
- If one or more updates are available this information is presented as follows:
  - The icon color of the **Last Verification** box changes to either yellow (update available for at least one component) or red (updates available for all components).
  - The value of the **Status** box of the respective component changes to `Out of Date`.
  - The color of the **Status** icon changes to yellow or red.

Local update manager status

To locally verify the status of the **Update Manager** , proceed as follows:

1. Go to the **Device Topology > Your Update Manager > Agent Configuration > Module Configuration > Update Management** node.
2. Select the **Update Status** tab.

This view displays the following information about the current status of the **Update Manager**:

Parameter	Description
Component	The fields of this column list all components of which the automatic update can be managed by the **Update Manager** .
Version	This field displays the currently installed version of the respective component.
Status	

Parameter	Description
	This field displays the current status of the component, that is, if the component is of the latest available version (`Up to Date`) or if it needs to be updated (`Out of Date`). Any type of failed status, such as `Download Failed` , `License expired` will be displayed via a red flag. During the update process this field will also display the different stages of the process until all components are up to date.
Available Version	After a check was executed and updates are available for individual components this field will indicate their version number.

Updating the components

After a verification indicated that updates are available for at least one component, proceed as follows:

1. Click the arrow next to **Status** Update all Components and select which components to update. You have the following options:
   - **Update All Components** to update all components for which an updated version is available.
   - **Update Security Products and Virtualization (before v12)** to update only the security products and the virtualization modules or
   - **Update Software Catalog** to only update the software catalog.
2. The update process is launched.

1. a. The available updates for the selected components are downloaded.
   b. The value of the **Available Version** changes to the version number of the version that was just downloaded.
   c. The installation process of the components is started.

After the update process is finished, the value of the **Version** box changes to that of the **Available Version** , the status will change to `Up to Date` , the icon turns green again and the **Last Update Time** changes to the current date and time value.

Any type of failed status, such as `Download Failed` , `License expired` will be displayed via a red flag. During the update process this box will also display the different stages of the process until all components are up to date.

Summary

This is the summary of all the diagnostics for a group. Tests are run on individual devices to ensure the device is in a healthy state and to identify individual problems. Details are available on the **Status** tab.

This table only displays the diagnostics that failed on at least one member of the device group.

Parameter	Description
Details	This field explains the result of the individual executed test.
Count	The number of group device members on which this test failed.

Parameter	Description
Solution	This column shows if a solution is available for the problem and, if yes, explains it. The field is always emtpy for successfully executed tests.

Canceling a running diagnostic

To cancel an executing diagnostic proceed as follows:

1. Select the running diagnostic to cancel in the table.
2. Click **Cancel Diagnostic** from the drop-down menu to the right above the table.
   A confirmation window appears.
3. Click **Yes** to confirm.

The selected diagnostic is stopped immediately.

Deleting diagnostic results

After you have finished analysing and taking care of any problems found by the diagnostics you can delete the now obsolete results. To do so, proceed as follows:

1. Select the respective entries in the table.
2. Click **Purge Diagnostic Result** from the drop-down menu to the right above the table.
   A confirmation window appears.
3. Click **Yes** to confirm.

The selected diagnostic result(s) are deleted from the view and from the database.

Repairing corrupted data in the database

This option is only available on the Master. It allows you to repair corrupted data in the CM database. To do so, proceed as follows.

1. Click **Repair Data Corruption at Next Start-up** from the drop-down menu to the right above the table.

All corrupted data in the database for which an automatic repair exists will be repaired at the next CM agent startup.

Filtering for specific diagnostic results

If you have executed many tests, the results table can be quite long. Above the table, two list boxes are available that provide you the possibility to filter and thus reduce the number of entries in the results table. To filter the table according to a specific result, proceed as follows:

1. In the box **Diagnostic Result** select the status to which you want to limit the list to:
   - **All** to display all executed diagnostics.
   - `Failed` to display all diagnostics of which at least one test failed.

- `Diagnostic Init Failure` to display only diagnostics of which at least one test could not be initialized.
- `Successful` to display only diagnostics that completed successfully.
- `Aborted` to display only diagnostics of which the execution was cancelled.

The list is immediately updated and will now only show the desired results.

Filtering for specific status values

If you have executed many tests, the results table can be quite long. Above the table, two list boxes are available that provide you the possibility to filter and thus reduce the number of entries in the results table. To filter the table according to a specific status, proceed as follows:

1. In the box **Execution Status** select the status to which you want to limit the list to:
   - **All** to display all launched diagnostics.
   - `Aborted` to display only diagnostics of which the execution was cancelled.
   - `Done` to display only diagnostics that are finished.
   - `Diagnostic in progress` to display only diagnostics that are still running.
   - `Waiting` to display only diagnostics that are launched but are still awaiting their execution.

The list is immediately updated and will now only show the results of the desired status.

Importing new diagnostic scripts

Diagnostic scripts can be added to CM at any time. After their scripts are created and put in the proper location on the master, they can be directly imported in the console.

To import new steps proceed as follows:

1. Put the files for the new scripts in the directory `data/Vision64Database/checkscripts` .
2. Select **Tools > Import Diagnostic Tool Scripts**  .
   The **Schedule Import of New Steps** window opens on the screen.
3. Specify in this window if the import is to be launched immediately or if it is to be fixed for a specific date and time by entering the values in the respective boxes.
4. Click **OK** to confirm the schedule and close the window.

The import of any new scripts will now be executed at the specified moment.

Managing mobile devices

This section provides information for the IT administrators who need the ability to configure, manage, and control the mobile devices that employees use to access the enterprise data. To enable mobile device management, the user first needs to enroll the device for mobile device management in BMC Client Management. When a mobile device is enrolled, it is referred to as a managed mobile device.

For more information about features and benefits of mobile device management in BMC Client Management, see Mobile device management.

> **Note**
>
> BMC Client Management supports mobile device management for only mobile devices with OS 8.x and later.

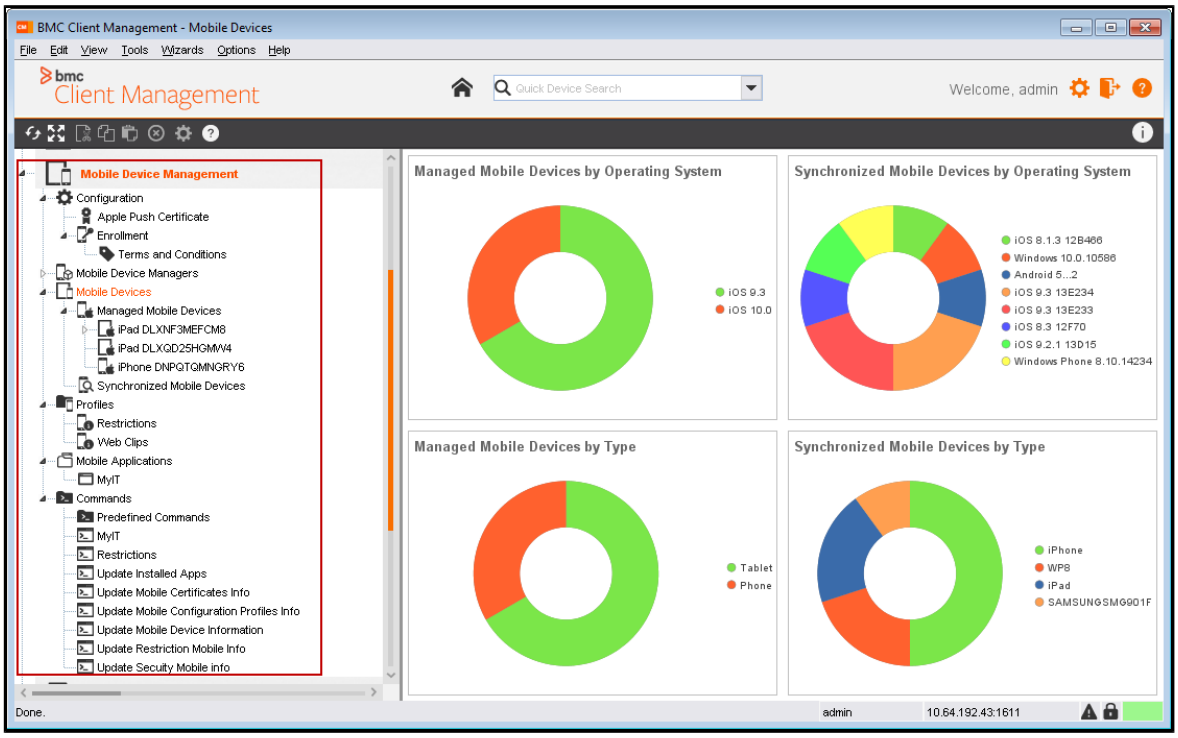
This section includes the following topics:

- Mobile devices in BMC Client Management
- License utilization
- User goals and instructions

Mobile devices in BMC Client Management

Using BMC Client Management, the IT administrators can discover all the mobile devices in the network. Although, BMC Client Management discovers all mobile devices registered with the directory server, only iOS mobile devices can be enrolled and managed in BMC Client Management.

The following screenshot shows a summary of all mobile devices in the IT infrastructure, categorized by operating system and mobile device type under **Mobile Device Management** > **Mobile Devices**.



Under **Mobile Devices** node, the mobile devices are listed in the following views:

- **Managed Mobile Devices**: All the iOS mobile devices that are enrolled for mobile device management are listed under **Managed Mobile Devices** node. For a managed mobile device, you can perform remote operations such as:
  - View and collect detailed inventory
  - Install or remove applications
  - Push or revoke configuration profiles
- **Synchronized Mobile Devices**: All mobile devices that are registered with directory server are listed under the **Synchronized Mobile Devices** node. For a synchronized mobile device, you can view device information such as:
  - Name
  - Mobile device type
  - Operating system
  - Model
  - Subscriber carrier

> **Note**
>
> The managed mobile devices are also listed in the **Synchronized Mobile Devices** list.

You can also assign or unassign directory servers to synchronized mobile devices.

License utilization

The following table explains how BMC Client Management licenses are utilized by a managed mobile device:

License type	A license is utilized when...	A license is released when...
BCM Agents	Mobile device is successfully enrolled	Mobile device is deprecated
Inventory	Inventory is collected for a managed mobile device	• Last inventory is purged • Mobile device is deprecated
Compliance Management	One or more compliance rules are assigned to the managed mobile device	All the compliance rules are unassigned from the managed mobile device

Note

Only one inventory license is utilized per managed mobile device. The inventory license is utilized as soon as the mobile device inventory is sent to database for the first time. Consequent inventory updates do not require additional inventory licenses.

For more information about BMC Client Management licenses, see License entitlements.

User goals and instructions

The following table provides links to relevant topics based on your goals:

Goal	Instructions
• Configure mobile device management to start managing mobile devices	Configuring mobile device management
• Enroll mobile devices for mobile device management in BMC Client Management	Enrolling mobile devices
• Collect and view inventory of managed mobile devices for organizational or legal compliance • View and assign objects to assign or unassign licensed software, compliance rules, and commands • View financial information of managed mobile devices	• Viewing information about managed mobile devices • Performing remote operations on managed mobile devices
• Create, configure, and install configuration profiles on managed mobile devices	Managing configuration profiles for managed mobile devices
• Create applications lists and remotely install applications on managed mobile devices	Managing mobile applications

• Collect inventory • Install or remove mobile applications • Install or remove configuration profiles • Lock, unlock, or wipe mobile devices to prevent unauthorized access to enterprise data	Performing remote operations on managed mobile devices

Enrolling mobile devices

This section provides information on how employees can enroll their iOS mobile devices for mobile device management in BMC Client Management.

The following BMC Client Management video (2:21 min) provides information about how to enroll mobile devices for mobile device management.

https://youtu.be/aRtCbYB9IV8

Employees who use their mobile devices to access enterprise data need to enroll their devices. The IT administrator sends the enrollment invitation to employees, who need to enroll their mobile devices, with an enrollment link.

After a mobile device is enrolled, the IT administrator can remotely perform operations to configure and manage the mobile device, such as:

- set up Wi-Fi connection
- set or reset a passcode
- configure email accounts
- install certificates and applications
- lock or wipe (factory reset) the lost mobile device to prevent unauthorized access to the enterprise data

BMC Client Management supports management of the following iOS mobile devices:

- iPod Touch 5th generation and later
- iPhone 4S and later
- iPad 2 and later (including iPad Air, iPad Pro, and iPad Mini series)

This section includes the following topics:

Before you begin

To enroll your mobile device, ensure that the following prerequisites are met:

- You have an active user account with a valid email address in the directory server
- Your mobile device is connected to Internet
- You have received the enrollment link (IT administrators sends out enrollment invitation with the enrollment link)

> **Note**
>
> Contact your system administrator if you have not received the enrollment invitation.

Enrolling mobile device

You can enroll your mobile device by accessing the enrollment link shared by your IT administrator. If you open the enrollment link in the Safari browser from a supported iOS mobile device, the enrollment wizard displays two options - **Enroll this mobile device** and **Enroll another mobile device** . If you open the enrollment link from a device other than a supported iOS mobile, only the **Enroll another mobile device** option is displayed.

If you are enrolling the mobile device for the first time, the enrollment wizard prompts you to first installs the **BMC Client Management Certificate Authority** (CA) certificate and then enrolls the mobile device. Also, if you are opening the enrollment link from a device other than the iOS mobile device you want to enroll, you should have a QR code scanning application (for example, QR Reader) installed on the mobile device to be enrolled. Alternatively, if you do not have a QR code scanning application, you can select the option to receive the links for adding the CA certificate and enrolling the mobile device in an email.

> **Note**
>
> The links (as an alternative to scanning the QR) to install CA certificate and enroll mobile device are valid for single use only.

To enroll a mobile device by accessing the enrollment link from the enrolling device

1. Open the enrollment link in the Safari browser of the iOS mobile device you want to enroll. The **Welcome** page displays the following options:
   - Enroll this mobile device
   - Enroll another mobile device

2. Click **Enroll this mobile device** and follow the on-screen instructions to complete the enrollment.
   After the mobile device is enrolled successfully, you will receive a confirmation message. If you do not receive a confirmation message, contact your IT administrator.

To enroll a mobile device by accessing the enrollment link from another device

1. Open the enrollment link.
   If you have opened the enrollment link in the Safari browser of a supported iOS mobile device, the **Welcome** page displays the following options:
   - Enroll this mobile device
   - Enroll another mobile device

   If you have opened the enrollment link in any other browser, only the **Enroll another mobile device** option is displayed.
2. Click **Enroll another mobile device**.
3. On the **Authentication** page, specify the email address where you received the enrollment invitation, enter your active directory user account password, and click **Next**.
4. Read and agree to the **Terms and Conditions** and click **Next**.
   The **Enrollment** page displays the QR codes that you can scan using a QR code scanning application to install the BMC CA certificate and to enroll the mobile device.
5. From the mobile device that you want enroll, scan the QR code under the **Add the certificate authority** step.

   Notes

   - If the mobile device was enrolled previously and you retained the BMC Client Management CA certificate, you can skip this step and directly scan the QR code under the **Enroll the mobile device** step.
   - You can verify the BMC Client Management CA certificate under **Settings** > **General** > **Profile & Device Management**.
   - If you do not have a QR code scanner application, you can select the option to receive the links for adding the CA certificate and for enrolling the mobile device in an email. These links can be used once, and you must open them in the Safari browser of the mobile device that you want to enroll.

6. After the CA certificate is installed, click **Show QR code** under the **Enroll the mobile device** step.
7. Scan the QR code from the mobile device.
   After the mobile device is enrolled successfully, you will receive a confirmation message. If you do not receive a confirmation message, contact your IT administrator.

Withdrawing device from mobile device management enrollment

You can withdraw an enrolled mobile device from the mobile device management any time by uninstalling the BMC Encrypted Configuration Profile and enroll it again later as per your requirement.

To withdraw device from mobile device management enrollment

1. In your managed mobile device, navigate to **Settings** > **General** > **Profile & Device Management**.
   The **BMC Encrypted Configuration Profile** and **BMC Client Management Certificate Authority** certificates are displayed. These certificates are used for managing your mobile device from BMC Client Management.
2. Select the **BMC Encrypted Configuration Profile** certificate and then tap **Remove Management.**
3. Tap **Remove** to confirm.
   The certificate is removed. The mobile device is no longer managed by BMC Client Management.
4. (*Optional*) To also remove the BMC CA certificate, select **BMC Client Management Certificate Authority** and remove it.

> **Note**
>
> Even if you retain the **BMC Client Management CA** certificate after withdrawing the enrollment, the mobile device is not managed by BMC Client Management. This certificate would be useful if you intend to enroll the mobile device again in the future.

Related topics

Viewing information about managed mobile devices

Managing mobile applications

Managing configuration profiles for managed mobile devices

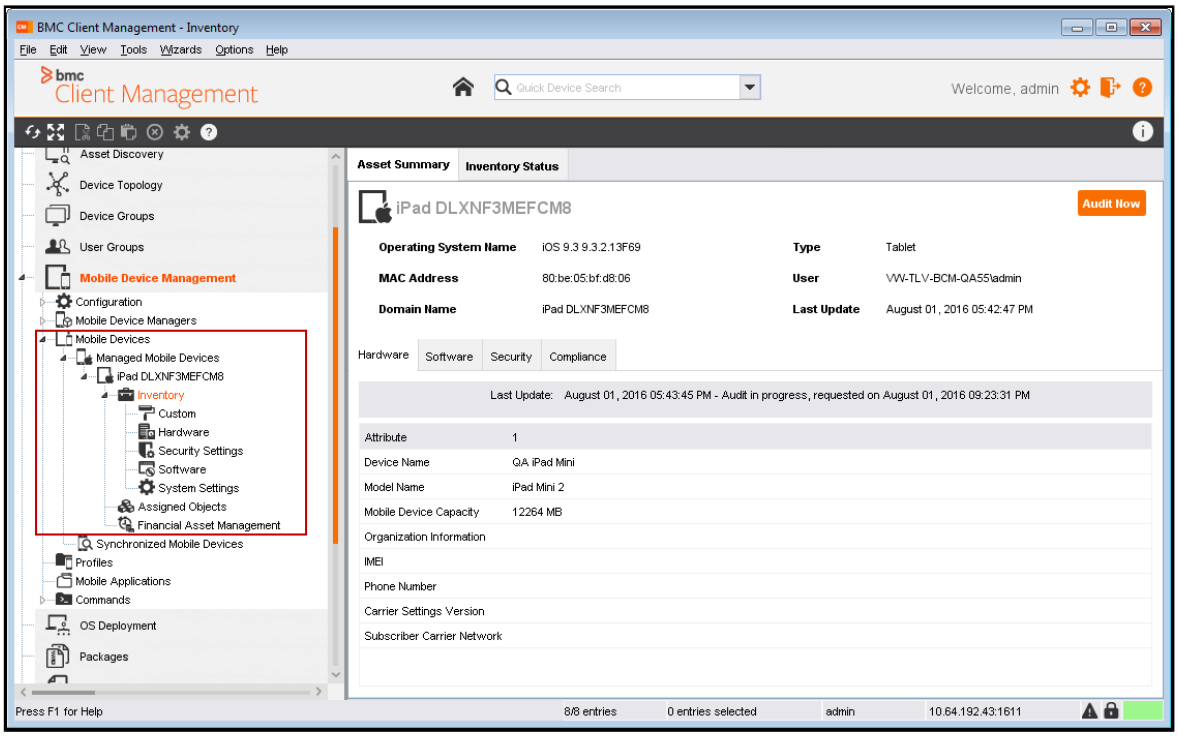
Performing remote operations on managed mobile devices

Managing mobile devices

Viewing information about managed mobile devices

After a mobile device is enrolled for mobile device management, the IT administrator can audit the mobile device to collect the inventory. After the inventory data is uploaded, you can view the detailed information about the mobile device in the console. The IT administrators can also configure the mobile device management to regularly collect the latest inventory of the managed mobile devices for organizational or legal compliance. After selecting a mobile device in the left pane, the IT administrator can launch audit to collect latest information about the mobile device and perform remote operations such as install or remove applications, directly lock, unlock, or wipe (factory reset) the mobile device, and so on.

The following screenshot shows basic information about a mobile device:



The section includes the following topics:

- To upload and view the inventory of a managed mobile device
- To view and manage the assigned objects of a managed mobile device
- To view the financial information of a managed mobile device

To upload and view the inventory of a managed mobile device

For a managed mobile device, you can view the following information:

- Hardware
- Software
- Security settings

- System settings

For a complete list of inventory attributes, see Inventory Types and Licenses.

1. In the left pane, select **Mobile Device Management** > **Mobile Devices** > **Managed Mobile Devices** > ***mobileDeviceName*** > **Inventory**.
   The **Asset Summary** tab displays the information from the last inventory.
2. In the right pane, click **Audit Now** to collect and upload the latest inventory.
   When the device connects to the internet, the following commands are assigned to the mobile device:
   - Update Device Information
   - Update Device Security
   - Update Installed Applications

   The information collected from these commands is uploaded to BMC Client Management and displayed under the **Inventory** node. The **Inventory Status** tab displays the last inventory update date and time and inventory license information.

To view and manage the assigned objects of a managed mobile device

Different objects can be assigned to or unassigned from managed mobile devices. These objects include licensed software, compliance rules, and commands. For a managed mobile device, you can view the details about each object, assign new objects, or unassign existing objects:

- Licensed software: Assign licensed software to a mobile device only if it is required; otherwise, unassign it.
- Compliance rules: Assign compliance rules to generate inventory reports that are required for organizational or statutory compliance policies. For more information about compliance rules, see Managing compliance.
- Commands: Assign commands (and also check command execution status) to perform remote operations on the managed mobile devices. For more information about commands, see Performing remote operations on managed mobile devices.

Example of assigning an object (licensed software)

The following example explains how you can assign a new licensed software to a managed mobile device:

1. In the left pane, select **Mobile Device Management** > **Mobile Devices** > **Managed Mobile Devices** > ***mobileDeviceName*** > **Assigned Objects** > **Licensed Software**.
2. Right-click anywhere in the right pane and select **Assign Licensed Software**.
3. In the **Assign Licensed Software** dialog box, search or browse and select the required licensed software and click **OK**.
   The licensed software is assigned to the device.

Similarly, you can assign compliance rules and commands.

To view the financial information of a managed mobile device

Like any other device, you can view financial information of a managed mobile device. The financial information view of a device provides the IT administrators an insight into the total cost of ownership and the current device lifecycle status. Based on this information, the IT administrators can make informed decision about when they need to replace a device. For more information about financial information of an asset, see Managing financial information for assets.

- To view financial information, select **Mobile Device Management** > **Mobile Devices** > **Managed Mobile Devices** > ***mobileDeviceName*** > **Financial Asset Management**.

Managing mobile applications

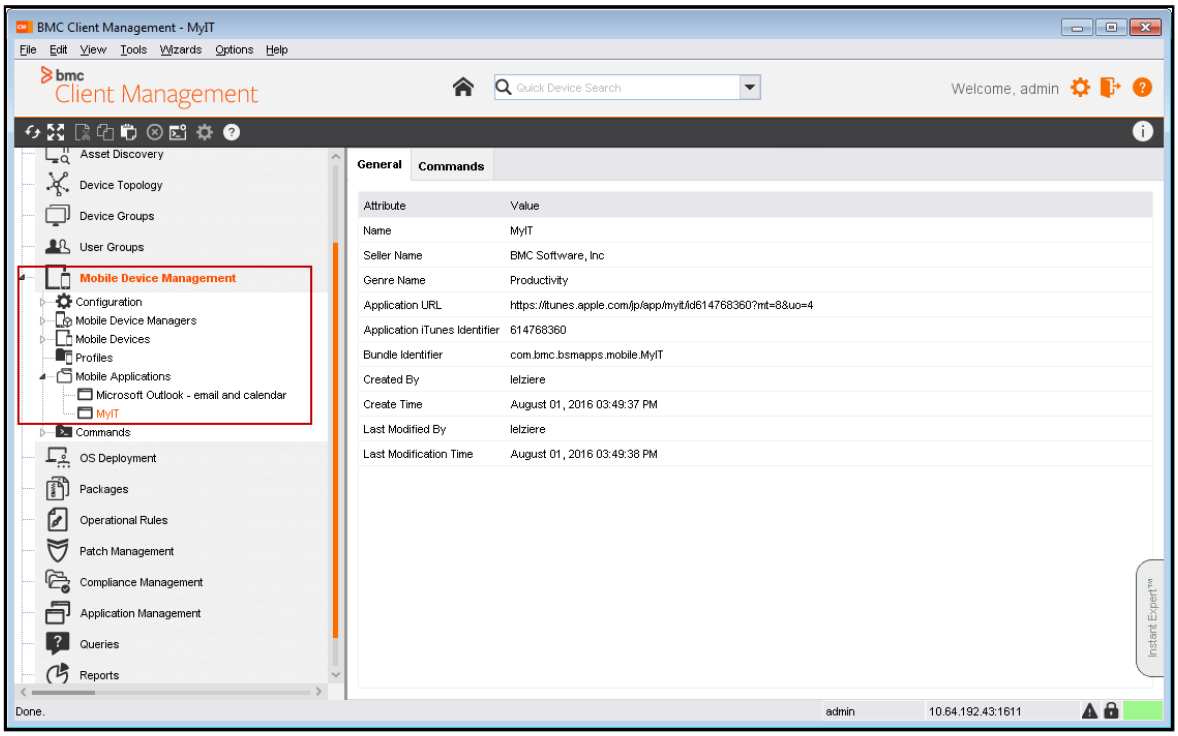
In BMC Client Management, the IT administrators can create and maintain a repository of mobile applications that they need to install on managed iOS mobile devices and remotely install them on the target mobile devices using mobile commands.

The following BMC Client Management video (3:14 min) provides information about how to create an application list and install applications on mobile devices:

https://youtu.be/6nmSMC9XaAw

Using different commands, you can install one mobile application on different target mobile devices. For example, you can add the BMC MyIT application to the mobile applications list. You can then create and assign two separate mobile commands to install BMC MyIT application on the mobile devices used by the marketing team and by the sales team.

The following screenshot shows an example of the mobile application list and the **General** tab of an application:



Perform the following tasks to add a mobile application to the mobile application list and install them on the target mobile devices:

- To search and add an application to the Mobile Applications list
- To install an application from the Mobile Applications list to a target mobile device

To search and add an application to the Mobile Applications list

1. In the left pane, select **Mobile Device Management**.
2. Right-click **Mobile Applications**, and select **Create Mobile Application** .

> **Tip**
>
> You can create multiple folders under **Mobile Applications** to organize your mobile applications.

3. In the Online Mobile Application Search window, enter the name of the application that you want to add to the application list, and click **Search** .
   You can limit the number of returned results. By default, 50 results are returned. The search result displays the name of the application with other information such as seller, price, size, genre, application URL, application iTunes identifier, and bundle identifier.

> **Note**

You can install an application to the target mobile device by directly using application iTunes identifier or the bundle identifier. For more information, see Performing remote operations on managed mobile devices.

4. Select the application that you want to add to the **Mobile Applications** list, and click **OK** .
   The application is added to the Mobile Application list. You are also presented with an option to create a command to install the application to the target mobile devices. For more information, see To install an application from the Mobile Applications list to a target mobile device.

To install an application from the Mobile Applications list to a target mobile device

1. In the left pane, right-click ***mobileApplicationName*** , and select **Create Mobile Command** .
   The **Command Wizard** is displayed.
2. In the Command page, enter the details as required, and click **Next** .
   By default, the application name, command type (Install Application), and priority (Medium) are populated.
3. In the Command Options page, click **Next**.
   The application name is selected by default.
4. In the Command Assignment page, assign the command to devices, device groups, users, or user groups, and click **Finish**.
   The command is assigned to the target mobile devices. When the command is executed on the mobile device:
   - If the mobile device is supervised, the application is automatically installed on the mobile device.
   - If the mobile device is not supervised, the user receives a notification to install the application. The user can either install the application or ignore the notification.

Tip

If your mobile device is supervised, a message is displayed below the screen lock. For example, *This iPad is managed by your organization.*

You can view all the commands that were created for an application in the **Commands** tab. For more information about commands, see Performing remote operations on managed mobile devices.

Managing configuration profiles for managed mobile devices

Using configuration profiles, the IT administrators can remotely configure managed iOS mobile devices.

The following BMC Client Management video (3:34 min) provides information about managing profiles:

https://youtu.be/ptV9DESMhNI

A configuration profile is a group of settings, which are known as *payloads*. For example, a Wi-Fi payload is a group of settings required to configure a Wi-Fi connection. Similarly, the Mail payload is a group of settings required to configure an email account on a managed mobile device.

In one configuration profile, you can configure multiple payloads including passcode, restrictions, Wi-Fi, and so on. The Passcode and Restrictions payloads can have only one instance each; however, all other payloads can have multiple instances. For example, in one configuration profile, you can configure two instances of Wi-Fi to set two separate Wi-Fi connections.

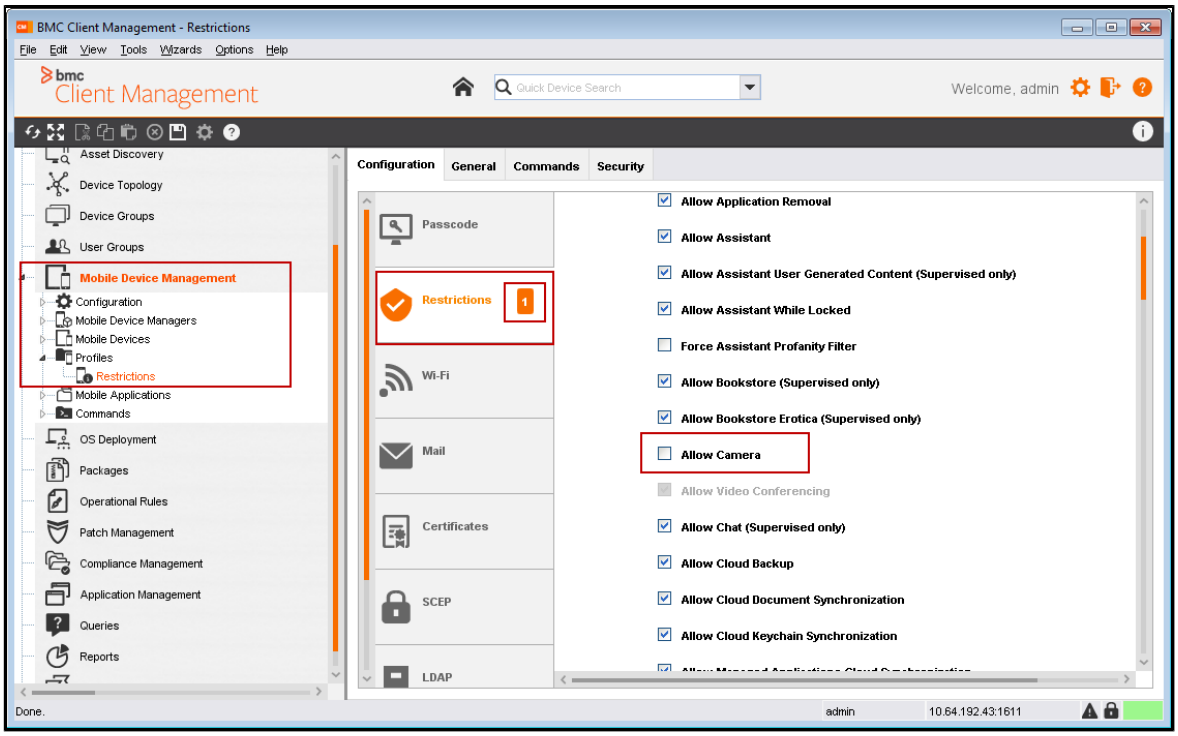
One payload can be consumed by another payload. For example, the signing certificate configured in the Certificates payload can be used in the Mails payload.

BMC Client Management supports the following payloads:

Payload	Description
Passcode	Configure passcode on device.
Restrictions	Configure restrictions on device in terms of using applications, mobile device functionality and media content.
Wi-Fi	Configure Wi-fi access with necessary authentication information.
Mail	Configure mails on device and define settings for POP and IMAP email accounts.
Certificates	Configure multiple certificates on device.
SCEP	Configure SCEP and define settings to obtain certificates from SCEP servers.
LDAP	Configure LDAP parameters.
Web Clips	Configure web clips.

The configuration profiles are installed to target mobile devices using mobile commands. Using different commands, you can install one configuration profile on different target mobile devices. For example, you can create a security configuration profile with restrictions. You can then create and assign two separate mobile commands to install the security configuration profile on the mobile devices used by the development team and by the quality team.

The following screenshot shows the list of configuration profiles, payloads, the number of instances of a payload, and configuration parameters for the restriction payload:



To create the configuration profiles and install them on the mobile devices, see the following procedures:

- To create and configure a configuration profile
- To install a configuration profile on the target mobile devices

To create and configure a configuration profile

1. In the left pane, select **Mobile Device Management.**
2. Right-click **Profiles**, and select **Create Mobile Profile** .

> **Tip**
>
> You can create multiple folders under **Profiles** to organize your mobile profiles.

3. In the **Properties** dialog box, specify the configuration profile name and other details, and click **OK**.
4. (*Optional*) You can specify the date and time to automatically remove a profile by entering values in **Date to automatically remove the profile**.
5. In the left pane, select the newly created profile.
6. In the right pane, under the **Configuration** tab, configure the payloads.
   The number next to a payload indicates the number of instances of that particular payload.

7. Click **Save** in the toolbar to save the profile.
   Next, you can assign the profile to the target mobile devices. For more information, see To install a configuration profile on the target mobile devices.

To install a configuration profile on the target mobile devices

You can assign commands to push a mobile configuration profile to target devices, device groups, users, or user groups.

1. In the left pane, select **Mobile Device Management** > **Profiles**.
2. Right-click ***profileName*** and select **Create Mobile Command** .
   The **Command Wizard** is displayed.
3. In the Command page, enter the details as required and click **Next**.
   By default, the profile name, command type (Install Configuration profile), and priority (Medium) are populated.
4. In the Command Options page, click **Next**.
   The profile name is selected by default.
5. In the Command Assignment page, assign the command to either devices, device groups, users, or user groups and click **Finish**.
   The command is assigned to the target mobile devices. When the command is executed, the configurations are set in the target mobile devices. You can view all the commands created for a profile in the **Commands** tab. For more information on commands, see Performing remote operations on managed mobile devices.

Performing remote operations on managed mobile devices

The IT administrators can remotely perform the on the managed iOS mobile devices.

The following BMC Client Management video (2:56 min) provides information about performing remote operations using commands:

https://youtu.be/AHHYgxuwOdU

Using commands, you can remotely perform the following operations on mobile devices:

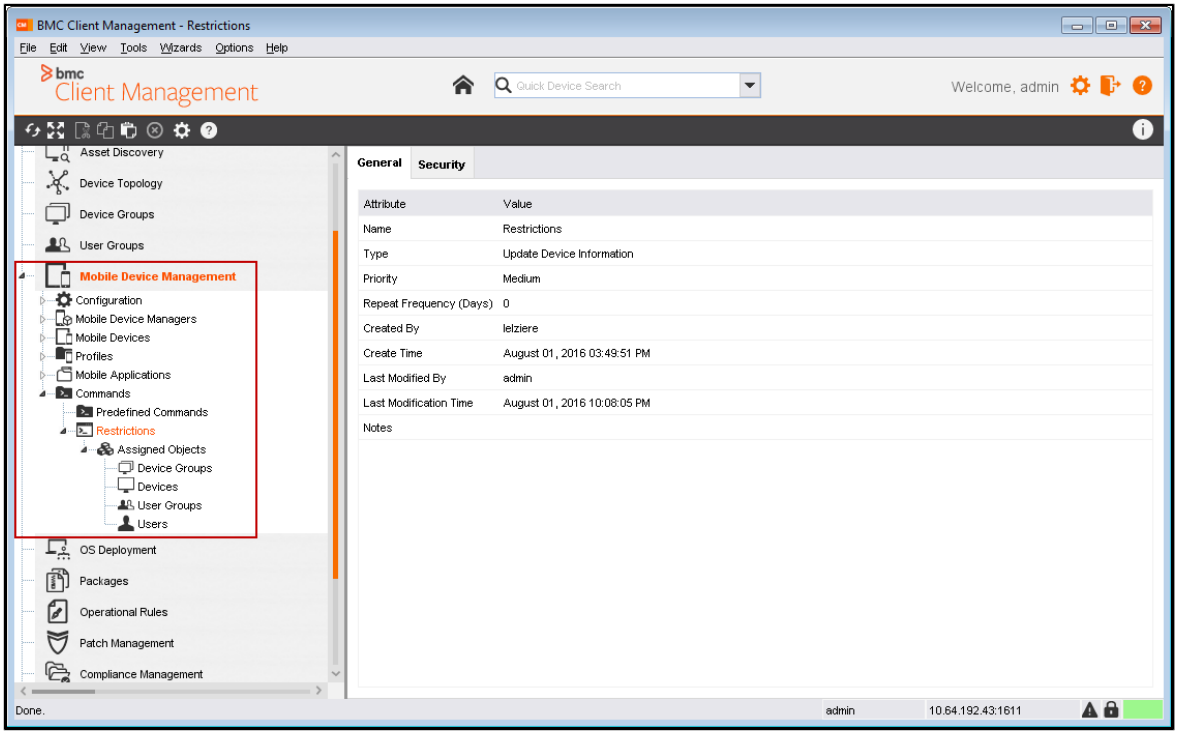
- Update information about the device, security, restrictions, applications, certificates, and profiles (collect inventory)
- Install or remove configuration profiles (manage profiles)
- Install or remove managed applications (manage applications)
- Lock or wipe (factory reset) mobile device (data security)
- Clear passcode (data security)

Using the **Repeat Frequency** option in the commands, you can:

- Collect inventories at regular intervals. For example, you might want to run a command to collect security inventory every seven days, installed applications inventory every 15 days, and device information inventory every 30 days.
- Ensure that users have important applications installed all the time. For example, you can create a command to install Outlook and set the Repeat Frequency option to one day. So, even if the user removes Outlook application from the mobile device, the command installs it again the next day.

You can also use commands to ensure that the enterprise data stored on the mobile device is accessed only by the authorized user. If the mobile device is stolen or misplaced, you use the Wipe or Lock command to ensure that your data is not accessible to unauthorized users. If the user forgets the passcode, you can remotely clear the passcode allowing seamless data access to your users.

The following screenshot shows the list of commands, the objects assigned to the command, and its **General** tab:



The following topics are provided:

- To create and assign a mobile command
- To view the status of a mobile command
- To use a direct access command to clear a pass code or to wipe or lock a mobile device
- To collect inventories
- To install an application that is not in your Mobile Applications list
- To remove an application by using a command
- Examples of remote operations

To create and assign a mobile command

1. In the left pane, select **Mobile Device Management.**
2. Right-click **Commands**, and select **Create Mobile Command** .
   The **Command Wizard** window is displayed.

> **Tip**
>
> You can create multiple folders under **Commands** to organize your mobile commands.

3. In the Command page, specify the details as required, and click **Next**.
   The Command Options page is displayed. Depending on the command type on the preceding page, different command options are displayed. For a detailed list of available command options, see Examples of remote operations.

> **Note**
>
> If the selected command type is an update command (**Update xxxx**), **Clear Passcode**, or **Wipe Mobile Device**, the Command Options page is not available and the Command Assignment page is displayed.

> The license could not be verified: License Certificate has expired!

4. Set the command options, and click **Next**.
   The Command Assignment page is displayed.
5. Assign the command to the target devices, device groups, users, or user groups, and click **Finish**.
   The command is created and assigned to the target mobile devices.

To view the status of a mobile command

After you assign the command to the target mobile devices, you can view the command status by navigating to the following locations in the left pane:

- **Mobile Device Management > Commands > *mobileCommandName* > Assigned Objects > Devices**
- **Mobile Device Management > Mobile Devices > Managed Mobile Devices > *mobileDeviceName* > Assigned Objects > Commands**

In the right pane, all of the commands that were assigned to the mobile device are displayed with their status.

- If the command is assigned to the mobile device for the first time, the sequence of the command status is as follows:
  Assignment Waiting > **Assignment Notified** > **Assignment Sent** > **Executed/Execution Failed/ Not Notified**.
- If the command is already assigned to the mobile device and the user initiates command reassignment, the sequence of the command status is as follows:
  Reassignment waiting > **Update notified** > **Update sent** > **Executed/Execution Failed/Not Notified**.

The following table describes different command status:

Command Status	Description
Assignment Waiting (Reassignment Waiting)	The command was assigned (or reassigned) to the target mobile device in the console, but the mobile device manager is yet to assign (or reassign) the command to the target mobile device.
Assignment Notified (Update Notified)	The command (or command update) was assigned to the target mobile device in the console and the mobile device manager has notified the Apple notification server about the command assignment. The Apple notification server will send the notification to the mobile device. There can be a delay in sending the command from the Apple notification server to target mobile device due to connectivity and other dependencies.
Assignment Sent (Update Sent)	The command (or command update) was sent to the target mobile device.
Executed	The command (or command update) was run on the target mobile device.
Execution Failed	The command (or command update) on the target mobile device failed. You can view more information in the **Error Details** column.
Not notified	The command (or command update) was sent to the target mobile device, but the target mobile device has not sent the status back to the mobile device manager.

To use a direct access command to clear a pass code or to wipe or lock a mobile device

The following are security-related commands that are accessible as direct access options for managed mobile devices:

- Clear Passcode
- Wipe Mobile Device
- Lock Mobile Device

Important

If you are using the **Wipe Mobile Device** command, the user is not informed about the mobile device being reset to factory settings.

1. Right-click the mobile device to which you want to assign the command, and select **Direct Access Tools**.
2. Select the command you want to use.
3. Click **OK** to confirm.
   The command is sent to the target mobile device.

To collect inventories

Depending on the type of the inventory you want to collect, you can use the following command types:

- Update Device Information
- Update Security Information
- Update Device Restrictions
- Update Installed Applications
- Update Configuration Profiles
- Update Certificates

When a mobile device is audited (using the **Audit Now** option), the following three mobile commands are assigned to the mobile device:

- Update Device Information
- Update Device Security
- Update Installed Applications

You can also set a command to regularly collect inventory using the **Repeat Frequency** option. This is helpful if regular inventory audits are part of your organization's compliance policy or a statutory requirement.

To install an application that is not in your Mobile Applications list

Using commands, you can install mobile applications on the target mobile devices. For more information about installing application added to the **Mobile Applications** list, see To install an application from the Mobile Applications list to a target mobile device.

To install applications that are not listed in the **Mobile Applications** list, you need to have either of the following identifiers:

- Application bundle identifier
- Application iTunes identifier

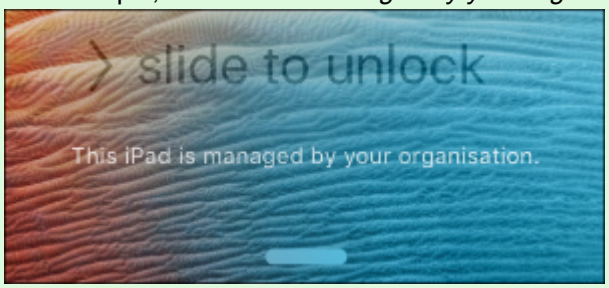
For more information about finding these numbers, see To search and add an application to the Mobile Applications list.

For example, you may get a request from users to have a public email service client (such as Gmail) installed on their managed mobile device. You may not have this application in your mobile application list, as this is not either an approved application or a restricted application as per your organization's policy.

1. Create a command using the command type **Install Application**. For more information, see To create and assign a mobile command.
2. On the Command Options page, in the **Application to install** list, select either the **Application bundle identifier** or **Application iTunes identifier** option, and specify the corresponding value.
3. Assign the command to the target mobile devices.
   When the command is executed on the mobile device:
   - If the mobile device is supervised, the application is installed on the target mobile device.
   - If the mobile device is not supervised, the user receives a notification to install the application. The user can either install the application or ignore the notification.

Tip

If your mobile device is supervised, a message is displayed below the screen lock. For example, *This iPad is managed by your organization.*



To remove an application by using a command

You can also remove applications using commands. For example, when an employee, who had enrolled a personal mobile device, leaves the organization. You had installed business-specific applications (such as BMC MyIT) on the employee's mobile device. As the employee is leaving the organization, you want to remove those applications from the employee's mobile device.

Note

You can remove only those applications that were installed by using mobile device management. You cannot remove applications that were installed by the user.

1. Create a command using the command type Remove Application. For more information, see To create and assign a mobile command.

2. On the the Command Options page, in the **Application to remove** list, select one of the following options:
   - If the application to remove is listed under Mobile Applications, select the **Application from list** option, and then browse and select the application that you want to remove.
   - If the application to remove is not listed in under Mobile Applications, select the **Select bundle identifier** option, and specify the value. For more information about finding the bundle identifier, see To search and add an application to the Mobile Applications list.
3. Assign the command to the target mobile devices.
   The application is removed when the command is run on the target mobile device.

Examples of remote operations

The following table lists the examples of remote operations that you can perform, the type of mobile commands that you can use, and available command options:

Remote operation example	Command type	Command options
The company policy requires a compliance audit on the seventh day of each month. The inventory must be collected at least once a month.	Update Device Information	Not available
	Update Security Information	
	Update Restriction Information	
	Update Installed Applications	
	Update Configuration Profiles	
	Update Certificates	
Each managed mobile device must at all times be configured with settings in a company-defined profile.	Install Configuration Profile	Select the mobile profile to be installed.
The user is going for a vacation. The configuration profile, which enforces restrictions on the mobile device, needs to be removed from the user's managed mobile device.	Remove Configuration Profile	Select the mobile profile to be removed.
The user has forgotten the passcode. The passcode of the managed mobile device needs to be removed.	Clear Passcode	Not available
The user's managed mobile device is stolen. The sensitive enterprise data on the mobile device must be removed.	Wipe Mobile Device	Not available

Remote operation example	Command type	Command options
The user has misplaced the mobile device within the office. The mobile device needs to be locked to avoid unauthorized data access by other employees.	Lock Mobile Device	• Message • Phone number
There is a list of Managed Applications set in BMC Client Management. These applications must be installed on all managed mobile devices.	Install Application	• Application to install • Application from list: Select the application from the list. • Remove on unroll: Select the check box to remove application when the user withdraws enrollment. • Prevent backup: Select the check box to prevent application data back up.

The user has requested to have some additional applications installed. These applications are not in the Managed Applications list.	Install Application	• Application to install
		  • Application bundle identifier: Specify the bundle identifier, or
		  • Application iTune identifier: Specify the iTune identifier.
		• Remove on unroll: Select the check box to remove application when the user withdraws enrollment.
		• Prevent backup: Select the check box to prevent application data back up.

The user no longer requires an application that was installed by using mobile commands.	Remove application	Application to remove • Application from list: Select the application from the list. • Application bundle identifier: Specify the bundle identifier.

Managing applications purchased through the Apple Volume Purchase Program

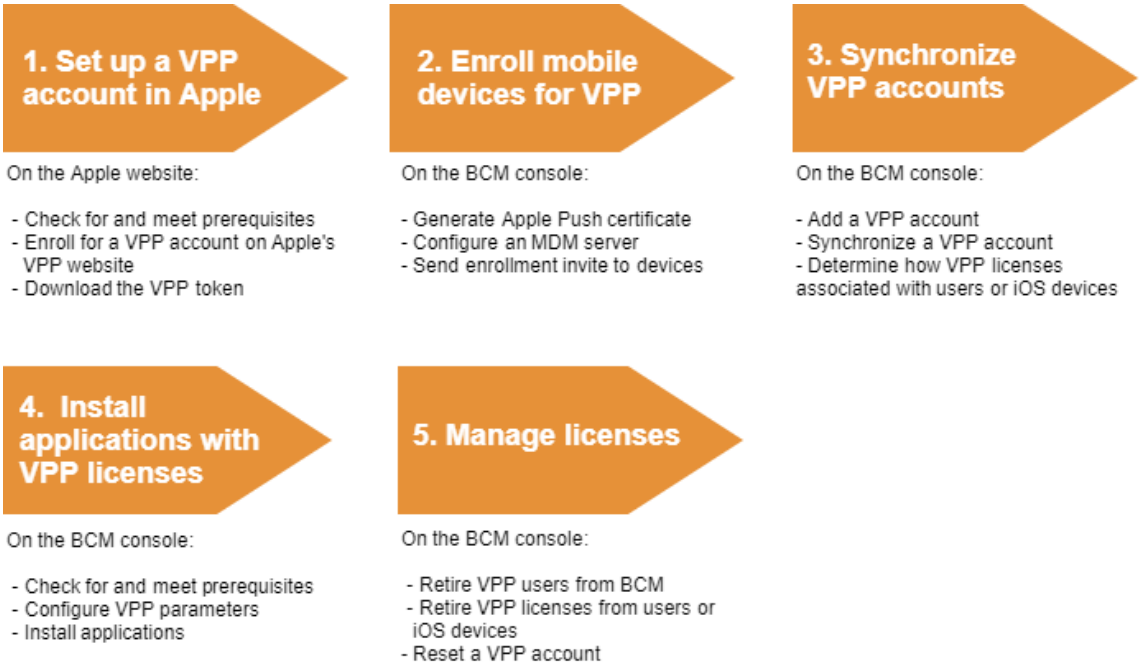
Volume Purchase Program (VPP) is a license management capability to manage applications installed on Apple iOS mobile devices, including iPhones, iPads, and iPods.

As an organization, if you decide to purchase a large volume of Apple applications for employees, the VPP functionality helps you license and distribute applications (assets) on iOS devices while allowing you to retain complete ownership of assets.

With iOS 9, new features enable more efficient distribution of VPP apps across your organization.

- Device-based app distribution: Businesses can gain an advantage of a Mobile Device Manager (MDM) solution with VPP to distribute and assign apps directly to a device (iOS 9.3 or later)—no Apple ID is required. This capability saves several steps in the initial rollout, making your deployment significantly easier and faster while giving you full control over managed devices and content.
- Multinational support: VPP apps can be assigned to devices or users in any country where the app is available, enabling multinational distribution for enterprises.

The following process diagram explains the end-to-end process from purchasing applications through Apple's VPP program to managing applications in BMC Client Management.



This BMC Client Management video describes how to manage applications purchased from the Apple Volume Purchase Program.

Use the following topics to manage applications that are licensed by the Apple Volume Purchase Program.

- Supported account types
- Setting up a VPP account with Apple
- Apple Volume Purchase Program integration with BMC Client Management
- Enrolling mobile devices for VPP
- Synchronizing VPP accounts in BMC Client Management

- Installing applications using VPP licenses
- Managing VPP licenses
- Troubleshooting VPP

Supported account types

BMC Client Management only supports business accounts.

BMC Client Management does not support:

- macOS applications
- iBooks purchased for bulk distribution
- Education accounts are not supported

Considerations related to VPP applications

- VPP applications that are directly licensed to a device must be running iOS version 9.3 or later.
- VPP applications that are licensed to BMC Client Management users can use devices that run any iOS version.

Setting up a VPP account with Apple

The following topics are covered.

- Before you begin
- To enroll for a VPP account
- To purchase applications through Volume Purchase Program
- To download the VPP token from the VPP website
- Where to go from here

Before you begin

- You must have a valid business email address to enroll for a VPP account.
- Your organization must have a valid D-U-N-S number. The D-U-N-S number is a unique nine-digit number that identifies business entities on a location-specific basis. Apple does not allow individuals to sign up for a VPP account.
- You can get VPP credit from Apple or use an Apple reseller or Credit card to purchase VPP applications.
- Provision an MDM server. One or more Mobile Device Managers (MDM) can help to streamline distribution of content purchased through VPP for mobile users.

To enroll for a VPP account

1. Log in to the Apple VPP website.
2. On the Volume Purchase Plan page, click **Enroll**.
3. Enter your details and click **Next**.
4. Complete your deployment development enrollment program.
   You are enrolled for a VPP account.

To purchase applications through Volume Purchase Program

After you enroll for a VPP account, you can purchase applications for your organization.

1. Log in to the Apple VPP website.
2. Search for available iOS apps in iTunes.
3. Enter your purchase credentials to process bulk purchasing of VPP applications.

To download the VPP token from the VPP website

The VPP token is required to authenticate the VPP account in BMC Client Management. After the VPP account is set up in BMC Client Management, the applications purchased through Apple are synchronized in BMC Client Management. When a VPP application is installed on a device or for a user, VPP licenses are used. The token also ensures that the license count is synchronized in Apple and BMC Client Management.

After you download the VPP token from the Apple website, BCM encrypts the token to enhance security as the token contains important information such as authentication keys.

To download the VPP token that needs to be imported to the MDM server.

1. Log in to the Apple website with a valid VPP account.
2. Download the VPP token associated with the managed distribution.

Where to go from here

After you set up your VPP account with Apple, enroll your mobile devices for VPP in BCM. In the BCM console, view a new node to configure VPP.

Apple Volume Purchase Program integration with BMC Client Management

Enrolling mobile devices for VPP

Synchronizing VPP accounts in BMC Client Management

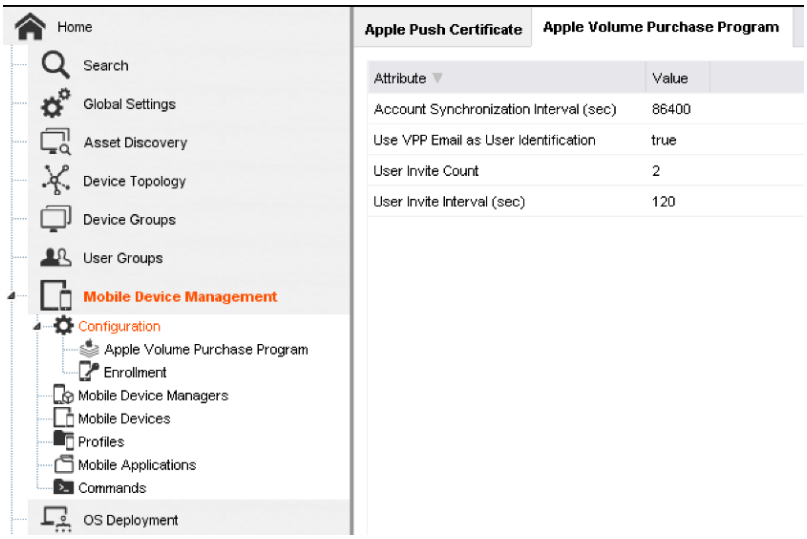
Installing applications using VPP licenses

Managing VPP licenses

Apple Volume Purchase Program integration with BMC Client Management

The Apple VPP is integrated with BMC Client Management. You need to configure a Mobile Device Manager solution to distribute applications purchased through VPP. The assets (applications) that are purchased through VPP are synchronized in BMC Client Management when the VPP account is registered with BMC Client Management.

The **Mobile Device Management** node in the BMC Client Management console enables you to perform tasks to distribute VPP assets and licenses to BMC Client Management users and iOS devices.



Where to go from here

On the BMC Client Management console, you must begin by enrolling mobile devices for VPP, before synchronizing VPP accounts in BMC Client Management.

Enrolling mobile devices for VPP
Synchronizing VPP accounts in BCM
Installing applications with VPP licenses
Managing VPP Licenses

Enrolling mobile devices for VPP

The following topics are covered in this section.

- Configuring a Mobile Device Manager in BCM
- Generating an Apple push certificate
- Enrolling mobile devices
- Where to go from here

Configuring a Mobile Device Manager in BCM

To distribute VPP assets and licenses, you need to configure a Mobile Device Manager (MDM) server in the BCM network.

1. On the BMC Client Management console, select **Mobile Device Management** > **Mobile Device Managers**.
2. Right-click **Mobile Device Managers** > Add Device.
3. On the **Add a new Mobile Device Manager** window, select the mobile device manager.
   The new mobile device manager is added to the console.

Generating an Apple push certificate

> ⚠ Note: Before you generate an **Apple push certificate**, ensure that an MDM server is available in BMC Client Management.

The Apple push certificate is required to manage iOS devices through the BMC Client Management console.

1. On the BMC Client Management console, select **Mobile Device Management** > **Configuration** > **Apple Push Certificate**.
2. Right-click **Apple Push Certificate** > **Prepare Certificate**.
3. On the **Create CSR Certificate** window, enter the appropriate values.
4. Click **Generate CSR Certificate** and save the certificate to a secure disk or system.
5. Click **Next**.
6. In the **Apple Manual Procedure** window, click **Apple Push Certificate**.
7. Sign in to the Apple portal website using your Apple account credentials.
8. Upload the CSR certificate to the Apple portal.
   Apple manually creates the final push certificate by using the uploaded certificate.
9. Click **Download** to download the final push certificate to a secure disk or system.
10. Click **Next**.
11. On the **Import Apple Push Certificate**, click **Browse** to select the final push certificate.
    The Apple push certificate is installed in BMC Client Management.

Enrolling mobile devices

You must enroll iOS mobile devices to the MDM server, because only then can BMC Client Management distribute and install VPP applications to these mobile devices. You can choose to synchronize a user group registered with the Active Directory or manually enroll users individually for VPP applications.

1. On the BMC Client Management console, go to **Mobile Device Management** > **Configuration** > **Enrollment**.

2. Add email domains, users, or user groups.
    a. In the **Authorized Email Domains** tab, right-click anywhere in the tab and click **Add Email Domain** to add an email domain.
    b. In the **Authorized Users** tab, right-click anywhere in the tab and click **Add User** to add a user to the authorized list.
    c. In the **Authorized User Groups** tab, right-click anywhere in the tab and click **Add User Group** to add a list of users to the authorized list.
    d. In the **Customization** tab, click **Browse** to select a new logo, customize it and apply that logo on the mobile device enrollment page that is sent with the enrollment email.
3. In the **Authorized Users** tab, right-click users, and **Send Enrollment Email** to invite mobile users to self-register for VPP applications.
4. In the **Authorized User Groups** tab, right-click user groups, and **Send Enrollment Email** to invite all mobile users in a group to self-register for VPP applications.

Where to go from here

After you enroll mobile devices for VPP, you can then synchronize the assets purchased through VPP in BMC Client Management.

Synchronizing VPP accounts in BCM

Installing applications with VPP licenses

Managing VPP Licenses

Troubleshooting

Synchronizing VPP accounts in BMC Client Management

You have configured an MDM server, generated the Apple push certificate and enrolled mobile devices to the MDM server. After enrolling mobile devices to the MDM server, you can synchronize VPP accounts in BMC Client Management to populate all the purchased VPP applications and licenses details. You need to synchronize the VPP account before you can install applications with VPP licenses.

The following topics are covered:

Synchronizing VPP accounts

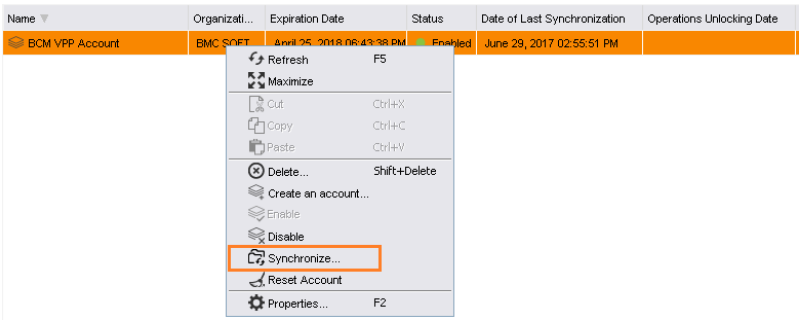
You must synchronize your VPP account in BMC Client Management to populate the latest applications purchased from the Apple website. Because the synchronization process is incremental, time it takes to synchronize VPP assets depends on whether you configure the VPP account for manual or a scheduled synchronization.

The following entity values are updated after each synchronization task:

- VPP Assets - These are the applications that are purchased from the Apple website.
- VPP Users - The VPP user or users who are also registered in the MDM server and are identified as BMC Client Management users.
- VPP Licenses - These licenses are only those associated with an iOS device or a VPP user.

Manually synchronizing the VPP account

1. From **Mobile Device Management,** select **Configuration > Apple Volume Purchase Program**.
2. Click **Synchronize.**



Automatically synchronizing the VPP account

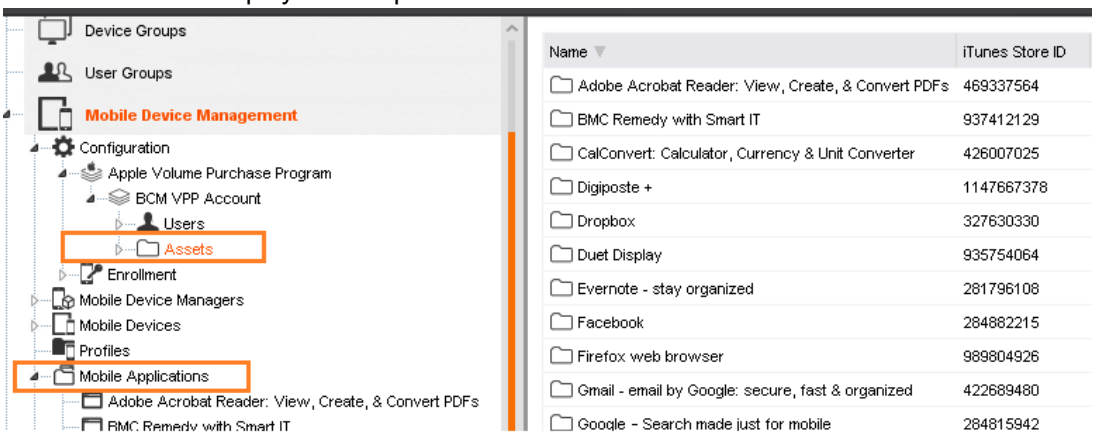
1. From the **Mobile Device Management,** select **Configuration > Apple Volume Purchase Program**.
2. Define the **Account Synchronization Interval (sec)** parameter.

> If this parameter is set to zero, you cannot enable the VPP account for automatic synchronization. You need to manually synchronize the account.
>
> Because data is synchronized incrementally, BMC recommends that you configure this parameter to prevent too many synchronization requests in a day. The manual synchronization action can be used if required, after purchasing additional assets.

Viewing the purchased VPP assets in BMC Client Management

After you synchronize the VPP account in BMC Client Management, you can view the VPP assets that are populated under the **Assets** node (under the VPP account). The same assets are also populated under the **Mobile Applications** node. It is required because applications can be installed on devices or for users directly from the **Mobile Applications** node.

1. From **Mobile Device Management,** select **Configuration > Apple Volume Purchase Program > *BCM VPP Account* >** Assets.
   The **Assets** node displays all the purchased VPP assets.



VPP licenses associated with users or iOS devices

VPP license can be associated in the following ways:

- Users: Licenses can be associated to the VPP user ID and VPP user iTunes account. This association allows a user to install the application on multiple iOS devices that are owned by the user and connected to a registered iTunes account.
- Devices: Licenses can be associated to the VPP user ID and iOS device serial number.

> Note:
>
> - A license associated with a single user can be installed on multiple iOS devices that are owned by that user. So, VPP distributes a single licence to a BMC Client Management user irrespective of the number of devices enrolled under that user.
> - A license associated with a single device can be only be used on that device.

The MDM solution ensures that the VPP assets are associated with all the user license and device license. VPP licenses are purchased from Apple. The licenses belong to one VPP account and are referenced by an iTunes application. The process of associating licenses is the key capability of the VPP. As an organization, it gives you complete ownership of licenses regardless of where they are distributed within your enterprise.

To view VPP licenses associated with users or iOS devices

1. From the **Mobile Device Management** node, select **Configuration** > **Apple Volume Purchase Program** > ***BCM VPP Account*** > **Assets** > ***Asset1.***
2. Open **User license** to verify that a VPP license is associated with that user.
3. Go to the **Device license** to verify that a VPP license is associated with that device.

When a VPP license is associated with a user, then BMC Client Management can license all the iOS devices enrolled with that user using that single license. So, multiple iOS devices can use the same license when a VPP license is assciated with a user.

Where to go from here

After you synchronize the assets purchased through VPP in BMC Client Management, you can install applications by using VPP licenses.

Installing applications with VPP licenses

Managing VPP Licenses

Troubleshooting

Installing applications using VPP licenses

The following topics are covered in this section.

- Prerequisites to configure VPP accounts
- Configuring VPP parameters in BMC Client Management
- Installing applications
- Understanding the installation status of applications
- Where to go from here

Prerequisites to configure VPP accounts

The prerequisites for associating a license to a user are as follows:

- The VPP user must be associated with an iTunes account. This iTunes account must not be already associated with a different VPP user.
- The VPP user can then be associated with an asset VPP license.

- The connected iTunes account must not be already associated with another VPP license related to this asset.
- At least one license must be available and related to this asset.

> ⚠ BMC Client Management verifies that the VPP user exists both in the MDM application and on the VPP Apple servers.

The prerequisites for associating a license with an iOS device are as follows:

- The iOS device must be enrolled in the MDM system.
- The iOS device must be running an iOS version 9.3 or later.
- The VPP asset must support the associated device.
- The device serial number can then be associated with an asset VPP license.
  - This device serial number must not be already associated with another VPP license related to this asset.
  - At least one license must be available and related to this asset.

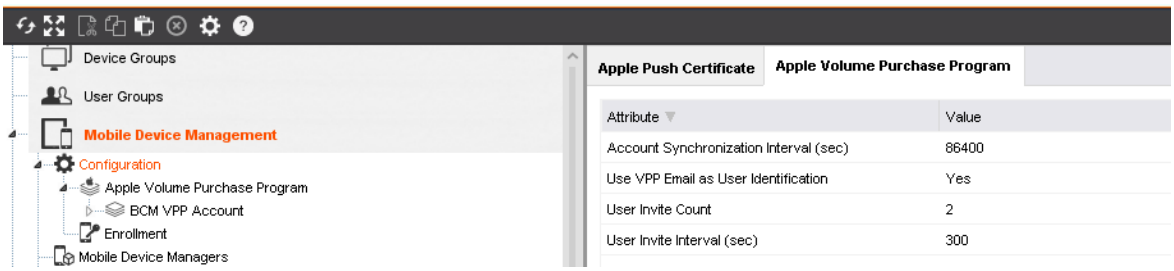
Configuring VPP parameters in BMC Client Management

After you add a VPP account in BMC Client Management, you can configure the following parameters:

1. Go to **Mobile Device Management** > **Configuration**.

2. Enter values for these parameters.

Parameter	Value
Account Synchronization Interval (sec)	Select time interval after which BMC Client Management synchronizes the VPP account.
Use VPP Email as User Identification	Select this box if you want to associate the VPP users with the BMC Client Management users who are using the VPP email address provided during the synchronization process. The email address must be the same for every user in BMC Client Management and VPP and it must be unique.
User Invite Count	Select the maximum count of VPP user invitations.
User Invite Interval (sec)	Select this time interval after which an invited VPP user is synchronized in BMC Client Management. If you set to 0, synchronization is deactivated.



Installing applications

> VPP licenses must be already associated with users or iOS devices before you install applications with VPP licenses.

After synchronizing the VPP account in BMC Client Management and enrolling mobile devices, you can install applications on the enrolled mobile devices.

1. On the BMC Client Management console, select **Mobile Device Management** > **Commands**.
2. Right-click **Commands** > **Create Mobile Command**.
3. In the Command wizard, enter the command name.
4. Select **Install Application**.
5. Enter values in the other fields.
6. Click **Next**.
7. In the Command Options window, complete the following steps:
    a. In the **Application to install** field, select the asset to be installed on the device.
    b. In the **Acquire a license from VPP account** field, select the VPP account that licenses the application
    c. If the application should be removed from the mobile device after the mobile device is no longer enrolled with BMC Client Management, select the **Remove on enrollment withdrawal** checkbox.
    d. If the application need not be backed up, select the **Prevent backup** checkbox.
8. If you selected the Application iTunes store, enter the iTunes Store ID.
9. Click **Next**.
10. In the **Command Assignment** window, you can select either device, device group or users.
    a. User: The selected application is installed on all mobile devices enrolled for this user.
    b. Devices or Device group: The selected application is installed only on the selected device or device group.
11. Click **Finish**.
    The application is installed on the selected devices or users. The **Commands** node is populated with the installed application and the assigned user or device licenses.

> The above procedure can also be performed from the **Mobile Device Management** node, select **Mobile Applications** node and proceed to install VPP applications.

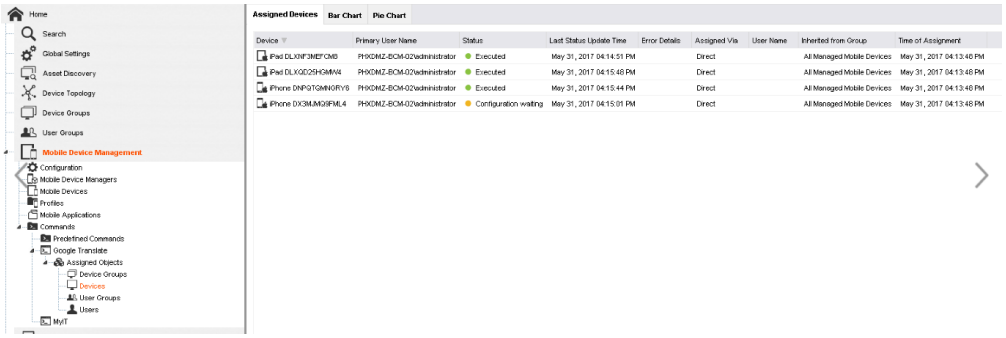
Understanding the installation status of applications

> If the install command is executed for a BMC Client Management user who is not associated with a VPP account, the BMC Client Management user is associated with a VPP user. The BMC Client Management user receives an invitation on the iOS device to connect to an iTunes account.
>
> The BMC Client Management user must connect to an iTunes account for installation to proceed.

To check the status of an installation on the iOS device:

- 1. From the **Mobile Device Management > Command** node.
  The **Status** column displays the current installation status of the application.

Status	Desciption
Configuration Waiting	(Only for users and not for devices) BMC Client Management has initiated the process to associate the BMC Client Management user with a valid VPP user, inviting users to connect to an iTunes account, associating users with licences.
Assign Waiting	BMC Client Management has configured the association of the BMC Client Management user with a VPP user
Update Notified	BMC Client Management has notified the Apple servers (APNS). This infrastructure is responsible for notifying the iOS device about invitation to enroll their mobile devices.
Executed	BMC Client Management successfully installed the application on the device.
Execution Failed	BMC Client Management was unable to install the application on the device.



Where to go from here

To learn more about how to manage VPP licenses, see the following topics:

Managing VPP Licenses

Troubleshooting

Managing VPP licenses

You must know how to retire licenses, retire users and retire VPP accounts based on your organization's needs.

The following topics are covered in this section.

Ensuring multiple VPP users are not connected to the same iTunes account

VPP users need to be associated with an iTunes account so that application licenses can be distributed to BMC Client Management users. After you synchronize a VPP account, the VPP user that is registered or associated with an iTunes account is displayed on the BMC Client Management console. If more than one VPP account is associated with an iTunes account, you cannot install applications using VPP licenses.

1. From **Mobile Device Management** > **Configuration** > **Apple Volume Purchase Program** > ***VPP Account*** > **Users**.
   The Users window displays the VPP users and related account details.
2. Ensure that the **Associated User Count** value is **1**.
3. If the value is more than 1, retire the other VPP users currently associated with the same iTunes account so that only one VPP user is associated with a single iTunes account.
   The **Status** field can take one of the following states.

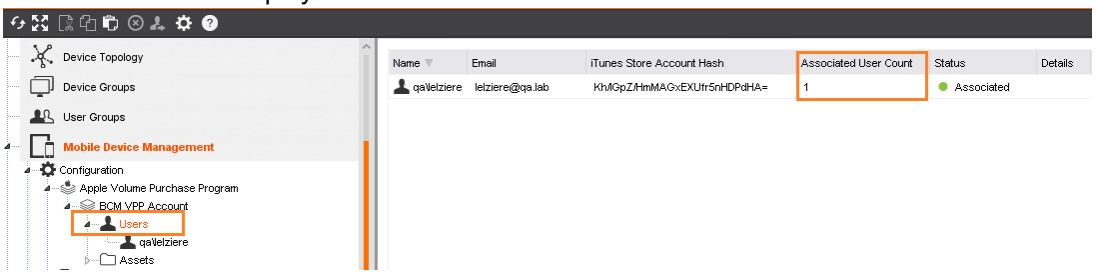
User field	Description
Associated User Count	Displays a number of different VPP users currently associated to the same iTunes account.
User status	Displays one of the following statuses: • **Registered**: The VPP user has been registered but is currently not connected to any iTunes account. • **Associated**: The VPP user has been registered and is currently connected to an iTunes account.

Retiring VPP users from BMC Client Management

To distribute VPP licenses to users or iOS devices, you need to ensure that only one VPP account user is associated with an iTunes account.

As long as **Associated User Count** value is equal to **1**, the asset license associations should succeed. You may need to retire VPP users from BMC Client Management if there are more than one VPP users associated to a single iTunes account.

1. From **Mobile Device Management,** select **Configuration** > **Apple Volume Purchase Program** > ***BCM VPP Account*** > **Users**.
   The Users window displays the VPP users and related account details.

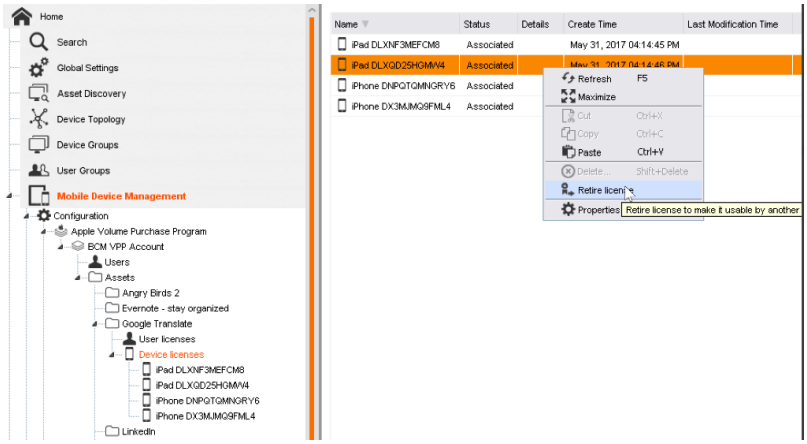


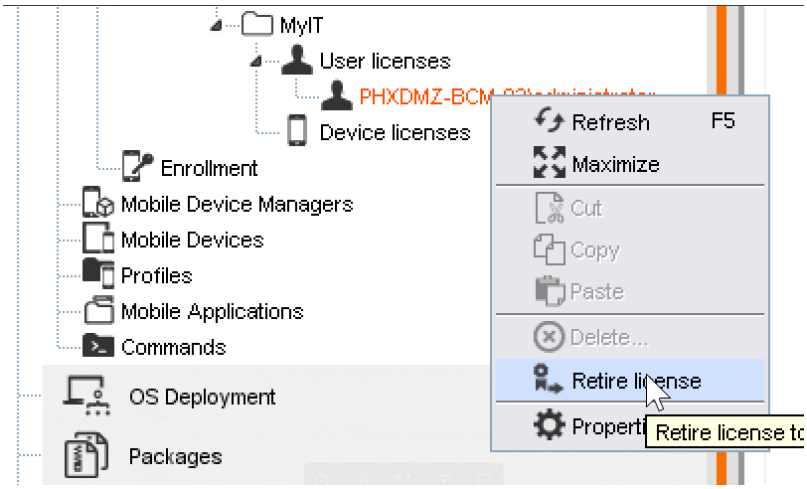
2. If the **Associated User Count** value is more than **1**, you must right-click a VPP user that is associated with the iTunes account and click **Retire**.
3. Continue to retire VPP users all of the VPP users until only one VPP user is associated with the iTunes account.

Retiring VPP licenses from users or iOS devices

When there is a need to reassign licenses between employee and devices, you need to retire existing licenses and re-assign them.

1. From **Mobile Device Management,** select **Configuration** > **Apple Volume Purchase Program** > ***VPP Account*** > **Assets**.
2. Under the application, click **User licenses** or **Device licenses**.
3. In the details window, right-click the license and click **Retire license**.





Resetting a VPP account

A VPP account distributes the licenses to users or iOS devices. BMC Client Management only displays those licenses that are associated with users or iOS devices, there could be licenses that are associated with unknown entities. In such cases, you can reclaim all the licenses distributed through a VPP account by resetting the VPP account.

1. From **Mobile Device Management**, select **Configuration** > **Apple Volume Purchase Program**.
2. In the window, right-click the VPP account, and click **Reset Account**.

Related topic

To know more about how to troubleshoot VPP issues, see the following topics:

Troubleshooting VPP

Troubleshooting VPP

The following table lists the issues and resolutions related to the Volume Purchase Program.

Issue	Description	Resolutions
Cannot associate assets to users	Possibly there are two or more users associated with the same iTunes account. The **Associated User Count** value must not be greater than 1.	1. Run the **Retire User** command to retire the additional users from the associated iTunes account. 2. Run the **Reset account** to reset the account so that one iTunes account is associated only to a single VPP user.
Cannot synchronize VPP assets in BCM	The VPP account is not enabled in BCM.	Check the status of VPP account. 1. Go to **Mobile Device Management** > **Configuration** > **Apple Volume Purchase Program.** 2. Check the **Status** column.

Issue	Description	Resolutions
		3. If the status is **Disabled**, right-click to ensure it is **Enabled.**

Administering

This section provides information and instructions for administrating BMC Client Management.

The following table provides links to the relevant topics based on your goals:

Goal	Instructions
Manage licenses within the network	• Managing licenses • Viewing license information • Importing licenses • Evaluating licenses • Searching and viewing events by license feature
Review and apply security within the network	• Managing security • Understanding security components • Understanding security operations and principles • Managing security profiles • Managing predefined administrator groups • Managing access rights and capabilities for specific cases
Centrally manage and share information about network resources and users	• Managing directory servers • Creating a directory server • Modifying the directory server parameters • Checking connection to the directory server • Deleting a Directory Server
Understand and review system variables that control behavior of the master	• Managing system viriables • Managing security settings • Managing event and logging settings • Managing connection behavior • Managing email settings • Managing default operational rule settings • Managing device menus • Managing packages settings • Managing patch group settings • Managing report settings • Managing software quality metrics • Managing quick search (indexing) settings
Review complete list of consoles currently connected to the master	• Viewing connected consoles

Goal	Instructions
Define the list of relays	• Managing relay list
Use tools for administering BMC Client Management	• Sending an email • Importing Out-of-the-Box objects • Importing report templates • Creating upgrade packages • Cleaning up old packages
Automatically detect an object that is not related to any other object in the database	• Managing lost and found objects
Group clients based on administrator-defined criteria	• Managing queries • Understanding types of queries • Performing basic query tasks • Performing advanced query tasks
Review information about all objects in the database	• Managing reports • Understanding types of reports • Creating a report • Creating a reports folders • Deleting a report or a reports folder • Managing report options • Adding a pie chart to an existing report • Managing subreports • Previewing a report • Scheduling report generation • Assigning a report • Generating a report • Viewing report results • Publishing a report • Setting up email for mailing reports • Managing Report Portal • Importing new report templates • Report creation wizard
Manage events and alerts	• Managing alerts and events • Event log model list • Configuring alert notification
Automatically reboot devices after specific operations	• Managing reboot windows • Creating a new reboot window • Defining reboot window time-slots • Assigning reboot windows • Activating reboot window • Reassigning reboot windows to their targets
Configure automatic update of BMC Client Management as per requirement	• Managing update configurations

Create, modify, or delete attributes of a device object	• Managing device object attributes
Manage asset discovery configurations	• Configuring asset discovery • Managing scan configurations • Adding existing devices as targets • Configuring target lists • Managing asset discovery scanners
Manage agent rollout to install BCM agents on all relays and clients	• Configuring for agent rollout • Preparing the console for rollout • Configuring rollout servers • Configuring post-install activities • Defining the rollout targets
Specify access to the BCM console	• Managing administrators, administrator groups and capabilities • What you have to know about administrators • What you have to know about administrator groups • Capabilities
Configure the local device management module	• Configuring Windows devices for device management
Configure power management module	• Configuring device settings for power management
Configure remote access to the devices	• Configuring remote access
Configure the diagnostic tool module	• Configuring the diagnostic tool
Configure operational rules as per requirements	• Configuring operational rules
Review configuration parameters of different types of inventory	• Setting up inventory • Managing inventory filters • Custom Inventory Object Types
Configure necessary financial data or values for devices in network	• Configuring financial asset management
Configure patching as per requirements	• Configuring patch management
Configure SCAP compliance	• Configuring SCAP compliance

Goal	Instructions
Configure Windows Device Management	• Configuring Windows Device Management
Define compliance constant	• Configuring compliance constants
Configure mobile device management	• Configuring mobile device management
Prevent local user from stopping or starting the agent service	• Locking BMC Client Management Agent service
Customizing the end-user dialogs to provide a personalized experience	• Customizing the end-user dialogs to provide a personalized experience

Managing global settings

In BMC Client Management, there are configurations that globally control the system behavior. You can manage the following global settings:

- Managing lost and found objects
- Managing administrators, administrator groups, and capabilities
- Viewing connected consoles
- Configuring for agent rollout
- Managing administrator credentials centrally for rolling out BCM agents
- Alternatives for rollout
- Managing reboot windows
- Managing directory servers
- Managing licenses
- Managing system variables
- Managing device object attributes
- Managing relay list

Managing lost and found objects

The **Lost and Found** node provides the ability to clear unattached objects of any type that are stored in the database. Unattached database objects are objects that were cut but not pasted, objects that the Autodiscovery could not resolve, and so on, that is, objects that do not have any relation with any parent.

CM has a lost/found intelligence circuit which automatically detects any object that does not relate to any other object in the database, that is, does not have at least one parent. Whenever an existing object becomes unrelated to any parent, the lost/found intelligence sends it to the **Lost and Found** node. This can happen when an object was deleted from a location but never been pasted into another location, or when the exact physical location of the object is unknown.

The table of the **Lost and Found** node provides the following information about the unrelated items:

Information	Description
Name	Displays the name of the unrelated object.
Object Type	The type of the unrelated object, for example Query Folder, Device or Operational Rule.

Adding a new relation

To return an unrelated object to its original or a new location, you can add a new relation:

1. Select the object in the table in the right window pane.
2. Select **Edit > Copy** .
   The object will be removed from the list.
3. Navigate to the new location.
4. Select **Edit > Paste** .
   The object will be pasted into its new locations.

The new relation has successfully been added.

Managing administrators, administrator groups, and capabilities

Security in general for Client Management is defined through a number of different objects and methods, such as authentication/authorization, encryption, privacy and audits. Security for the console in the Client Management is ensured via a number of different methods and objects, one of these are the administrators and administrator groups. Each of these has a capability list which dictates what an administrator can do. The Administrators and Administrator Groups nodes and their Capabilities definitions specify the access to the console in general, that is, who can interrogate or manipulate the database and its information.

Related topics:

- Managing administrators
- Managing administrator groups
- Capabilities

Managing administrators

Administrators and administrator groups are the main objects through which security is enforced in the . Each of these has a capability list which determines what an administrator can do and dictates the access to the Console in general, that is, who can interrogate or manipulate the database and its information.

Every user who might need to log on to the Console must be defined as an administrator in the CM database with a login name and a password. These administrators can then be restricted in their capabilities to specific object types and operations and grouped.

The **Administrators** subnode (**Global Settings > Administrators**) collects all administrators that exist in CM and enables you to manage them. The subnode for each administrator provides specific information about each individual administrator that exists in CM and provides access to its different aspects for modification.

The **Group** tab under each administrator node displays the groups the administrator belongs to. It is structured as follows:

- **Member of** : Displays the list of group names of which the administrator is a member.
- **Share Objects** : Displays if the objects created by the currently selected administrator are to be shared with the other members of the group or groups he belongs to. This means that the other group members have the same access rights to these objects and thus can use them, modify and delete them. The default value is *No* .

At installation time of the master database two administrators will be created automatically:

- **admin** : The admin user is a user with all permissions and capabilities. It cannot be deleted, non of its capabilities or other information (such as static and dynamic objects) can be modified, only its password can be changed. It cannot be added to the Security tab of individual objects either, because it has access to all by default.
- **system** : The system user is the login used by the master server itself for all database actions which it executes automatically, such as those of the identity or autodiscovery module. None of its settings can be modified and you cannot use this login to log on to the Console . The icon of this administrator is dimmed to indicate that it is not editable.

Related topics

- Basic Administrator Tasks
- Advanced administrative tasks
- The Group tab of an administrator

Basic Administrator Tasks

This section provides more first examples on how to work with administrators.

- Creating an Administrator

Creating an Administrator

To create an administrator, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrators** in the left window pane.
3. Select **Edit > Create Administrator** .
   The **Properties** dialog box appears on the screen.
4. Enter the desired data in the respective boxes in the **General** tab.
5. Select the **Authentication** tab and specify the type by which the administrator is to be authenticated when logging on:
   - **Internal** : Selecting this radio button indicates that the administrator will be verified by the master server database using the passwords defined in this box. Therefore enter the password to be used into the **New Password** field. Then confirm it by entering into the second field. For security reasons the passwords will only be displayed in the form of asterisks (*).

     > **Note:**
     >
     > You can only use ISO-Latin characters (all lower case and upper case Western European letters and numbers) even if you are using a Japanese, Greek or Arabic localization.

   - **External** : This option provides the possibility to have the login verified either by the local system or for Linux systems by PAM. Select the respective value from the list. If you select this option, don't forget to ensure that you activated the **Create Default System Administrator** option in the **System Variables ' Security** tab, otherwise the newly created administrator will not be able to log on. Adminsitrators synchronized with Active Directoy servers are automatically assigned system access and their access will be verified by the directory server.
6. Click **OK** at the bottom of the window to confirm the data for the new administrator.

A new administrator with the specified properties was created.

Modifying your Personal Information

In CM some account properties of the administrator currently logged on can be modified, even if he does not have regular write access to this part of the software.

To modify your personal account properties , proceed as follows:

1. Select **Options > My User Account** .
   The **Properties** dialog box appears.

2. Make the desired changes of your personal information in the **General** tab.
3. Select the **Authentication** tab if you want to change your password.
4. Click **OK** at the bottom of the window to confirm the changes of your personal information.

Deleting an Administrator

> **Note:**
>
> When deleting an administrator you loose all capabilities and access rights accorded to this administrator as well.

Administrators which are acting as a populator can transfer their direct access rights (not those inherited through a group) to another administrator.

To delete an administrator, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrators** in the left window pane.
3. Select the administrator to be deleted from the list in the right window pane.
4. Select **Edit > Delete** .
   The **Warning** dialog box appears.
5. Click either the:
   - **Yes** to transfer the access rights to another administrator
   - **No** to delete the administrator without transfering the access rights
     If you selected **Yes** , the **Select an Administrator** dialog box appears prompting you to select the administrator to inherit the access rights of the administrator to be deleted.

The administrator has now been deleted.

Advanced administrative tasks

This section provides more advanced examples on how to work with administrators.

Sharing or unsharing objects

The share objects option, which by default is set to *No* can be modified to make objects of the current administrator accessible to other group members. The access rights are assigned to the group and not the individual administrator, thus if a new administrator is added to a group he will automatically also have access to these objects, or if one is removed he no longer has access. The option to share objects also can be disabled. However, not sharing will only be valid for all objects which will be newly created. All objects which already exist will still be accessible by all group members.

The share objects option, which by default is set to *No* can be modified to make objects of the current administrator accessible to other group members. The access rights are assigned to the group and not the individual administrator, thus if a new administrator is added to a group he will

automatically also have access to these objects, or if one is removed he no longer has access. The option to share objects also can be disabled. However, not sharing will only be valid for all objects which will be newly created. All objects which already exist will still be accessible by all group members.

To share or unshare objects, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrator Groups** in the left window pane.
3. Select the administrator group which contains the administrator whose objects you want to share in the left window pane.
4. Select the desired administrator in the left window pane.
5. Select the **Group** tab in the right window pane.
6. Double-click the entry in the **Member of** column.
   The **Share Objects** dialog box appears.
7. In the dialog box either:
   - Check the **Share new objects** box to share all objects which the selected administrator will create from now on with the other members of his group
   - Clear the **Share new objects** box to disable the sharing objects option
8. Click **OK** to confirm.
   If you choose to share new objects, a dialog box appears prompting you to specify whether you want to share all objects that already been created by the administrator or not. If you chose to disable the sharing objects option a dialog box appears on the screen informing you about the circumstances of unsharing objects.
9. Click the respective button to confirm your choice.

The Group tab of an administrator

Administrators can be grouped together according to specific criteria to assign them common capabilities. The **Group** tab displays the groups the administrator belongs to.

Parameter	Description
Member of	The column displays the list of group names of which the administrator is a member.
Share Objects	This column indicates if the objects created by the currently selected administrator are to be shared with the other members of the group or groups he belongs to. This means that the other group members have the same access rights to these objects and thus can use them, modify and delete them. The default value is **No** .

Managing administrator groups

The **Administrator Groups** subnode (**Global Settings > Administrator Groups**) collects all administrator groups which exist in CM , and it provides you with the possibility to manage these.

Administrator groups are a way of organizing all existing administrators within your system. The structure defined through your groups is individual and freely configurable by the responsible person.

Administrators can belong to more than one group. Contrary to other group types in CM , administrator groups cannot contain further groups.

Administrator groups can either be static and thus be populated manually or be dynamic and populated via a directory server. Dynamic administrator groups cannot be populated via queries or a compliance rule.

Related topics

- Criteria for Administrator Groups
- Basic Administrator Group Tasks
- Advanced administrator group tasks
- Manually populating administrator groups

Criteria for Administrator Groups

Administrator groups can be created, for example, according to the following criteria:

- geographical location and the administrators' function there
- corporate structure and the administrators' position within
- assigned capabilities

Basic Administrator Group Tasks

This section provides more first examples on how to work with administrator groups.

Creating an administrator group

To create an administrator group, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrator Groups** in the left window pane.
3. Select **Edit > Create Administrator Group** .
   The **Properties** dialog box appears.
4. Enter the desired data in the respective boxes.
5. Click **OK** at the bottom of the window to confirm the data for the new administrator group.

A new administrator group with the specified properties was created.

Deleting an administrator group

> **Note:**
>
> Be aware, that when deleting an administrator group you loose all capabilities and access rights accorded to this group as well. All administrators that were members of only this group are not able to execute their tasks if they are not either directly assigned their necessary rights or if they are not members of another group providing them with the necessary rights.

To delete an administrator group, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrator Groups** in the left window pane.
3. Select the administrator group to be deleted in the right window pane.
4. Select **Edit > Delete** .

The selected attributes will be deleted immediately.

Advanced administrator group tasks

This section provides more advanced examples on how to work with administrator groups.

Modifying the Status of a Dynamic Administrator Group

In CM you can change the status of dynamic groups of any type. The status of a group can either be *active* or *inactive* .

To modify the status of a group, proceed as follows:

1. Select in the left window pane either:
   - **Device Groups** , or
   - **User Groups** .
2. Select the desired group in the left window pane.
3. Select the subnode **Dynamic Population** in the left window pane.
4. Select from the **Group Status** drop-down list of the preceding table in the right window pane the desired status.

The new status was saved and applied to the selected group.

Manually populating administrator groups

This section provides information about manually populating administrator groups.

Adding an administrator to an administrator group

Grouping administrators makes it possible to assign specific capabilities to a number of administrators at the same time without having to define them for each individually. The group capability definitions are always added to the individual administrator ones, however, once an administrator belongs to a group its capabilities cannot be modified individually anymore. Administrators can belong to any number of groups.

To add an administrator to an administrator group, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrator Groups** in the left window pane.
3. Select the administrator group you want to add an administrator to in the left window pane.
4. Select **Edit > Add Administrator** .
   The **Select an Administrator** dialog box appears.

5. Select an Administrator to be added to the selected group.
6. Click **OK** at the bottom of the window to confirm.

The selected administrator is now a member of the selected administrator group.

Removing administrators from a group

To remove an administrator from an administrator group, proceed as follows:

1. Select **Global Settings** in the left window pane.
2. Select the subnode **Administrator Groups** in the left window pane.
3. Select the administrator group from which an administrator is to be removed in the left window pane.
4. Select the administrator to be removed in the right window pane.
5. Select the **Group** tab in the right window pane if not already active.
6. Select **Edit > Remove Administrator from Group** .
   A **Confirmation** dialog box appears.
7. Click **Yes** to confirm the removal.

The selected administrator has now been removed from the administrator group selected in step 3.

Capabilities

The **Capabilities** node lists the capabilities in the right window pane in accordance with the purchased licenses. The node provides the following information:

- **Name**
  This column displays the name of the individual capability. **Capabilities** on almost all BCM database object types are divided up into the following basic access types:

Parameter	Description
View	This access type is the most restrictive of all and provides administrators with the general access to a specific object type, such as reports or devices. If the View capability is not assigned, the main node of the object type will not appear among the nodes in the left console window and no operations of any type may be executed on it. For example, if you do not provide an administrator with the capability to **View Device Groups** , the **Device Groups** node will not be displayed on the left console window and thus the administrator cannot manage or populate any device groups, because he cannot see them.
Manage	This capability allows administrators to create new objects of the specified type, for example, the capability **Manage Operational Rules** allows you to create any number of operational rules under the main **Operational Rules** node. It also allows you to delete any existing operational rules or modify them. It also allows for the creation of links between objects (which are not a device or a device group) such as adding and defining the query for a report. However, this capability does not allow you to assign the operational rule to a software distribution for a client device or group.
Assign	Permits administrators to create the relations between database objects of the specified types. You only need to have the assign capability for the object being assigned, for example, when assigning an operational rule to a device group you only need the **Assign Operational Rules** capability. Creating links between any type of objects that do not have the assign capability falls under the manage capability. With the exception of operational rules and rollouts, this capability also includes the possibility to define the schedule for the object relation.
Configure	

Parameter	Description
	This capability allows the administrator to access the **Configuration** node of the following CM modules to define their configuration parameters: **Compliance Management** , **OS Deployment** , **Patch Management** , **Task Management** and **Software License Management** .

The special capabilities are the following:

Parameter	Description
Populate Device Groups	This capability is necessary for all operations which might influence the content of a device group, such as assigning a directory server to manage the contents of the dynamic group.
Populate User Groups	This capability is necessary for all operations which might influence the content of a user group, such as assigning a directory server to manage the contents of the dynamic group.
Schedule Operational Rules	This capability is required if an administrator is to be able to actually schedule operational rules. Since the execution/installation of packages and patch packages is based on the execution of operational rules an administrator will also need this capability if he is to schedule packages and patch packages.
Schedule Rollouts	This capability is required if an administrator is to be able to actually to schedule rollouts. It also allows him to cancel a rollout. If you are upgrading from a earlier version without this capability, any administrator assigned the assign rollout capability will be automatically assigned this capability as well.
Manage Rollout User Accounts	This capability allows the administrator to manage, that is, add or remove, the user accounts for the rollout. If you are upgrading from a earlier version without this capability, any administrator assigned the manage rollout capability will be automatically assigned this capability as well.
File Transfer	This capability is required if an administrator is to use the file transfer functionality of the direct access function.

Related topics

- Capabilities and Access Rights
- Capability

Capabilities and Access Rights

Capabilities define the general access types which can be assigned to an administrator or an administrator group to access a specific object type and execute operations on it. They can be assigned to an administrator directly and via an administrator group of which he is a member.

The access rights to the individual objects of a specific type, such an individual operational rule or a report, are defined through the **Security** tab.

Capability

Capabilities define the general access types which can be assigned to an administrator or an administrator group to access a specific object type and execute operations on it. They can be assigned to an administrator directly and via an administrator group of which he is a member.

After you selected a capability node in the left window pane, it displays information via its tabs:

- Administrator: The **Administrator** tab concerns administrators to which this capability is assigned.
- Group: The **Group** tab concerns administrator groups to which this capability is assigned.

Viewing connected consoles

You can view the complete list of consoles that are currently connected to master from the **Global Settings** > **Connected Consoles** node. The view works as a sort of log file; every time a console window is opened on the master a new entry is created in this table with the respective information. Consoles that have not given a sign of life for a maximum of 20 minutes will be considered closed and erased from the list. This may occur when the console was not properly closed due to an electrical power outage for example.

The table of the **Connected Consoles** node provides the following information:

Parameter	Description
Administrator Login	The columns of this field display the login names with which someone is currently connected via the console to the master.
IP Address	The IP address of the device on which the console is open.
Last Verification	This column displays the date and time in the time format defined in the User Preferences at which the console ogon was initially validated and the console opened on the remote device and then is modified every time the console reports being open (every 10 minutes). If a console failed to check in to the master, the master will send a verification requires to the console after a maximum of 15 minutes; if the console does not answer it will be considered closed and removed from the list, if it answers the time value will be updated.

The information in this node is part of the Administrator capabilities, therefore this view will only be displayed for administrators with the View Administrators capability. Furthermore the administrator can only see those connected administrators on whom he has at least read access.

Configuring for agent rollout

When your master relays are installed, you are ready to configure Client Management to roll out the agent to all computers in your network. The agent rollout automatically installs the CM agents on all relays and clients. This process is made very easy by the rollout wizard. The two main components involved in the rollout process are:

- The *Rollout Server* , a device that generates the self-extracting agent installation packages and can push them on the target devices.
- *Rollouts* , objects that contain the agent installation files, the list of target devices and any further rollout options.

Before you can start rolling out your first agents, you need to log on to the Client Management console, prepare it for your use, configure the rollout server and create your target groups.

This section includes:

- Preparing the console for rollout
- Configuring rollout servers
- Configuring post-install activities
- Defining the rollout targets

Before you begin

Before starting a rollout, ensure that the following general prerequisites are fulfilled:

- Remote shares are accessible from the master device (for example, *//ClientComputer1/C$*)
- The RPC service is started
- No NAT-configurations are used
- The remote services are accessible
- For Linux installations:
  - Ensure that the SSH service is installed and running on the targets
  - The root account must be enabled on the targets

> **Note:**
>
> These prerequisites are *not* only applicable to the master relays, they are applicable to all relay and client rollouts.

Preparing the console for rollout

Before you can execute any operations in the console such as rolling out the agents across your network, you must provide the license for your system. You can download this license from the BMC website. If you are unable to download the license, contact BMC to provide you with one. However, a basic temporary license will automatically be installed with the software to enable you to launch it. This license is limited to 20 managed devices and 15 days. It is erased and replaced as soon as you import your full license.

The license file contains all the necessary information about the purchased product options. After it is installed you can access all of these. Licenses are imported via their files and cannot be added manually. If you have a license that excludes some features of the product, you can acquire an additional license for these features at any time. If your license is expired only the **Licenses** node will be shown in the console so you can import a new one.

Changing the console language

The console is available in seven different languages: American English, British English, Brazilian Portuguese, French, German, Japanese and Spanish. The language chosen by default is the language of your operating system. If that language is not supported, the display language defaults to American English. If you prefer to work in some other language you can change it as follows:

1. Select **Tools > User Preferences** or click the **Your Preferences** link in the **Welcome** part.
   The **Preferences** window appears on the screen.
2. In the **General** tab select the language from the **Language** list.
3. Click **OK** to confirm and to close the window.

The console refreshes and displays in the selected language.

Importing the license

Before you can execute any operation in Client Management you need to import your license. You should have received a license in the form of a text or xml file from the Support Team.

For more information about licenses, see the following topics:

- Available licenses for BMC Client Management
- License considerations for a super master architecture

> **Note:**
>
> You must install the master on the device for which you provided that data to the Support Team, because this information is used to generate the license; it is not valid for any other device.

1. Click the **Global Settings** node and select from its children the **Licenses** node in the left window pane.
2. Select **Edit > Import License** .
   A dialog box opens displaying the directory structure in a Windows Explorer-like format.
3. Select the file containing your license.
4. With the file selected, click **Open** at the bottom of the window. The information is then read from the file and displayed in the table in the right window pane as follows:

- **Name**
  The fields in this column display the names of the licenses.
- **Count**
  This number indicates how many agents the license contains (that is, on how many devices you can install clients). If you have a temporary license for testing purposes, this number is 20. For all other licenses, this field displays 1 if the license is activated (that is, purchased) or 0 if you do not have this license.
- **Available**
  This column indicates the number of remaining licenses. It is applicable to all functionalities with agent counts, such as the agents themselves, patch management, inventory, compliance management, software distribution and so on. It displays how many licenses are still free to be used. For all other purchased licenses this field always displays 1.

- **Expiry Date**
  This field is empty, if you have an unlimited license for use in your system. If the license is temporary and thus limited, this field displays the expiry date of the license, in the default format defined in the user preferences. A temporary license is valid 30 days.
- **Status**
  This field shows the current status of the license, which should be **Valid** . If you are using the test license it displays **Expiring** .

Now that you have installed your license and thus validated your database and console, you are ready to start working with BMC Client Management . You can proceed to installing a relay and rolling out the agent throughout your network, as detailed in the next topics.

Configuring rollout servers

A *Rollout Server* is a BMC Client Management agent used to deploy other agents. By default, the first relay that is installed in your environment is defined as the rollout server. If you want to use this predefined rollout server for your rollouts you can skip this topic and continue immediately with the next topic, Defining the Rollout Targets .

Notes

- To remotely deploy agents to Windows targets, the rollout server *must* also have a Windows operating system.
- Any rollout server can remotely deploy BMC Client Management agents to other operating systems, that is, Linux and MAC OS.
- If you have a very heterogeneous or distributed environment, you might want to define specific rollout servers for subnets or the different operating system platforms.

The following topics are provided:

- Defining rollout server page
- Adding a rollout server
- User Accounts
- Related topics

Defining rollout server page

The agent running on the rollout server has an additional page, the Rollout Server page. This page cannot be accessed through the regular agent interface. To log on to this page you must either have an admin logon, the system login of the master computer, or a login specifically defined by the admin. This page is only accessible via a browser through the following address: `http://<rollout server name> :<rollout server port number>/rollout` , for example `scotty:1611/rollout`.

> **Note**
>
> You can enter the host name either as its short or full network name such as *scotty* or *scotty.enterprise.com* , or in the form of its IP address. Be aware that when you use IPv6 you need to put square brackets around the IP address, for example, *[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611*.

For our first test this is the master and you can use the predefined login *admin* with no password.

The rollout server page provides the following information about all existing rollouts that are defined as being available on the respective rollout server:

Parameter	Description
Rollout Name	The name of the rollout as defined at its configuration in the console.
Rollout Type	The installation operation executed by the rollout (that is, if it is an agent installation, reinstallation, or uninstall).
Operating System	The operating system type and version of the target devices.
Auto-extractable Name	This is the name of the rollout package – the actual installation package of the agent as defined in the console. This entry is a direct link to the location of the package from which you can download it or launch it through the use of your mouse buttons.
Publication Date	This date box appears the date and time at which the package was made available on this page for download.

Adding a rollout server

1. Go to the **Global Settings > Rollouts > Servers** node.
2. Click **Add Rollout Server** .
   The **Add a new rollout server** window appears.
3. Click the **All** tab in the left window part.
   The **Add a new rollout server** window appears, listing all master relays that you installed in your environment.
4. Select the device which is to be *Your Rollout Server* .

5. Click **OK** to add it and close the window.

The selected device is added the role of rollout server and is now ready to deploy CM agents to the devices in your environment.

User Accounts

From the User Accounts page, you cannot create a new administrator account to roll out agents. You can only add existing administrator account to a rollout.

> To add user accounts that can be associated with rollouts, you need to create an account under the Account Credentials node.

1. In the **User Accounts** page, right-click to view the menu options.
2. Click **Add Account**.
   The Add an account credentials window displays available account credentials.
3. Select the accounts you want to add to the User Accounts page.
4. Click **OK**.

Related topics

Managing administrator credentials centrally for rolling out BCM agents

Configuring post-install activities

From the **Post-Install** node, you can configure the rollout to add and edit a script to be executed after the rollout of the agent has terminated and to add files to be installed on the remote client. This could be to fine-tune agent settings for a specific computer or to simply add some individual configuration files.

The following topics are provided:

- Executing scripts after rollout
- Adding files after rollout

Executing scripts after rollout

The **Script** tab allows the administrator to write and edit a script in the Chilli language to be executed after the termination of the rollout process of the agent on the managed device. This script defines the actions to execute after a rollout has successfully taken place and what is to be done with the files that were added with the script. The default location of the script is `Installation Directory/data/CoreUtils` on the client device, and it is created and stored on the master when you leave the **Post-Install** node.

Adding files after rollout

The **Files** tab provides you with the possibility to add files to the rollout package which are installed or added on the local client after the actual rollout procedure. In which way they are to be treated is defined through the script explained in the preceding tab. By default the list is empty, however, as soon as the script has been created it is automatically added to the list. The table displays the following information about the added files:

Parameter	Description
Name	Displays the name of the file to be installed or added on the client computer.
Define the destination path on the client for the selected files:	Shows the path, either full or relative to the agent, where the file is to be installed on the client device.

Defining the rollout targets

Before starting the rollout of the CM agent on all devices of your infrastructure you should set up the different target groups, for example, for the second and third level relays, one for the clients, or relay and client groups for the different locations or according to operating system, and so on. The two most common methods are explained in this topic, if you are using neither there are more possibilities explained in the Rollout alternatives topic.

The following alternatives for creating your target groups are explained in detail:

- Defining the rollout targets via an directory server
- Defining the rollout targets via an asset discovery scan

Defining rollout targets via asset discovery

Asset discovery scans specific parts of your network and finds all devices on which a CM agent can be installed. When the scan is done you can use the results to create your target groups. For this you need to go through the following steps:

1. defining the asset discovery scanner .
2. Creating and running an automatic asset discovery scan, for which you have the following options:
    a. Creating and running an automatic asset discovery scan of the main scanner's subnet .

OR

1. a. Configuring and running an asset discovery scan of a specific part of your network .

and launch the rollout from either scan result.

Configuring and running an asset discovery scan of a specific part of your network

Configuring and running an asset discovery scan of a specific part of your network

This type of scan job allows you to individually configure all parts of the network scan:

- the scanner to use
- The scanning methods
- The protocols to use
- The targets
- The scan's schedule

This is the recommended scan to use if:

- Your scan targets are located in a different subnetwork than the scanner
- You want to scan your network for virtual and physical devices.

1. Click **Wizards > Asset Discovery** .
   The **Asset Discovery Wizard** appears.
2. Select **Configurable** .
   The **Configurable Discovery** window appears. In this second window you can define which parts of the scan are to be specifically defined, and for which the default values are to be used.
3. Check all configurable options.

   > None of the required objects exist yet. The only configurable option you will not select is the schedule, because you will want to run the scan immediately and only once, which is the default schedule.

4. Click **Next** .
   The **Scanner** window appears.
5. Select a scanner from the list.

   > If you have only one relay installed this list box only shows this one device and it is already preselected as the scanner. If you have several defined as scanners select the scanner to use.

6. Click **Next** .
   The **Scan** window appears.
7. Enter a descriptive name for this scan in the **Name** box, for example *My configurable rollout scan job* .
8. *(Optional)* Select the folder in which the scan is to be located by clicking the **Browse** button and selecting the target folder from the list. You can also create a new folder by clicking **New Folder** . Enter a name for the new folder and click **OK** ; thenc click **OK** again to confirm the selected folder.

9. Click **Next** .
   The **Scan Configuration** window appears.
10. Enter a descriptive name for this scan configuration in the **Name** box, for example *My configurable scan configuration for rollout* .
11. *(Optional)* Select the folder in which the scan configuration is to be located by clicking the **Browse** button and selecting the target folder from the list. You can also create a new folder by clicking **New Folder** . Enter a name for the new folder and click **OK** ; then click **OK** again to confirm the selected folder.
12. Click **Next** .
    The **Protocols** window appears.
13. Either keep all the protocols that are activated by default, or deactivate one or more protocols by clearing the check boxes next to them.

    If you are not scanning for virtual devices, clear the **VMware vSphere** and **Hyper-V** protocols.

14. To add credentials to a protocol, select its entry in the table and then click **Add Credential** to the right.
    The **Credentials** box becomes available.
15. To add a new user identification, click **Add** at the bottom.
    The **Properties** dialog box appears.
16. Enter and confirm the login name and corresponding password.

    The login name must have the following format:
    - `<domain name>/<user logon>` if you are on a domain
    - `<user logon>` if you are not on a domain

17. If you are adding credentials for the SNMP protocol, you must enter the name of the community and confirm it by re-entering it.
18. To view the passwords/communities, clear the **Hide Passwords** check box.
    Both password boxes are now displayed in clear text format.
19. To confirm the new user account, click **OK** at the bottom of the window.
    The account is added to the list at the right side of the dialog box.
20. Repeat the preceding steps to add more authentications, if necessary.
21. To delete an existing user login from the selected protocol select it in the table and click **Delete** below the box.
22. Click **Next** .
    The **Target List Configuration** window appears.
23. Enter a name for the new target list in the **Name** box, for example *My configurable scan rollout target list* , and define a specific folder, if necessary.

24. Add the devices to the scan. The easiest way to do so is to add IP address ranges to scan:

    > When you specify an address range with IPv6 addresses, be careful to not add complete subnets, which are very large and take very long to complete.

    a. Click **Add Existing Device** .
    The **Add a Device** dialog box appears on the screen.
    b. Enter the target ranges to be added to the list in the respective text box. These can be entered:

- As a comma-separated list of names or ranges, for example, `scotty; 192.168.4.45-192.168.4.47; 2001:0db8:85a3:0000:0000:8a2e:0370:7334` which includes computers `scotty.enterprise.com` , `192.168.4.45, 192.168.4.46` , `192.168.4.47` and `2001:0db8:85a3:0000:0000:8a2e:0370:7334` .
- As CIDR notation in the form of `192.9.205.22/18` or `2001:0db8:85a3:0000:0000:8a2e:0370:45/123`
    1. Click **OK** to add the range and close the window.

1. Click **Finish** .
2. In the **Confirmation** dialog box, click **Yes** to change the focus of the console window to the scan view.
   The focus of the console switches to **Asset Discovery > Scanners > Your Scanner > Assigned Scans > My configurable rollout scan job** .
3. Select the **Assigned Schedule** tab.
4. To follow the scan process, check the **Status** column.

   > This view displays detailed information about the scan currently running on each device with specific counters.
   > The **Status** column starts with `Assignment Waiting` . Then it goes through all the respective stages and displays `Executed` .

   The scan is finished when the status `Done` or `Unreachable` appears.
5. Select the node of your scan in the left window pane.
6. In the table to the right, select the target devices for the relay or client rollout.
7. Right-click your mouse button on your selection and select the **Agent Rollout** option from the pop-up menu.
   The **Agent Rollout Wizard** appears.

Where to go from here

- **If you are installing on site:**
  Continue the rollout procedure with step 2 of either the relay rollout or the client rollout .
- **If you are installing in the cloud:**
  Continue the rollout procedure with step 2 of either the relay rollout or the client rollout .

Creating and running an automatic asset discovery scan of the main scanner's subnet

Creating and running an automatic asset discovery scan of the main scanner's subnet

This scan job scans the complete subnet of your scanner immediately. It is completely automated. You only need to provide the access credentials and select the scanner.

If your scan targets are located in a different subnetwork than the scanner or you want to scan your network for virtual and physical devices, you need to configure and run a specific asset discovery scan.

1. Select **Wizards > Asset Discovery** .
   The **Asset Discovery Wizard** appears.
2. Leave the preselected **Automatic** option selected.
3. Enter the credentials required to access the devices in the scanner's subnet in the **Windows Login (DomainLogin)** and **Windows Password** boxes.

   > The login name must have the following format:
   > - <domain name>/<user logon> if you are on a domain,
   > - <user logon> if you are not on a domain.

4. Click **Next** .
   The **Scanner** window appears.
5. Select a scanner from the list.

   > If you have only one scanner installed, it is preselected.

   Your scan is now completely configured and ready to run.
6. Click **Next** .
   The **Automatic Scan** window appears.
7. Click **Scan Now** to launch the scan.
8. In the **Confirmation** dialog box click **Yes** to change the focus of the console window to the scan view.
   The focus of the console switches to **Asset Discovery > Scanners > Your Scanner > Assigned Scans > Your Scan Job** .
9. Select the **Assigned Schedule** tab.
10. To follow the scan process, check the **Status** column.

> The **Status** column starts with `Assignment Waiting` . Then it goes through all the respective stages and displays `Executed` when the scan of the target device is finished.

This view displays detailed information about the scan currently running on each device with specific counters. The scan is finished when the status `Done` or `Unreachable` appears.

11. Select the node of your scan job in the left window pane.
12. In the table to the right, select the target devices for the relay or client rollout.

> You can select more than one device by holding the CTRL key while selecting the devices.

13. Right-click your mouse button on your selection and select the **Agent Rollout** option from the pop-up menu.
    The **Agent Rollout Wizard** appears.

Where to go from here

- **If you are installing on site:**
  Continue the rollout procedure with step 2 of either the relay rollout or the client rollout .
- **If you are installing in the cloud:**
  Continue the rollout procedure with step 2 of either the relay rollout or the client rollout .

Defining the asset discovery scanner

By default your master relay (or the first-level relay that was first installed) is automatically defined as the asset discovery scanner. But you can also define any other device on which the CM agent is already installed as your scanner. If you want to proceed with your current scanner you can skip this topic and continue with either Creating and running an automatic asset discovery scan of the main scanner's subnet or Configuring and running an asset discovery scan of a specific part of your network if you need to define a scan with specific parameters. Otherwise proceed as follows:

1. Select the **Asset Discovery** node and then go to the **Scanners** node in the left window pane.
2. Click **Edit > Add Device** .
   The **Add a Scanner** pop-up menu displays displaying the list of all devices that can be a scanner due to their operating system.
3. Select the device to be added from one of the list boxes.
4. Click **OK** to confirm and close the window.

The device is added to the list of available scanners and its configuration parameter is updated.

Defining rollout targets via directory servers

If you have a well set up directory server for your environment, the easiest method to define your rollout targets is to base them on the OUs of this directory server. Even though this server already exists in your environment you still need to make it known to the Client Management database. For this, you need to do the following:

1. Creating a directory server in Client Management .
2. Assigning a directory server to the target group and synchronizing .

Assigning a directory server to the target group and synchronizing

Assigning a directory server to the target group and synchronizing

1. In the left window pane, select the **Device Groups** node.
2. Click **Edit > Create Device Group** to create a new group.
   The **Properties** dialog box appears.
3. Click **OK** .

> It is not necessary to give a name to this group, as it is automatically renamed to the name of the directory server and OU as soon as it is assigned.

4. Select the new group in the left window pane.
5. Select the new group's subnode **Dynamic Population > Directory Server** .
6. Click **Edit > Assign Server** .
   The **Select a Directory Server** dialog box appears on the screen. The dialog box lists all available directory servers with their organizational units depending on the base object. That is, when under a device group, it displays all available device groups, and when under a user or administrator group, it displays all available user groups.
7. Select an entry from the list.

> You can select either the directory server itself or one of its children. If you want to synchronize all elements of a directory server in a flat list you can check the **Synchronize All Devices/Administrators/Users** box above this list together with the directory server root in the box below. To synchronize with the server root or an OU maintaining, that is, recreating the directory structure in Client Management , do not check this box.

8. Click **OK** to confirm.
   The **Properties** dialog box appears on the screen.
9. From the list, select an option to specify if all devices are to be synchronized, or only those with a CM agent installed.

10. Click **OK** to confirm.
    A confirmation window appears.
11. Click **OK** to synchronize now.
    The connection with the directory server is established and all members of the selected entry are added to your current group. The **Directory Server Synchronisation** window displays a confirmation that lists all objects that were added, along with their status, which in this case is either *New Object* or *Error* .
12. Click **OK** to close this window.

The name of your group is changed to the name of the directory server entry followed by the full name of the server in dotted notation. For example, if you synchronized your group with an organizational unit called *Relay Servers* , the name of your group is now *Relay Servers.Full. Directory.Name* . If the selected group has subunits, these are also synchronized and added to the group as *subunit.group.server name* .

If all elements of a type were synchronized, the name of the group changes to the full name of the directory server. The elements are added to this group in a flat list, ignoring any hierarchy they were sorted in on the directory server.

Repeat this procedure for all target groups to which you need to roll out the agent.

When you have created all necessary target groups, you are ready to create the rollouts and assign the target groups to them.

Where to go from here

- **If you are installing on site:**
  See Rolling out relay agents and Rolling out client agents .
- **If you are installing in the cloud:**
  See topics Rolling out relay agents and Rolling out client agents .

Creating a directory server in Client Management

1. Select **Global Settings > Directory Servers** in the left window pane.
2. Select **Edit > Create Directory Server**
   The **Properties** window appears, displaying the values for the directory server it has found on the master's domain.
3. Enter the required information in the respective boxes or modify the preselected values to those of another directory server that you want to add.

Field	Description	
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.	
Notes	Free text field that may be edited to display general information about the object and its contents.	
Directory Server Proxy	Specify the device to be defined as the directory server proxy by clicking the **Select a Device** icon to the right.	

Field	Description	
Type	Select from this dropdown list the type of directory server that is to be defined.	**MS Active Directory**
Field	**Description**	
AD Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .	
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).	
Alias	This field is empty by default. If you enter a value it is used as the user domain for the object types **Administrator** and **User** instead of the domain name that was recovered via the base DN. For example, a user who is registered under *europe.world.enterprise.com* could be indicated via his OU called *Americas* .	**IBM Domino**
Field	**Description**	
Domino Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .	
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).	
Organizational Unit	The name of the Domino organizational unit to which the user belongs, similar entity to the alias and OU of Directory Server, for example, a Domino directory of which the organization name is *World* and which includes the organizational units *Americas* , *Europe* and *Asia* .	**LDAP Server**
Field	**Description**	
LDAP Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .	
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).	
Base DN	Enter the unique name of the base DN to which you want to connect. The base DN is the entry point to the directory organization and different from all others. You can enter this value either in LDAP or UNC format. For example: the entry *world.entreprise.com* of Active Directory can be entered in LDAP notation as *dc=world, dc=enterprise, dc=com* or as *world.enterprise.com* in UNC notation.	
Domain Alias	This field is empty by default. If you enter a value it is used as the user domain for the object types **Administrator** and **User** instead of the domain name that was recovered via the base DN. For example, a user who is registered under *europe.world.enterprise.com* could be indicated via his OU called *Americas* .	**Novell eDirectory**
Field	**Description**	
eDirectory Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .	

Field	Description	
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).	
Context	The name of the context that is to be referred in eDirectory. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings and is the same as a complete domaine name in Active Directory. A context called *world.enterprise.com* that redirects to the directory part referencing the desired user.	
Tree	The name of the eDirectory tree to which you want to connect. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings; it is the same as an Active Directory **Alias** and may be required in certain cases. A user of context *europe.world.enterprise.com* may for example be part of a tree called *Americas* in which exists a unit *USA* .	**Credentials**
Field	**Description**	
Anonymous Access	Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.	
Authenticated Access	Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in.	
User	Defines the name uniquely identifying the user: • **sAMAccountName notation** , example *DOMAINUser* , this is the recommended syntax • **LDAP notation** , for example, *cn=username, cn=usergroup* where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory *Users and Computers* • as the **simple user name** , for example, *administrator* (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain). • **UPN notation** , for example, *user@domain.com* (for users in other than the AD domain). 	
Password	Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).	

4. Check that the entered values are correct by clicking the **Test Login** button.
5. Click **OK** to confirm.

A new directory server with the specified data is created.

Managing administrator credentials centrally for rolling out BCM agents

You can centrally manage administrator credentials using the Account Credentials functionality. The Account Credentials functionality is represented as a node on the BMC Client Management console. You can associate one or more rollouts to credentials.

When you update an administrator credential that is centrally managed under the Account Credentials node, BMC Client Management automatically applies any changes you made to that credential to all the associated rollouts. A ny update to credentials are automatically refreshed for each rollout. Therefore, managing several rollouts that are associated to a single account becomes efficient.

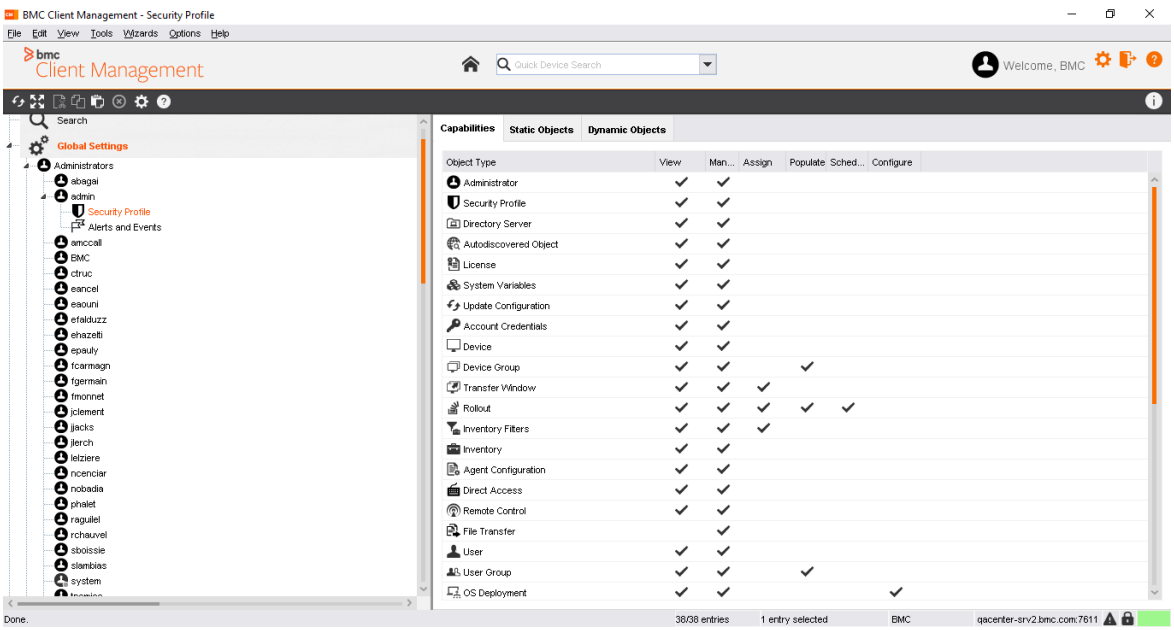
This topic covers the following topics:

Before you begin

- Ensure that you have credential details to create an account
- Rollouts are ready to be associated with accounts

Enable capability to use the Account Credentials functionality

- On the BMC Client Management console, go to **Global Settings** > ***ClientManagementAdmin*** > **Security Profile**.
- Enable **Account Credentials**.



Creating a new account credential

Create your account under the Account Credential node. Later you can associate it to rollouts.

1. On the BMC Client Management console, click **Global Settings** > **Account Credentials**.
2. In the **Account Credentials** window, right-click and click **Create Account Credentials**.
3. In the **Properties** window, enter the required information and click **OK**.
   A new account credential is created.

- You cannot create two accounts with the same domain name and login user name.
- You can create several accounts without assigning any domain, but with the same login ID and a different password for each account.

Associating accounts with rollouts

As an administrator, you can associate accounts to rollouts. Rollouts on several assets can be efficiently managed even when administrator credentials change.

1. On the BMC Client Management console, click **Global Settings** > **Rollouts**.
2. Click a ***rollout*** > **Servers**.
3. Click target server where you want to add the new account credential.
4. Click the **User Accounts** tab.
5. Right-click in the User Account window and click **Add Account**.
6. From the **Add an account credentials** window, select the accounts you want to add to the rollout.
   The selected account credentials are added to the rollout.

You cannot create a new account from **Global Settings** > **Rollouts**.

You can create or add a new account in the **Agent Rollout** wizard, on the menu bar, click **Wizards** > **Agent Rollout**.

Updating account credentials

You can update account credentials only from the **Account Credentials** node.

1. On the BMC Client Management console, click **Account Credentials** > ***Account Credential Name***.
2. To update the account credentials, click **F2** or double-click the account credential, or right-click > **Properties**.
3. Click **Ok**.
   The new account credentials are used while rolling out agents on assets.

Status of rollouts when an associated account is modified

When a parameter of the account is modified, then roll out configurations take specific states.

- If the Domain name or Login ID is modified, the status of the rollout configurations is updated to **Paused** state.
- If the Password is modified, BMC Client Management displays a popup asking whether the rollout package should be rebuilt.
  - If you select **Yes**, the rollout package must be rebuilt, the rollout configuration state is updated to **Reassign Waiting**.
  - If you select **No**, the rollout package must be rebuilt, the rollout configuration state is updated to **Paused**.

Upgrade considerations

- When you upgrade, BMC Client Management checks every account under the User Accounts node and creates a corresponding account under the Account Credentials node. The account takes the domain or login user name as the account name if the domain field is not empty. Otherwise, the account name is set to *New Account Credential x*.
- If several user accounts exist with the same domain and login user name, only one Account Credential account is created with the password of the last updated user account.
- All administrators or admin groups having the Rollout Populate capability and the Assign Access rights on a rollout, automatically have the Account Credentials capabilities and the access rights on the account credentials assigned to the configurations linked to the rollout.

Results

Possible results

- Check whether rollouts are populated under the Account Credentials node.
- Check whether accounts are populated under the Rollouts node.
- Upon changing credential details, BMC Client Management automatically authenticates rollouts with the new credential details. The Account Credentials functionality ensures that you do not have to manually authenticate each rollout.

Where to go from here

Perform rollouts on assets that are associated to the **Account Credentials** node.

Related topics

Rolling out agents

Alternatives for rollout

This section describes alternative ways to roll out the CM agent to the target population, such as via the Microsoft Network Neighborhood or to a specific IP address range.

Related topics

- Rolling out client agents via the Microsoft network neighborhood
- Rolling out CM agents to specific IP address ranges
- Scheduling the rollout at a specific date and time

Rolling out client agents via the Microsoft network neighborhood

This procedure rolls out client agents to Windows 7 devices using the Windows network neighborhood.

1. Select **Wizards > Agent Rollout** .
   The **Core Setup Configuration** window appears.
2. Check the **Configure the relay selection or use master otherwise** box.

   > If you want to schedule the rollout at a specific date and time check the box for second last question.

3. Click **Next** .
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** box.
5. Enter the name for the rollout package executable in the **Auto-extractable Name** box (for example, *win7clientagent12.exe*).
6. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** box (for example, *Windows XP/2003... (64 bit)* .

7. Click **Next** .
   The **Communication** window appears.
8. To find the relay click **Import Devices from CSV File** next to the **Parent Name** box.
9. Click **All** .
10. Select the desired parent device from the list and click **OK** .
11. Click **Next** .
    The **Targets & Accounts** window appears.
12. Click **Add Device from List** .
    The **Select Devices from the List** window appears. It provides you with the different methods to select the rollout targets.
13. Select the **Network** tab in the left window bar.
    The box **Available Devices** displays now the Microsoft Windows Network Neighborhood structure on the screen.
14. Open the tree structure under which the target devices are located.
15. Select the devices to be added to the list by highlighting and moving them to the **Selected Devices** list to the right via **Add** .

    - You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you have already installed the master and probably at least one relay.
    - You cannot add the master as a target device.

16. Click **OK** to add the selected devices and close the window.
17. Click **Add Administrator** .
18. Enter the required data for the account login into the respective boxes.
19. Click **Verify Rollout** to ensure that the entered account data is correct.
20. Click **OK** and then **Finish** .
21. In the **Confirmation** dialog box, select the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
22. If you did not check the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode. In the **Assigned Schedule** tab, you can follow the general progress of the client rollout assignment.
23. After this value reads `Executing` , select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now rolled out the CM agent to specific devices of your infrastructure that were provided by the Microsoft Network Neighborhood.

Rolling out CM agents to specific IP address ranges

Rolling out CM agents to specific IP address ranges

To roll the agent out to specific IP address ranges instead of selecting the devices from the network neighborhood, an autodiscovery must be executed before starting the actual rollout procedure.

Running an autodiscovery on an IP address range

1. In the left window pane of the console select the device which is to execute the autodiscovery of the network; this should be the relay under which the clients are to be located.
2. Select the **Agent Configuration > Module Configuration > AutoDiscovery** node.
3. Select **Edit > Properties** .
   The **Properties** dialog box appears on the screen, displaying the module's parameters.
4. Enter the indicated values for the following parameters and leave all others as they are:

Timeout (sec)	2
Address Range	The IP address range to scan
Address Verification Interval (sec)	2
Use Network Neighborhood	Yes

5. Click **OK** to confirm the new parameters and to close the window.
   The autodiscovery is launched immediately. You can follow its progress by going to the **Device List** tab.
6. To see the list populated with devices found by the relay, click **Refresh** from time to time.

Rolling out client agents to specific IP address ranges

1. Select **Wizards > Agent Rollout** menu item .
   The **Core Setup Configuration** window appears.
2. Check the **Configure the relay selection or use master otherwise** box.

> If you want to schedule the rollout at a specific date and time check the **Configure a custom schedule for this rollout (default is one immediate execution)** box.

3. Click **Next** .
   The **General Parameters** appears.
4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** box.
5. Enter the name for the rollout package executable in the **Auto-extractable Name** box (for example, *win7clientagent12.exe*).

6. Select the operating system group to which the agent is to be rolled out from the list of the **Operating System** box (for example, *Windows XP/2003... (64 bit)* .
7. Click **Next** .
   The **Communication** window appears.
8. To find the relay click **Add Device from List** next to the **Parent Name** box.
9. Click **All** .
10. Select the desired parent device from the list that appears and click **OK** .
11. Click **Next** .
    The **Targets & Accounts** window appears.
12. When selecting the rollout targets from the autodiscovery you have two possibilities to do so:
    a. You can select the targets from a general list displaying all autodiscovered devices.

    > The tab is the preselected tab when the window is opened. It displays the list of all devices found by all devices executing autodiscoveries in the network.

13. Select the device/devices to be added to the list by highlighting the different devices and moving them to the **Selected Devices** list to the right via **Add** .
    You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.
    You cannot add the master as a target device.
14. Click **OK** to add the selected devices and close the window.
    a. You can select the targets from the autodiscovered list of a specific device.
15. Select the **AutoDisc Device** tab ( ) in the left window bar.
    The **Select a Device** window appears.
16. Click **All** and then select the device that carried out the autodiscovery, that is, the parent relay in this example).
    The **Available Devices** box now displays the list of all devices found.
17. Select the device/devices to be added to the list by highlighting the different devices and moving them to the **Selected Devices** list to the right via **Add** .
    You can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.
    You cannot add the master as a target device.
18. Click **OK** to add the selected devices and close the window.
19. Click **Add Administrator** .
20. Enter the required data for the account login into the respective boxes.
21. Click **Verify Rollout** to ensure that the entered account data is correct.
22. Click **OK** and then **Finish** .

23. In the **Confirmation** dialog box, select the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
24. If you did not check the **Go to Rollout** box at the end of the wizard, select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

> In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.

25. After this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now rolled out the CM agent to a specific subnet of your infrastructure.

Scheduling the rollout at a specific date and time

In the **Core Setup Configuration** window, ensure that the **Configure a custom schedule for this rollout (default is one immediate execution)** box is selected. Then, after the **Targets & Accounts** window, the **Schedule** window appears.

1. Select the **Validity** tab.
2. Define in the **Execution Date** box at what moment the rollout is to be launched for the first time (for example, at the next device startup).
3. Define in the **Termination** box when the rollout is to be run for the last time (for example, stop after 5 executions).
4. Select the **Frequency** tab.

> Here you can define the exact day, time or frequency at which the rollout is to be launched on the target. To run the rollout more than once makes sense only if you expect that some rollout executions might not succeed at the first try.

5. Click **Finish** .

The rollout is now defined and scheduled to be executed at the specified time.

Managing reboot windows

BMC Client Management provides automated rebooting after specific operations, such as after a patch or a software installation, when it is necessary. However, end users should not be interrupted with a reboot request at the wrong time. Reboot windows are specifically designed with regards to critical situations and allow the BMC Client Management administrator to define timeframes in which devices can be rebooted or are absolutely not to be rebooted. A reboot window's role is to provide a simple lookup service to verify whether the reboot can take place.

All reboot windows are created and managed under the **Global Settings > Reboot Windows** node. Each reboot window consists of information for every hour of the week, starting from 0:00 on Monday all the way to 23:00 on the following Sunday. As such the window does not, and cannot, control rebooting based on anything such as predefined calendar dates or times. As an example, the setting configured for the 8:00 slot on Wednesday controls device reboots between 8:00 and 8:59:59 for every Wednesday regardless of date. A reboot window authorizes, for example, the reboot of a device requested by a patch, but does not execute it.

Reboot windows can be assigned at will to devices and device groups. A device can have more than one reboot window assigned. But be aware, that if there is more than one window assigned and these windows do not have common allowed timeframes, the device can never reboot.

This topic includes:

Creating a new reboot window

1. Select **Edit > Create Reboot Window**  .
   The **Properties** dialog box appears on the screen.
2. Enter a descriptive name in the **OK** box, for example, *Pre-round reboot* .
3. *Optional:* Check the **UTC Time** box if required.
   Activating this option might be useful if the new reboot window is assigned to devices in a number of different time zones.
4. *Optional:* Enter a description of the reboot window in the **Notes** box.
   This might be very helpful if you have many different windows and allows you to see at a glance when the window permits or prohibits reboots, and especially, if a device is assigned more than one window, to ensure that the prohibited and allowed slots do not cancel each other.
5. Click **OK** at the bottom of the window to confirm the new reboot window.

Defining reboot window time-slots

Reboot windows allow for a better control of when devices can be rebooted. The hourly slots are represented in the visual form of a spreadsheet. Each slot or cell represents the reboot permission of one hour of the week. By consulting this planning, agents know if they can reboot a device at the requested time. If no reboot window is assigned to a device, reboots are always allowed. Whenever a reboot window is assigned to a device, a message displays in the reboot log file.

To define a reboot window

1. Click the slot which is to be prohibited. By default all time slots are permitted.
   You can also select a range of slots by dragging your mouse button over the desired range.
2. Click **Deny Time-slot** .
   The selected time-slot or slots are prohibited and do no longer permit reboots to take place during these hours.
3. To allow a prohibited time-slot select it and then click **Allow Time-slot** .
4. Repeat these steps for all other slots or ranges to be defined or modified.

Assigning reboot windows

You can assign more than one reboot window to the targets. There are two ways to assign a reboot window to a target:

- To assign reboot windows to devices or device groups
- To assign devices or device groups to reboot windows

> **Note**
>
> If you are assigning more than one window to a target ensure that the allowed and prohibited slots are not mutually canceling each other. Combining reboot windows always uses the most restrictive possibility, that is, if one window allows a slot and the other does not, the slot is prohibited.

To assign reboot windows to devices or device groups

1. Select the **Assigned Objects** of the device or device group to assign in the left window pane.
2. Select the **Reboot Windows** subnode.
3. Click **Edit > Assign Reboot Window** .
4. Click **Yes** to automatically activate the reboot window that is to be assigned, or click **No** to manually activate it later in the appearing **Confirmation** window.
   The **Assign a Reboot Window** dialog box appears.
5. Select the desired reboot window(s) from the list in the dialog box.
   You can select more than one window by holding the CTRL key while making your selection. If you select more than one window, ensure that the defined reboot time-slots do not cancel each other and make the device un-rebootable.
6. Click **OK** to confirm the assignment.

The selected reboot window is now assigned to the device or device group. If you chose to directly activate the assignment, the targets are only rebooted if the reboot request arrives within the allowed time-slots from now on. If the request arrives the reboot must wait until the next possible allowed time-slot arrives. If you have not chosen to activate the assignment you need to manually activate is via the **Activate Reboot Window** option for the defined reboot restrictions to take effect.

To assign devices or device groups to reboot windows

1. Select the **Assigned Objects** of the reboot window to assign in the left window pane.
2. Select the **Device Groups** or **Devices** subnode, depending on which type of target you want to assign.
3. Click **Edit > Assign Device Group** or **Edit > Assign Device**  .
4. Click **Yes** to automatically activate the reboot window that is to be assigned, or click **No** to manually activate it later in the appearing **Confirmation** window.
   The **Assign to Device** or **Assign to Device Group** dialog box appears.
5. Select the desired target(s) from the list in the dialog box.
6. Click **OK** to confirm the assignment.

The selected reboot window is now assigned to the device or device group. If you chose to directly activate the assignment, the targets are only rebooted if the reboot request arrives within the allowed time-slots from now on. If the request arrives the reboot must wait until the next possible allowed time-slot arrives. If you have not chosen to activate the assignment you need to manually activate is via the **Activate Reboot Window** option for the defined reboot restrictions to take effect.

Activating reboot window

If you have not activated the reboot window when you assigned it, it must be individually activated for the defined reboot settings to take effect on the target.

To activate a reboot window

1. Select the entry to activate in the table in the right window pane.
   You can select the entry from different locations:
   - under the reboot window's node:
     - **Global Settings > Reboot Windows > My reboot window > Assigned Objects > Device Groups**
     - **Global Settings > Reboot Windows > My reboot window > Assigned Objects > Devices**
   - under the device group's node: **Device Groups > My device group > Assigned Objects > Reboot Windows**
   - under the device's node: **Devices > My device > Assigned Objects > Reboot Windows**
2. Select **Edit > Activate Reboot Window**  .

The reboot window is immediately activated and its defined reboot settings take effect as soon as the activation has arrived at the target device.

Reassigning reboot windows to their targets

If you made modifications to a reboot window which is already assigned to a device group or a device the window must be reassigned for the modifications to take effect. This means that the reboot window is updated with its modifications on the assigned devices. The reassignment will always be executed on all members of a device group if it is selected.

There are two ways to reassign the reboot window:

- To reassign the modified reboot window on all targets
- To reassign the modified reboot window on an individual device

If the reboot window is assigned to more than one target, it is easier to reassign from the modified reboot window.

To reassign the modified reboot window on all targets

1. Go to **Global Settings > Reboot Windows** and select the modified reboot window.
2. Then go to the selected window's **Assigned Objects > Device Groups** or **Assigned Objects > Devices** subnode.
3. Select all devices or device groups in the table in the right window pane.
4. Click **Edit > Reassign Reboot Window**  .

The reassignment process of the reboot window is launched immediately. As soon as the target devices received the modified window they applying the new reboot settings.

To reassign the modified reboot window on an individual device

The reboot window can also be reassigned individually via the assigned devices or device groups. The example below shows how to do this for an individual device, proceed in the same way to reassign the window to the target groups, via the device group's node.

1. Select the device's node in the left window pane.
2. Then go to the selected device's **Assigned Objects > Reboot Windows** subnode.
3. Select the modified reboot window in the table in the right window pane.
4. Click **Edit > Reassign Reboot Window**  .

The reassignment process of the reboot window is launched immediately. As soon as the target device has received the modified window it applies the new reboot settings.

Managing directory servers

The LDAP Client (notably Microsoft Windows Active Directory) functionality presents organizations with a directory service designed for distributed computing environments. It allows organizations to centrally manage and share information about network resources and users while acting as the central authority for network security.

In addition to providing comprehensive directory services to a Windows environment, the directory server is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies require.

A directory service differs from a directory in that it is both the directory information source and the services making the information available and usable to administrators, users, network services, and applications. Ideally, a directory service makes the physical network topology and protocols (formats for transmitting data between two devices) transparent so that a user can access any resource without knowing where or how it is physically connected. To continue the user account example, it is the directory service that lets other authorized users on the same network access stored directory information (such as an email address) about the user account object. In addition to providing a place to store data and services to make that data available, it also protects network objects from unauthorized access and replicates objects across a network so that data is not lost if one domain controller fails.

CM allows you to synchronize its device database with directory services already existing in your network. You can thus 'copy' existing directory services items such as organizational units (OU), computers, and so on, into CM groups and members to then administer these via the CM console. You can 'import' all different types of groups including security groups and users and computers. This node allows you to define the existing directory servers for use with CM , the actual synchronization is done through the nodes of the groups to be synchronized.

A directory service is the main switchboard of a network operating system. It manages the identities and brokers relationships between distributed resources so they can work together. Further, it is a place to store information about corporate and organizational assets such as applications, files, printers, and users. It provides a consistent method for naming, describing, locating, accessing, managing, and securing information about the resources

When Active Directory is installed on your Windows Server a new Active Directory forest or domain is created. In Active Directory, the network and its objects are organized by constructs such as domains, trees, forests, trust relationships, organizational units (OUs), and sites. The server which is the first domain controller in this forest is called the **Directory Server** . The directory server is the computer running the server that manages all user access to the network which includes logging on, authentication an access to the directory and shared resources. Each directory server has a **Dynamic Groups** subnode.

The following topics are provided:

- User fields

Computer fields

This tab lists all available fields for devices that may be synchronized with their original name and the matched field name within the console. It displays the following information:

Parameter	Description
The name of the object class to synchronize.	This field above the table displays the type of object to which the following fields refer.
Attribute	This field displays the name of the field as it displays in the CM console .
Value	This field displays the name of the field as which it is known by the directory server.

User fields

This tab lists all available fields for administrators and users that can be synchronized with their original name and the matched field name within the console. It displays the following information:

Parameter	Description
The name of the object class to synchronize.	This field above the table displays the type of object to which the following fields refer.
Attribute	This field displays the name of the field as it displays in the CM console .
Value	This field displays the name of the field as which it is known by the directory server.

This section includes:

- Creating a directory server
- Modifying the directory server parameters
- Checking connection to the directory server
- Deleting a Directory Server

Creating a directory server

1. Select **Global Settings> Directory Servers** in the left window pane.
2. Select **Edit> Create Directory Server**
   The **Properties** window appears displaying the values for the directory server it has found on the master's domain.
3. Enter the required missing information into the respective boxes or modify the preselected values to those of another directory server to add.

Parameter	Description
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.
Notes	Free text field that may be edited to display general information about the object and its contents.
Directory Server Proxy	Specify the device to be defined as the directory server proxy by clicking the **Select a Device** icon to the right.
Type	Select from this dropdown list the type of directory server that is to be defined. Based on the directory type, the other options are populated. The options include: • MS Active Directory • IBM Domino • LDAP Server

Parameter	Description
	• Novell eDirectory

4. Specify the credentials as required. The options include:
   - **Anonymous Access**: Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.
   - **Authenticated Access**: Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in:
     - **User:** Defines the name uniquely identifying the user:
       - **sAMAccountName notation**. For example, DOMAINUser. This is the recommended syntax.
       - **LDAP notation**: For example, cn=username, cn=usergroup where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory Users and Computers
       - as the **simple user name**. For example, administrator (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain).
       - **UPN notation**. For example, user@domain.com (for users in other than the AD domain).
     - **Password:** Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).
5. Check that the entered values are correct by clicking the **Test Login** button.
6. Click **OK** to confirm.
   A new directory server with the specified data was created.

List of supported directory servers

MS Active Directory

Parameter	Description
AD Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Alias	

Parameter	Description
	The name of the eDirectory tree to which you want to connect. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings; it is the same as an Active Directory **Alias** and may be required in certain cases. A user of context *europe.world.enterprise.com* may for example be part of a tree called *Americas* in which exists a unit *USA* .

IBM Domino

Parameter	Description
Domino Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Organizational Unit	The name of the Domino organizational unit to which the user belongs, similar entity to the alias and OU of Directory Server, for example, a Domino directory of which the organization name is *World* and which includes the organizational units *Americas* , *Europe* and *Asia* .

LDAP Server

Parameter	Description
LDAP Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Base DN	Enter the unique name of the base DN to which you want to connect. The base DN is the entry point to the directory organization and different from all others. You can enter this value either in LDAP or UNC format. For example: the entry *world.entreprise.com* of Active Directory can be entered in LDAP notation as *dc=world, dc=enterprise, dc=com* or as *world.enterprise.com* in UNC notation.
Domain Alias	The name of the eDirectory tree to which you want to connect. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings; it is the same as an Active Directory **Alias** and may be required in certain cases. A user of context *europe.world.enterprise.com* may for example be part of a tree called *Americas* in which exists a unit *USA* .

Novell eDirectory

Parameter	Description
eDirectory Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Context	The name of the context that is to be referred in eDirectory. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings and is the same as a complete domaine name in Active Directory. A context called *world.enterprise.com* that redirects to the directory part referencing the desired user.
Tree	

Parameter	Description
	The name of the eDirectory tree to which you want to connect. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings; it is the same as an Active Directory **Alias** and may be required in certain cases. A user of context *europe.world.enterprise.com* may for example be part of a tree called *Americas* in which exists a unit *USA* .

Modifying the directory server parameters

1. Select **Global Settings > Directory Servers** in the left window pane.
2. Select the directory server to modify in the right window pane.
3. Select **Edit > Properties** .
   The **Properties** window appears.
4. Make the required modifications in the respective parameter boxes.
5. Click **OK** to confirm.
   Any changes made were saved and applied to the selected directory server.

Checking connection to the directory server

To ensure that your directory server entry is valid and working, BMC recommends that you verify the connection.

> **Note**
>
> If you have Windows XP and 2003 32-bit devices in your environment ensure that you have correctly configured the server certificate verification, that is, the server certificate is included with the trusted certificates of the clients. If the server certificate cannot be verified by the client all communication between server and client will not be encrypted.
>
> For more information about this issue on Windows devices, see the Microsoft Knowledge Base article 835208. For more information about certificates and how to configure and install them, see the Client Management and SSL topic of the Reference section.

1. Select **Global Settings > Directory Servers** in the left window pane.
2. Select the directory server node for which you want to verify the connection in the left window pane.
3. Select **Edit > Check Connection** .
   The console will verify its connection with the directory server and make the results known in a message box displayed on the screen. The results are either `Connection successful!` or `Connection failed!` If the connection failed this could be due either to a physical issue with the network or some incorrectly entered directory server data.

Deleting a Directory Server

To delete a directory server, proceed as follows:

1. Select **Global Settings > Directory Servers** in the left window pane.
2. Select the directory server to be deleted in the right window pane.
3. Select **Edit > Delete** .
   The selected directory server was deleted immediately.

Managing licenses

From the **Licenses** node of the the **Global Settings** page, you can manage the BMC Client Management licenses within your network. Licenses control your access to functionalities on the console. If you do not have required license for a functionality, the respective main node is not visible at all and the subnodes (such as assigned devices or assigned device groups) are dimmed.

If you are evaluating BCM features with the temporary license that comes on the product DVD, a maximum of 20 agents can be licensed for a period of 30 days.

While planning to purchase licenses, you can either purchase the complete license suite or purchase license modules for specific BCM features depending upon your business needs. For example, when you purchase the BMC Client Management - Inventory commercial license module, you get access to Application Management, Inventory licenses.

This topic includes:

- Available licenses and commercial license modules for BMC Client Management
- License utilization
- License types
  - Full License
  - Temporary License

For more information about license management operations, see:

- Viewing license information
- Importing Licenses
- Evaluating Licenses
- Searching and viewing events by license feature

Available licenses and commercial license modules for BMC Client Management

The following table describes licenses that are bundled with commercial license modules:

License	Description	Commercial License Module
Application Management	Activates all the different options of application management, that is, the monitoring and prohibiting of applications and self-healing functionalities as well as the software license management for Windows devices, application monitoring, prohibiting and software license management for Linux devices.	BMC Client Management - Inventory
BCM Agents		All licenses

License	Description	Commercial License Module
	The basic license of the product; it provides you with the maximum number of agents installed on clients which the database accepts. For the initial and evaluation license this number is fixed at 20. Note that unconnected devices for which the inventory is integrated do not decrease this value (that is, these devices are not counted for licensing purposes).	
Compliance Management	Activates the device compliance management of BMC Client Management. If you want to include software compliance you require the Software Catalog-specific license as well.	BMC Client Management - Compliance Management
Direct Access	Provides the direct access features to the remote clients of your installation.	BMC Client Management - Remote
Inventory	Activates all base inventories: software, hardware, custom, connectivity, security, and the inventory of unmanaged devices. All other inventory types are part of their respective functionality.	BMC Client Management - Inventory
Multicast	Activates the multicast transfer option for transferring packages and other information between the CM agents.	All licenses
Operating System Deployment	Activates the operating system deployment module which allows you to create OS images and deploy them to any device within your network. This feature is only available for Windows devices.	BMC Client Management - Deploy
Patch Knowledge Base Update	Required to maintain the patch knowledge base up to date on which the patch management functionality is based.	BMC Client Management - Patch Management
Patch Management	Defines how many devices can be patched at the same time. For the initial and evaluation license this number is fixed at 20. This license is not available for Linux or Mac OS devices.	BMC Client Management - Patch Management
Power Management	Activates the Green IT / Power Management feature.	BMC Client Management - Compliance Management
Remote Control	Activates the remote control feature. This feature is not available for Linux devices.	BMC Client Management - Remote
Security Configuration Updates	Required to maintain the Security Products catalog up to date, which is required for the Security Products inventory.	BMC Client Management - Compliance Management
Software Catalog Updates	This license is required to maintain the Software Catalog up to date.	BMC Client Management - Compliance Management

License	Description	Commercial License Module
Software Catalog	Activates the Software Catalog option. It is used for software inventory, software compliance, software license management and application management.	BMC Client Management - Compliance Management
Software Distribution	This license activates all software distribution features of the product such as package generation and scheduling the distribution.	BMC Client Management - Deploy
Super Master	This license is required for a super master architecture with a super master and a number of site masters.	BMC Client Management - Compliance Management
Topology Graph	Activates the graphical display of your network topology.	All licenses
Windows Device Management	This license activates the peripheral device monitoring and controlling functionalities for Windows devices.	BMC Client Management - Compliance Management

License utilization

The following table explains how a license is consumed or released:

License	Consumed when...	Released when...
BCM Agent	• An agent uploads its identity. • A mobile device is enrolled and is integrated in the database. **Note** A deprecated/unmanaged device does not consume a license.	• An agent or a mobile device is removed from the database. • An agent is deprecated.
Compliance Management	• A device is assigned to at least one Compliance Rule. • An agent collects Security Product Inventory. • An agent is assigned to a SCAP job.	A device is no longer assigned to any compliance rule, Security Product Inventory of an agent is purged, and an agent is no longer assigned to any SCAP job.
Software Catalog	An agent collects Software Catalog inventory	Software Catalog Inventory of an agent is purged.
Inventory	A device (except a deprecated device) collects at least one of the following inventory types:	All inventories for a device (except a deprecated device) are purged.

License	Consumed when...	Released when...
	• Custom • Hardware • Software • Security Settings • Connectivity • System (iOS) ⚠ An unmanaged device on the network consumes an inventory license if it collects Hardware and Software inventory.	
Application Management	An agent is assigned to at least one Application List.	An agent is no longer assigned to any Application List.
Patch Management	An agent collects Patch Management Inventory.	The Patch Management Inventory of an agent is purged.
Direct Access /Remote Control	One license allows remote control/direct access to unlimited devices.	Direct Access/Remote Control license is never released. It may be released if you import a new license without this functionality.
Operating System Deployment	One license allows deployment of unlimited OS on unlimited devices	Operating System Deployment license is never released. It may be released if you import a new license without this functionality.
Software Distribution	An agent is assigned to an operational rule with type Software Distribution.	An agent is no longer assigned to any operational rule of type Software Distribution.

Windows Device Management	• An agent collects Windows Devices Event Log.
	• An agent is assigned to an operational rule with one of the following steps:
	  • Create Device Management Rule
	  • Disable Windows Burning Service
	  • Disable USB Storage Write Access
	  • Disable Wi-Fi for LAN Connection
	  • Enable Windows Burning Service
	  • Enable USB Storage Write Access
	  • Reset Device Management Rule
	  • Wi-Fi Status Verification
		An agent is no longer assigned to any operational rule with the listed steps and has no Windows Devices Event Log.

Power Management	• An agent collects Power Management Inventory.
	• An agent collects Power Management Event Log.
	• An agent is assigned to an operational rule with one of the following steps:
	  • Delete Power Plan
	  • Hibernate
	  • Define Power Plan
	  • Suspend
		An agent is no longer assigned to any operational rule with the listed steps and has no Power Management Event Log or Inventory.

License	Consumed when...	Released when...
	• Update Power Management Inventory • Create/Modify Global Power Policies • Create/Modify Power Plan • Create/Modify Advanced Power Plan	

License types

Full License

This license provides the necessary access to the software and its basic components. When it is imported it will erase any previously imported license, such as an earlier full license or a temporary license. This type of license defines the number of licenses that are available for each purchased functionality. If a functionality exceeds its license count all administrators with the capability to manage licenses will be notified of this fact by email, if they have one defined in their profile.

Also, when the console is opened a pop-up-window appears to inform you which licenses have exceeded. In this case some functionalities such as assigning objects to each other might no longer be available under the respective nodes.

Temporary License

Each DVD of the software comes with a temporary license which is valid for all features but limited to 20 devices and 30 days of usage after installation. When installing the master a selection of the features to be evaluated must be made which are then included in this temporary license.

This type of license cannot be combined with any other license, as soon as you import any other type of license it is erased. In the same way all already existing licenses will be removed when you import a temporary license. If this license expires without being replaced by a full license, only the only node shown in the console will be the license node, no other object will be accessible anymore.

If a license is expired all administrators with the capability to manage licenses will be notified of this fact by email, if they have one defined in their profile. Also, when the console is opened a pop-up-window appears to inform you which licenses have expired. In this case the respective nodes will no longer appear in your console.

Viewing license information

The main **Licenses** tab provides the following information about the available licenses.

Column	Description	
Name	Displays the name of the license. This can be either BMC Client Management for the basic license of the software, or the names of individually licensed modules, such as ***Remote Control*** .	
Count	Indicates for how many agents the license is valid for the basic license.	

Column	Description	
Available	This column indicates the number of remaining licenses.	
Expiry Date	If the license is a limited license, such as an evaluation license, this field displays its expiry date, in the default format defined in the user preferences. The basic license which comes with the software is limited to 30 days after the date of installation. If the license is unlimited this field remains empty.	
Status	**Valid**: This value shows that the current license is valid and working. **Expired**: This value indicates that the system date is after the expiry date for the license. This means that the license is effectively invalid and must be renewed to work again. **Expiring**: This status warns you that your current license is about to expire. The status will change to this value 15 days before it will actually expire. **Exceeded**: This value indicates that the date until which the license was valid was passed. The license is therefore effectively invalid and must be renewed. **Invalid**: This value indicates that the current license is invalid. Licenses in the BMC Client Management are stored in the database with a checksum, which can legally be modified through newly imported licenses. If the license is changed any other way than through the console and an imported license, such as directly via the database, the license will become invalid.	

Importing Licenses

Licenses are not entered manually, they can only be imported via files which contain the licensing information. You need to import the initial license before starting to work with the console and you can add any type of license to your currently existing licenses.

To import licenses, proceed as follows:

1. Select **Global Settings > Licenses** in the left window pane.
2. Select **Edit > Import License** .
   A dialog box opens displaying your directory structure in which you need to select the file containing the new licenses.
3. Select the license and click **Open** .

The license will be automatically added to the existing licenses if it is a new license or it will overwrite the "old" information, if the license already exists and is upgraded or renewed.

The information is then read from the file and displayed in the table in the right window pane.

If the new license adds new functionalities to your installation, the required modules will automatically be loaded.

Evaluating Licenses

It is possible at any time to launch a manual re-evaluation of all licenses and their current situation.

To evaluate the licenses, proceed as follows:

1. Select **Global Settings > Licenses** in the left window pane.
2. Select **Edit > Evaluate Licenses** .

The license data will now be re-evaluated for all available licenses and the display will be updated.

Searching and viewing events by license feature

This tab displays the list of all events registered for the selected license feature.

This view provides the following selection options which can be combined for the display:

Parameter	Description
License Type	Select from this list the license type for which to display the logged events. Only those license types are displayed for which events have occurred. If there are no license events this list remains empty.
Start Date	Select in this box the date from which on the logged events are to be displayed. Click the down arrow to open the calendar to select a value. To remove the entry in this box click **Remove**
End Date	Select in this box the date up to which the logged events are to be displayed. Click the down arrow to open the calendar to select a value. To remove the entry in this box click **Delete**
Find	Select this button to apply the filter to the events and display them.
Purge	To permanently delete all events corresponding to the filter defined in the preceding explained fields click **Purge**

After the desired events are found the following details are displayed:

Column	Description
Device Name	The name of the device for which the event occurred.
Event Date	The date and time at which the event about the license management was logged by the agent.
Type	The object type for which the event occurred, for example, Compliance Rule.
Status	This field displays the license status for the event, for example, `License expired` or `License Exceeded` .
Description	This box can contain a further textual information the license event. For example for an exceeded compliance license this might display the name of the compliance rule at which the license exceeded.

Managing system variables

The **System Variables** (**Global Settings > System Variables**) node provides tabs for all types of variables which control the behavior of the master server.

This section includes the following topics:

- Managing security settings
- Managing event and logging settings
- Managing BCM agent connection behavior
- Managing email settings
- Managing default operational rule settings
- Managing device menus
- Managing packages settings
- Managing patch group settings

- Managing report settings
- Managing software quality metrics
- Managing user settings
- Managing quick search settings
- Managing company logo
- Managing Remedy SSO parameters

To modify system variables

1. Select **Global Settings > System Variables** in the left window pane
2. Select the tab of the desired topic in the right window pane.
3. Select any line in the table in the right window pane.
4. Select **Edit > Properties** .
   The **Properties** window appears.
5. Make the desired changes in the respective boxes.
6. Click **OK** to confirm.
   The new settings are taken into account immediately.

Managing security settings

From the **Security** tab of the **Global Settings > System Variables** page, you can define the following default security settings of your system:

Parameter	Description
Create Default System Administrator	The value in this field defines if system authentication is used for logon. If the value set is `Yes` , your general system login can be used. This means that all attempted logins which are authenticated by the system cause a matching login to be created in the database. For security reasons, however, no capabilities will be assigned to these logins. All of these automatically created administrator logins have their **System Password Check** box in the **Properties** window checked. If the value is set to `No` , a specific user login must be created for each administrator to log on to the BMC CM console. The default value for this attribute is `No` . For more information about how to create administrator logins, refer to the What you have to know about Administrators topic.
Display Hidden Devices in the Topology Graph	This parameter defines, if users without read access rights to the master or relays can view their devices in the topology graph. By default this option is set to `No` , they cannot. If the option is activated, the administrator can see the part of the topology including the devices on which he has access rights but all devices on which he does not have at least read access, that is, master and relays will appear dimmed and are not accessible. All other devices on which he has no access rights will not appear in the view.
Maintain Administrators at Directory Server Synchronization	This parameter defines if administrators are also removed from synchronized groups during resynchronization. Normally, if an administrator is removed from his AD group it will also be removed from his CM group during the next synchronization. However, if the capabilities or access rights of this administrator are transferred via the administrator group, this might cause a number of problems, if the administrator in question is assigned as a populator for groups for example, causing the groups to "depopulate" and if operational rules are assigned to this group, they will be unassigned from the devices of the group.
Disable all administrators that are not a member of any	As administrators might have functionalities that are to be transferred to other administrators when they are deleted, such as being a populator, it is not possible to automatically delete administrators if they no longer belong to any group. This option allows however, to disable the administrators that are not a member of any administrator group to distinguish them. By default this option is deactivated.

Parameter	Description
group at a directory server synchronization	
Allow Object Assignments to Unknown Device	If this option is activated devices unknown to the CM database can be assigned to the available objects, that is, operational rules, transfer windows, and so on. In this case the unknown device displays the **Assigned Objects** node in addition to the **Inventory** and **Events** nodes. After the device becomes known to the database it will synchronize all assigned objects and thus be operational automatically. By default this option is not activated.
Block Access to MyApps	**Block Access to MyApps** This option deactivates the access to the application kiosk MyApps of the browser agent interface. If it is activated neither user nor administrator can access this page.
Authorize Deprecation of Relays	Check this box to allow the deprecation of relays even though it still is the parent to other devices. In this case the relay will be moved to **Lost and Found** from where it can be deleted and its former children will be removed from the **Topology** view but they can still be displayed via their device groups.
Request System Credentials for Windows Remote Access	Check this box to force the use of credentials when directly accessing Windows devices. In this case you is required to enter your credentials when accessing the target device via the Direct Access or Remote Control functionality.
Request System Credentials for Linux Remote Access	Check this box to force the use of credentials when directly accessing Linux devices. In this case you is required to enter your credentials when accessing the target device via the Direct Access or Remote Control functionality.
Request System Credentials for Mac OS Remote Access	Check this box to force the use of credentials when directly accessing MAC OS devices. In this case you is required to enter your credentials when accessing the target device via the Direct Access or Remote Control functionality.
Remote Access Acknowledgement Timeout (sec)	This parameter defines the timeout in seconds after within which the remote user can allow remote access request to an administrator. If the timeout is reached the administrator is informed that the remote user did not respond within the time allowed for the direct access or remote control request. If the value is set to zero, the timeout functionality is disabled.
Lock the new installed agent services	Check this box to lock the newly installed agent services.
Service Unlock Password	Enter the service unlock password.

Managing event and logging settings

In the **Event Management** tab of the **Global Settings > System Variables** page, you can define the following default settings for the event and alert logging functions of your system:

Event : An event is any action that is initiated either by the user or the device.

Alert : An alert is any type of event for which a notification can be sent if required.

The table of the **Event Management** tab displays the following information:

Parameter	Description
Maximum Number of Alerts to Store in History	This entry defines the maximum number of all alerts logged into the database. After this number is reached and a new event is generated, the new event will replace the "oldest" event currently logged in the database. The default value for this number is ***10000*** .
Maximum Age for Events in History (days)	Defines the maximum time in days that persistent events stay logged in the database. The default value is ***365*** days.
New Alert Check Interval (sec)	The time interval after which new alerts are checked. The default value is 3600 seconds. If set to 0, the check is deactivated.

Managing BCM agent connection behavior

From the **Global Settings > System Variables > Connection Management** tab, you can define the default settings for how connections to devices are managed.

This topic describes the settings that define the connection between a BCM agent and the BCM master database.

- Defining the agent connection settings
- Which attributes are used to generate GUIDs
- How BCM generates GUIDs for devices
- How is GUID generated when a BCM agent is re-installed on devices
- Connection Parameters

Defining the agent connection settings

Modifying any of these values affects the entire operation of BMC Client Management. It is therefore strongly recommended to make the definition of these settings part of the initial planning before any deployment to your network. If, however, you execute any changes later on, you must restart the agent service on the master server before launching a network rollout process.

Which attributes are used to generate GUIDs

The attributes used to generate GUID are defined on the **Global Settings > System Variables > Connection Management** tab.

- **Use the serial number of the main logical volume disks to uniquely identify device**
- **Use host ID to uniquely identify device**
- **Use the domain name to uniquely identify device**
- **Use the MAC address to uniquely identify device**
- **Use the NetBIOS name to uniquely identify device**

How BCM generates GUIDs for devices

For eliminating duplicate Global Unique Identifiers (GUIDs) associated to devices, BCM has enhanced its GUID generation mechanism. The new mechanism uses all the attributes to generate a GUID. Therefore, any change in the attribute values does not cause BCM to consider the device as a new device. BCM performs an attribute match in the master database. If an attribute match is

found, the registered GUID for the device is retained in the database. This ensures that GUIDs are not duplicated in the master database and there are no communication issues between the master database and the agents.

The only case where the mechanism changes is when an agent needs to be re-installed on a device.

How is GUID generated when a BCM agent is re-installed on devices

When a BCM admin rolls out an agent on a device for the first time, the agent generates a new GUID for the device. For some reason, if the agent needs to be re-installed on the same device, the agent regenerates a GUID for that device. This creates multiple GUIDs for the same device.

BCM does the following to ensure GUID uniqueness:

- Checks whether there are two GUIDs
- Finds a match between the new GUID values and the existing GUID values in the BCM database
- If BCM finds GUID values that match, it replaces the existing GUID in the BCM database with the new GUID
- Records the new GUID value in the BCM database

Connection Parameters

From BMC Client Management 12.6 onwards, BMC Client Management uses all the attributes of a device to generate GUIDs, irrespective of whether an attribute is enabled or not. These system variables are used to uniquely identify a device in the master database.

Parameter	Description
Use the domain name to uniquely identify device	Check this box if you want to use the host name to uniquely identify the device. For most companies this attribute would be the most recommended, because in their networks the host names of the clients are in almost all cases unique. If the names are not unique but this option is nevertheless to be used for identification, make sure to select the **Complete Name** option for the **Client Identification Type** , otherwise one or more of the devices with the same name cannot be recognized as different clients if you have not activated the following option **Allow Duplicate Device Names** .
Use host ID to uniquely identify device	Check this box if you want to use the host ID to uniquely identify the device. Do not use this option if you do not have a system with exclusively new devices, because this attribute is only unique if the clients have WMI. If the clients do not have WMI the value returned is empty.
Use the NetBIOS name to uniquely identify device	Check this box if you want to use the NetBIOS name to uniquely identify the device.
	Check this box if you want to use the MAC address to uniquely identify the device. Do not use this option if you switch network cards between devices or have devices with several network cards.

Parameter	Description
Use the MAC address to uniquely identify device	
Use the serial number of the main logical volume disk to uniquely identify device	Check this box if you want to use the serial number of the main logical to uniquely identify the device. Do not use this attribute if you use ghosts in your network.
Automatically Update Device Name	Check this box if the device name is to be automatically updated when it is changed. By default, the box is enabled. If this functionality is disabled, only the NetBIOS name will be updated to the device's new name if it is changed. This functionality should only be used in environments in which a lot of name changing takes place such as through regular ghosting, to ensure consistency in device tracking and identification as well as reliable queries.
Case of Device Name	Specifies if the names of the devices are to be case sensitive. By default this option is set to **Indifferent** , indicating that the name will be entered into the database in exactly the way it was entered by the user. If for example, the option **Upper Case** is selected and the name is entered in a mixture of upper and lower case letters the name will be automatically stored in the database with upper case letters only, and vice versa for the option **Lower Case** .
Client Identification Type	Defines the identification type used when a new client is installed. If the value entered exists already in the database, the client is regarded as an already existing device and will not be added again. The possible types of identification are the following: **Complete Name** , **Host Name** , **IP Address** and **NetBIOS Name** . If the network names of your clients are not unique and you are using the host name to uniquely identify the devices, this variable must obligatorily be set to **Complete Name** . Otherwise one or more of the devices might not be recognized as different clients. Also, if you are using a super master architecture this value is strongly recommended to be used, to avoid cases in which two devices could have the same short name in two different sites. In such a case the super master would regard these two devices as one, therefore only store one device and each new upload from one or the other site master will overwrite the previous data in the database.
Lost Client after Delay of	Defines the time interval which can elapse after the last update from a client agent before it is declared as lost. The default value is ***24 (hours)*** .
Unit for Lost Client	Defines the unit for the value defined in the preceding field. Possible values are ***Seconds*** , ***Minutes*** , ***Hours*** , ***Days*** and ***Weeks*** .
Lost Relay after Delay of	Defines the time interval which can elapse after the last update from a relay agent before it is declared as lost. The default value is ***24 (hours)*** .
Unit for Lost Relay	Defines the unit for the value defined in the preceding field. Possible values are ***Seconds*** , ***Minutes*** , ***Hours*** , ***Days*** and ***Weeks*** .
Allow Duplicate Device Names	Check this box if devices with the same name and IP address are considered as the same device or as different devices. If this option is deactivated, that is, set to No, a second device with the same name and IP address will be considered to be the same device as the first one and thus will update the old data with its new data. If the option is activated, the second device will be created as a new device with the same name as the first suffixed by a number, that is, scotty for the first device, scotty (1) for the second.

Parameter	Description
Automatic Agent Version Upgrade	Check this box to ensure that the environment's agent are automatically upgraded once the master is upgraded to a new version.
List of banned GUIDs	Allows the administrator to provide a comma separated list of prohibited GUIDs. The Identity module on the devices regulary checks if this list has changed. When a device generates its GUID it verifies that the generated GUID is not part of the list. If this should be the case the GUID generation is cancelled.

Managing email settings

From the **Mail** tab of the **Global Settings > System Variables** page, you can define the default settings for the email system. When defining the mail server, the agent will try to establish a connection with the server via the entered values to make sure all entries are correct. If the connection cannot be established, an error message is displayed and the window can only be closed by entering the correct values or via the **Cancel** button if you do not have the correct information.

Name	Description
Mail Server Name	Defines the name of the mail server to which all mail is set for routing, the default is `localhost` .
Mail Port Number	Defines the port number of the mail server, the default value is ***25*** .
Encryption	This parameter defines if the mail server requires encryption for its communication, possible values are **Force encryption** , **Encrypt if possible** or **Never Encrypt** .
Encryption Type	If the mail server requires encryption this text box defines which type of encryption is used, such as ***sslv2*** , ***sslv3*** , ***tlsv1*** , and so on.
Authentication	This parameter defines if the mail server requires authentication for its communication, possible values are **Force Authentication** , **Authenticate if possible** or **Never Authenticate** .
Authentication Type	Enter into this text box the type of authentication to be used for connections to the mail server. If no authentication is required this text box can remain empty.
User Name	Enter into this text box a valid login to the mail server. This can be any login, not necessarily that of the user defining his preferences in via these options.
Password	The corresponding password.
Alert Administrator Email Address	Enter the email address that is to send the email alerts to the recipients, for example, ***alertmanagement@myspycompany.com.***
Type of email for alerts	Defines how much information the alert email contains: **Notification only** - only informs the administrator that alerts occurred and should be checked in the respective node in the console. **Complete (full alert detail)** - contains the full details of the alert, that is, the same information as in the alert view of the console.

Name	Description
Maximum number of alerts to include	This parameter is only applicable if the option **Complete (full alert detail)** is selected for the email content. In this case if the threshold defined for this parameter is reached, the content of the mail will automatically be switched to the **Notification only** content.

After setting up the email, you need to verify the settings.

To verify email settings,

1. Select **Global Settings > System Variables** in the left window pane
2. Select the **Mail** tab in the right window pane.
3. Select any row in the table in the right window pane.
4. Select **Edit > Properties** .
   The **Properties** window appears.
5. Click **Verify** at the bottom of the window.
   A pop-up menu appears displaying the result of the verification. If an error has occurred it indicates which part of the verification produced the error.

Managing default operational rule settings

From the **Operational Rules** tab of the **Global Settings** > **System Variables** page, you can specify the following default parameters of the operational rules:

Parameter	Description
Automatic general operational rule reassignment after device reinstall	This column defines if the general operational rules are to be automatically reassigned after a client was reinstalled. By default this value is ***No*** , indicating the rules will not be automatically reassigned.
Limit Operational Rule Dependencies	This parameter defines if dependencies are taken into account when assigning an operational rule to a group. Possible values are Yes and No, the default value is No. Yes indicates that if an operational rule has a dependency on another rule that is ***NOT*** assigned to the this group, the dependency is ignored and the operational rules will be executed in the order defined but without the missing rule. If you select No for the same case as the preceding one, you either must also assign the missing rule to the respective group or remove the dependency from the current rule.
Wake Up Switched Off Devices	This parameter defines if by default devices that are switched off when an operational rule is assigned to a device or device group are to be woken up via the WOL option when the assignment is sent. By default this option is deactivated.
Upload intermediary status values for operational rules	This option activates the choice to upload all status values, that an operational rule execution (general as well as software distribution) runs through or only to upload the final status values. By default this option is activated, that is, all status values are uploaded. Contrary to all other packages, the ConfigFiles.cst package does not use this parameter.

Parameter	Description
Automatic software distribution rule reassignment after device reinstall	This value specifies if the software distribution rules are to be automatically reassigned after a client was reinstalled. By default this value is No, indicating the rules will not be automatically reassigned.
Status Modification Window	This parameter defines if the modification of an operational rule, that is, when a step was added or removed, etc., is to impact the operational rule status of all assigned devices. By default this option is deactivated, that is, no status will be modified.
Modify the operational rule schedule when importing a CSV file	This parameter specifies if for devices that are imported to a device group to which operational rules are assigned a specific schedule for these operational rules can be defined. By default this value is deactivated. If set to Yes, a pop-up menu will provide the possibility to modify the existing operational rule schedule.
Automatic dependency activation of published operational rules	This parameter enables/disables the automatic execution of dependencies of advertised rules (for both user and device). If the parameter is enabled, no pop-up displays and dependencies are automatically assigned (if necessary) to the device when a rule is selected via MyApps. Else, a pop-up displays that the dependency check has failed and the operation rule thus could not be executed.However a reduced dependency management is still done even with this option disabled. It is possible only if all dependencies are present on the device, else the `Verification Failed` status will appear.
Take chronological dependencies into account after device reinstall	Defines if the chronological dependencies of operational rules are taken into account and followed during resynchronization after a device reinstall. By default this option is activated. Deactivating this option makes the rule synchronization faster, however, this might lead to inconveniences or even problems on the devices if some rules which are dependent on each need to be executed in the specified order for proper functioning.
Remove relations with devices created by MyApps	After an optional rule is unassigned from a user assignment, the user can no longer activate it via MyApps . If this option is activated, all devices are automatically unassigned if the link between the user the rule is removed. By default this option is not activated.
Automatic creation of the operational rule when a package is published	For a package to be distributable and installable a corresponding operational rule must exist that defines the operations to execute during the package installation. This parameter defines if this rule is automatically created when a package is published. The value is applicable to all types of packages. By default this option is not activated, that is, the rule is not created.
Automatic reassignment of all general operational rules if the local database is corrupted	This parameter defines if all general operational rules are to be automatically reassigned after the recreation of a corrupted local database. By default this value is ***No*** , indicating the rules will not be automatically reassigned.
Automatic reassignment of all software	This parameter defines if all general software distribution rules are to be automatically reassigned after the recreation of a corrupted local database. By default this value is ***No*** , indicating the rules will not be automatically reassigned.

Parameter	Description
distribution rules if the local database is corrupted	
Take chronological dependencies into account at the first device installation	Defines if the chronological dependencies of operational rules are taken into account after the first installation of a device. This option is useful if your environment relies heavily on device provisioning. After the new devices have uploaded their identity for the first time, all their assignments are already in place and will be activated directly.

Managing device menus

You can create specific menu items for devices. After being defined, these can be called and executed on any device which is part of your system. The menu items are created under a new menu section called **Customized Menus**, which is appended to the regular pop-up menu for a device. This section is only available for pop-up menus called in the left window pane.

This topic includes:

- Creating a device menu
- Deleting a device menu

You can create menu items for the following different types of operations to be executed on the selected device:

- launching an executable file
- opening a web page
- defining a command line to be executed

> **Note**
>
> You need the **Manage Direct Access** capability to be able to see and use these custom menus.

The device menu list displays the following information:

Column	Description
Name	This column lists all the menu items defined for the personalized device menu.
Value	These fields display the respective action that is to be taken when calling the menu item, such as for example, `<installation path>/calc.exe` to launch the calculator.

Creating a device menu

Individual actions and operations can be added to the pop-up-menu of a device when called in the left window pane.

1. Select **Global Settings> System Variables** in the left window pane
2. Select the **Device Menu** tab in the right window pane.
3. Select **Edit> Create Device Menu** .
   The **Properties** window appears.
4. Enter the data into their respective boxes:

Parameter	Data
Name	Enter a short descriptive name for the action this menu item is to execute, for example, Registry Editor.
Value	Enter the value for the action to execute in this text box, which depends on the type of the menu. For example to run the calculator enter the path to the executable file, <installation path>/calc.exe, or http://\ {DeviceName}:<port number> to launch a web page.The following device attributes, which are case sensitive and must always be enclosed in braces ({}), can be used for all types of device menus, but they are not mandatory. These attributes will then be replaced by the real value of each device, for example, ping {IPAddress} will be translated to ping 192.196.1.1 for a device with that IP address. DeviceName HttpPort IPAddress NetworkName NetbiosName MACAddress HostID AssetTag PrimaryUser
Menu Type	In this drop-down box the type of the menu, possible values are: Command Line to execute a command line, Executable to launch a program via its executable file on the selected device and HTTP to open a specific web page on the device.

5. Click **OK** to confirm the new menu item.
   The new device menu item was created.

Deleting a device menu

1. Select **Global Settings > System Variables** in the left window pane
2. Select the **Device Menu** tab in the right window pane.
3. Select the device menu to be deleted in the right window pane.
4. Select **Edit > Delete Device Menu** .
   The **Properties** window appears. The menu item is directly deleted from the list and database.

Managing packages settings

From the Packages tab of the **Global Settings** > **System Variables** page, you can define default settings for all types of supported packages.

Parameter	Description
Activate Network Installation Option	This option allows to define if the network installation is possible for MSI and custom packages and the administrative install for MSI packages.By default this option is not activated. Administrative installation in this case means, that the package will not be downloaded to the target client but remains on the relay and the installation will be executed from the relay. The network installation is very similar to the administrative installation with the

Parameter	Description
	difference that the package is only extracted at the relay and the clients will launch a normal installation via the network. An administrative installation will install the package on the network and the targets will simply execute the installed package. The advantage of an administrative installation compared to a network installation lies with regards to patches which are to be applied to packages: If the package is patched future target clients will directly install the patched version of the package. If a network installation is used clients first install the version without the patch and then need to install the patch on it separately.Be aware that this option is only applicable to packages which were created with a packager of version 5.3.1 or later. If you would like to use packages created with an earlier version, you need to send them back to a packager, modify them (the checksum must change) and then republish them.

Managing patch group settings

From the Patch Group tab of the **Global Settings > System Variables** page, you can define the general behavior of patch groups.

Parameter	Description
Information Window for Patch Group Activation	This option defines if an information window is to be displayed to the user after he has modified a patch group. It warns the user that an activation of the patch group is necessary to take into account any modifications.
Show effectively installed patches in patch jobs	This option effectively shows the number of patches installed after the last patch was installed. For example, on a Windows system, if you install a patch that replaced the 20 earlier patches, then the last patch has effectively installed the earlier 20 patches.
Remove old patches automatically	This options removes old patches that are not referenced anymore in patch groups and patch jobs are automatically removed from the system.

Managing report settings

Define the settings for style-based reports and know how to customize logo for reports.

Report parameters

From the Reports tab of the **Global Settings > System Variables** page, you can define some default settings for the style-based reports.

Parameter	Description
Encoding	Defines the encoding to be used by default when creating reports.
Style Sheet	Defines the style sheet to use by default when displaying style-based reports in one of the following ways: • From the console, you can browse for a style sheet and apply it for style-based reports. • 2 files are delivered with the software, but you can adapt these to your requirements or add custom style sheets. These must be located in the `<InstallDir>/data/Vision64Database/reports/common/css` directory of the master. The **BMC.css** file is the default file. It has a default width of ***1024 pixels*** . The `Compatible.css` file has the same values as the **BMC.css** file but no fixed width and is to be used if you are upgrading from an earlier version to be used with existing reports.

Customize report logo

The logo is only applied to style-based reports. It cannot be applied to template-based reports.

You can either select an available logo from the drop-down list or add a new logo for the report.

1. Click **Browse**.
2. Select the image and click **Open**.
3. You can resize the image by using the cropping tool that borders the selected image. You can zoom in or zoom out the image by using the pointing device (mouse wheel) on your computer.
4. Click **OK**.
5. To apply the selected logo, click **Apply**.
6. To reset back to the default logo, click **Reset**.

> Note:
>
> You cannot delete a logo from the console.
>
> If you do not want any logo on the reports, do not select any logo from the drop-down logo menu. The logo name is the same as the filename.
>
> Supported formats are PNG and JPG
>
> Minimum logo size is 272 x 91 pixels

Managing software quality metrics

From the **Software Quality Metrics** tab of of **Global Settings > System Variables** , you can d efine the default behavior of the BMC Software Quality program. You can set the following parameters:

Parameter	Description
Enable software quality metrics	Activates sending product usage information to BMC Software; if it is deactivated the following 4 parameter values are ignored and no data will be collected and sent. The default value is as defined during the installation/upgrade process for the master.
Send anonymous data	Allows to send all data collected about the product usage as anonymous user.
Gather system environment	Allows to gather information about the system, the operating system version, the hardware, and so on.
Gather product usage statistics	Allows to collect information about the usage of the product.
Gather product performance data	Allows to collect information about the performance of the product, for example, the connection times between console and server, etc.
Enable satisfaction survey when a new administrator is created	Allows all newly created administrators to participate in a satisfaction survey about CM , that is, the respective parameter (**Enable regular prompts for participation in on-line satisfaction surveys**) in the **Preferences** is activated.

Managing user settings

The **Users** tab of **Global Settings** > **System Variables** page defines specific parameters for BMC Client Management users.

The following parameters are available:

Parameter	Description
User Identification Type	Defines the identification type used when a new user is created. If the value entered exists already in the database, the user is regarded as already existing and will not be added again.
Case of User Name	Specifies if the names of the users are to be case sensitive. • **Indifferent:** The name will be entered into the database in exactly the way it was entered by the user. • **Upper Case:** If the name is entered in a mixture of upper and lower case letters, the name will be automatically stored in the database with upper case letters only. • **Lower Case:** If the name is entered in a mixture of upper and lower case letters, the name will be automatically stored in the database with lower case letters only.

Managing quick search settings

The **Quick Search** tab of the **Global Settings** > **System Variables** page provides an easy means of finding devices that match one or more specific criteria.

The information that is indexed for a device are its identity, and its hardware and software. The indexing of the available device information is managed via the following two parameters:

Parameter	Description
Update	This schedule defines the frequency with which the database is checked for new or updated objects, which are then indexed right away, if any are found.
Maintenance	This parameter defines the frequency with which the database is searched for deleted objects which are then removed from the index. BMC recommends to not run this operation too often or only during quiet times, such as during the night or on weekends, as the process is quite time and resource consuming.

Both parameters display the following details:

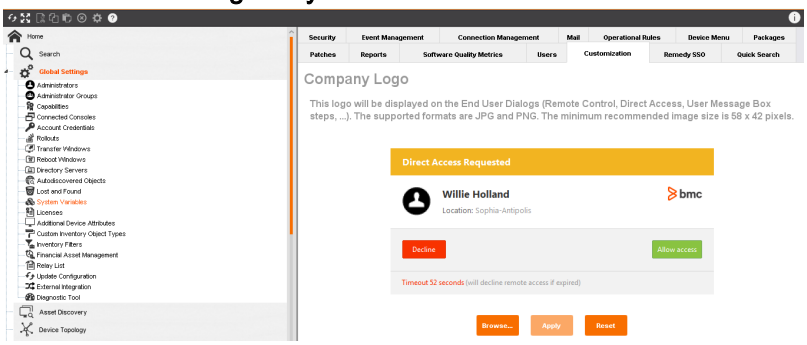
Parameter	Description
Status	The current status of the index operation.
Last Indexed Time	Displays the date and time at which the last index operation was executed.
Activation	This field shows the condition on which the index operation will start executing.
Schedule	The fields of this column display the frequency with which the index operation will be executed.
Termination	This field displays on which condition the index operation will definitely terminate its execution cycle.

Managing company logo

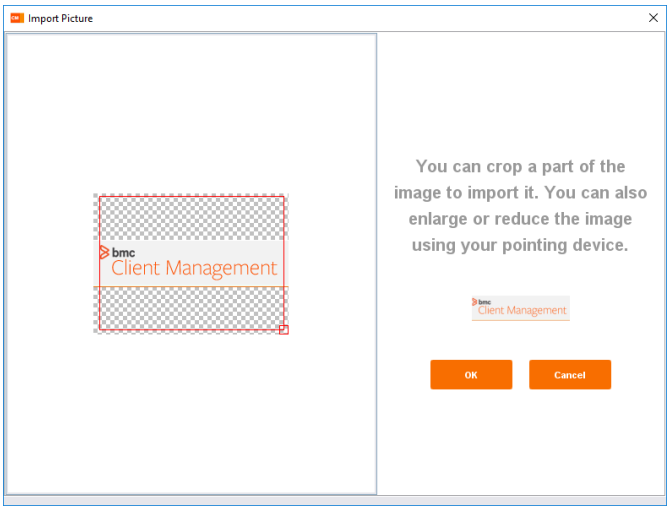
The **Customization** tab of **Global Settings** > **System Variables** page defines specific parameters for BMC Client Management users.

To customize the company logo that appears on end-user dialogs such as, Remote Control, Direct Access, User Message box and so on:

1. Go to **Global Settings** > **System Variables**.



2. In the **Customization** tab, click **Browse**.
3. Select the image and click **Open**.
4. You can resize the image by using the cropping tool that borders the selected image. You can zoom in or zoom out the image by using the pointing device (mouse wheel) on your computer.
5. Click **OK**.



6. In the **Customization** tab, click **Apply** to use the logo in all the end-user dialogs.

7. If you want to reset to the default logo, click **Reset**.

Your changes are applied to the sample dialog box shown in the tab.

> ⚠ The minimum recommended image size is 58 x 42 pixels.

Only PNG or JPG image formats are supported.

Managing Remedy SSO parameters

The **Remedy SSO** tab of **Global Settings** > **System Variables** page defines specific parameters required to integrate BMC Client Management with Remedy SSO server.

As a BCM administrator, you must get the following settings from a Remedy SSO administrator. The following parameters are required to configure Remedy SSO with BCM :

Parameter	Description
Enabled	Defines whether the Remedy SSO server authentication is activated.
RSSO Server URL	Enter the URL for the BMC Remedy SSO server. The Remedy SSO server URL must begin with https and have the same domain as the BCM master server. For example, use *bcm.calbro.com* and *rsso.calbro.com*.
RSSO Realm ID	A realm is a virtual identity provider used to authenticate a domain. Contact your Remedy SSO administrator for the Realm ID.
Product Identifier	Defines the identifier for BMC Client Management. The identifier must be unique for each application that provides authentication through Remedy SSO server.
RSSO Token revalidation period	Enter the revalidation period in minutes. For more information, contact your Remedy SSO administrator.
Certificate Authority Bundle	Configures the list of certificate authorities that BMC Client Management must trust when connecting to a Remedy SSO server.
Server Certificate	Defines the server certificate to accept when connecting to the Remedy SSO server.

For more information on configuring Remedy SSO server with BMC Client Management, see Integrating with BMC Remedy Single Sign-On.

Managing device object attributes

The **Additional Device Attributes** provides the ability to create, modify and delete attributes of a device object.

This topic includes:

- Adding additional device attributes
- Modifying additional device attributes
- Changing the order of device attributes
- Deleting additional device attributes

The table of the **Additional Device Attributes** node provides the following information about the unrelated items:

Information	Description
Attribute	Displays the name of the created attribute.
Type	Displays the data type of the attribute, for example string, integer, path, and so on.
Title	The display name of the column. This can but must not necessarily be the same as the Attribute name.
Display Order	Indicates the display order of the attribute in the **Properties** window of a device.

Adding additional device attributes

1. Select **Edit> Add Attribute** .
   The **Add Attribute** pop-up menu appears.
2. Enter the data for the new attribute in the respective text boxes.
   The Column Name text box is not displayed in the table of the node in the right window pane. You need to enter the database column name of the new attribute.
3. Click **OK** to confirm and close the window.

Modifying additional device attributes

1. Double click the attribute in the right window pane you want to modify.
   The **Properties** pop-up menu appears.
2. Make the desired changes in the respective boxes.
3. Click **OK** to confirm.

The new settings are taken into account immediately.

Changing the order of device attributes

1. Select **Additional Device Attributes** in the left window pane.
2. Select the attrribute to be moved in the right window pane.
3. Select **Edit> Move Up** or **Move Down** .
   The selected attribute was immediately moved up or down in the list. Repeat step 3 until the attribute is at the desired position.

Deleting additional device attributes

1. Select **Edit > Delete Attribute** .
   The **Confirmation** dialog box appears.
2. Click **Yes** to confirm.
   The selected attributes will be deleted immediately.

Managing relay list

In this view you can define the list of relays to use for the **Relay Selection** method of the same name. Each entry represents a relay that is defined as such for a specific subnet. It also specifies the relay's priority in case a child device is on two subnets, for example, if it is on WIFI and on a normal subnet the subnet relay has precedence over the WIFI relay.

Parameter	Description
Relay Name	The network name of the relay, either as its short or complete network name, for example, *scotty* or *scotty.enterprise.com* , or as its IP address in dotted notation, for example, *194.45.245.5* or *2001:db8:85a3::8a2e:370:7334* .
Client Subnet	The network address of the Subnet served by this relay (in the form of a single address, such as *192.168.1.0* or *10.5.50.128*).
Relay Port	The port number of the direct parent to which the device is to connect. If the port number is not listed the default port *1610* is assumed.
Priority	Defines the priority of the relay within the relay list. This decides to which relay a device is to connect if it finds itself with two or more possible relays. If two possible relays for a device have the same priority the agent selects the relay arbitrarily; the same applies if the value is set to *0* .

To add a new relay

To add a relay to the list of relays used by the **Relay Selection** method and configure its priority,

1. Click **Add Relay** .
   The **Properties** window opens.
2. Enter the information for the new relay into the respective boxes.
3. Define its priority in the **Priority** box.
4. Click **OK** to confirm.

Managing security

Security in general for BMC Client Management is defined through a number of different objects and methods, such as authentication/authorization, encryption, privacy and audits. Security for the console in BMC Client Management is ensured via a number of different methods and objects, one of these are the administrators and administrator groups. Each of these has a capability list which dictates what an administrator can do.

https://www.youtube.com/watch?v=w8EZNVwb9cc&feature=youtu.be

The following topics are provided:

- Understanding security components
- Understanding security operations and principles
- Managing security profiles
- Managing predefined administrator groups

- Managing access rights and capabilities for specific cases

Understanding security components

Security in BMC Client Management must be set up on two different levels: on the clients and on the console. It is defined through a number of different objects and methods, such as authentication /authorization, encryption, privacy and audits.

The following topics are provided:

- Administrators and administrator groups
  - Administrators
  - Administrator Groups
- Access rights and capabilities
- Security considerations
  - Capabilities
  - Access Rights

Administrators and administrator groups

Security for the console in BMC Client Management is ensured via a number of different methods and objects, one of these are the administrators and administrator groups. Each of these has a capability list which dictates what an administrator can do. The administrator and administrator group nodes and their capability definitions specify the access to the console in general, that is, who can interrogate or manipulate the database and its information.

Administrators

Every user that might need to log on to the CM console must be defined as an administrator in the BCM database with a login name and a password. These administrators can then be restricted in their capabilities to specific object types and operations and grouped accordingly.

Administrator Groups

Administrator Groups are a way of organizing all existing administrators within your system. The structure defined through your groups is individual and freely configurable by the responsible person. Administrators can belong to more than one group. Groups can be created for example according to the following criteria:

- geographical location and the administrator's function there,
- corporate structure and the administrator's position within, or
- assigned capabilities

Access rights and capabilities

The security of the console is enforced through the administrators and administrator groups registered in the BCM database . Each administrator and administrator group has a CCL (Capability Control List) which dictates what it can do. The administrators and administrator groups

nodes and their capability definitions specify the access to the console in general, that is, who can interrogate or manipulate the database and its contents. The access of administrators to objects is restricted by an ACL (Access Control List) that includes the following possibilities: READ/WRITE /ASSIGN. The **Security Profile** node or the **Security** tab define these access rights for specific objects. When you log on to the console for the first time and go to the **Administrators** node under the **Global Settings** node you can see two administrators already been created:

- **admin**
  The admin user is equipped with all permissions and capabilities, that is, it has full access rights on all objects in the database. It cannot be deleted but its password can be modified, however, neither its capabilities nor its static and dynamic objects. It can also be regarded as the superadministrator.
- **system**
  The system user is the login used by the master server itself for all database actions which it executes automatically, such as those of the data mover or autodiscovery module. None of its settings can be modified. The icon of this administrator is dimmed to indicate that the account is not activated.

Security considerations

Before you start to create administrators and groups you should sketch your system and the people administrating it as well as establish a list of all tasks to be executed and by whom to define which administrators and groups to create and which capabilities and access rights to assign to them.

Considerations to be taken into account when defining the access rights to the objects for each administrator are the following:

Capabilities

- Which object types is the administrator or group concerned with?
- Which other objects are implicated through the original object, such as when you create or modify queries, do you also need to be able to see the queries' object type?
- What operations is the administrator or group to execute on the object type: only see it or be able to do something with it, such as creating new objects of this type, modify existing ones or deleting them, being able to assign them to object of other types, etc.?

Access Rights

- Which top nodes does the administrator need access to, is it easier to provide access via a group and then populate it accordingly?
- For which objects types is it necessary to create queries to make sure any newly created objects of the type will be accessible by administrators through the dynamic objects?
- To which other object types do you need at least read access, for example, for reports you need at least read access to some queries, devices and device groups, for operational rules and packages you need read access to some device groups and devices.

- No general security is specified for the following main nodes: **Administrators** , **Administrator Groups** and **Directory Servers** , the security is specified via its members. All these nodes are located under the Global Settings.

Understanding security operations and principles

The following list shows which capability and access types are needed for which basic operation. The capabilities and access rights listed are the minimum requirements to execute these operations, but, of course the administrator can have more extensive permissions than those. For example, when specified *Write Access Deny* , this means that no write access is necessary to execute this operation, but of course the administrator can be assigned write access to these objects anyway.

Groups are divided in two different types: those with and those without the capability populate. User and device groups have the additional capability populate. The capabilities for administrator groups are the same as for administrators, thus they do not have the capability populate. Administrator groups are treated not as groups but as folders, to learn about their basic operating principles see the explanations concerning folders in the following paragraphs.

Also, be aware, that to be able to assign or modify access rights for other administrators you also must be assigned the capability **Manage Security**.

The following topics are provided:

Creating or delete an object in a folder

When you want to create an object within a folder or delete one from a folder you need the following capabilities and access rights:

- View and manage capabilities of the object type,
- Write access on the object under which the new one is created.
  By default the administrator creating the new object has read/write/assign access on this new object.

Example

To create a new operational rule under a folder called *Your Operational Rules* or to delete it you need:

Capabilities	Access Rights
View Operational Rules	**Read Allow, Write Deny** on the **Operational Rules** top node,
Manage Operational Rules	**Read Allow** and **Write Allow** on the folder *Your Operational Rules* .

Creating or deleting an object in/from a group

To create an object within a group or to delete it from there you need the following capabilities and access rights:

- View and populate capabilities on the group.
- Write access on the object itself and its parent.

Example

To delete a device called *Your Device* from the group called *AllYourDevices* you need:

Capabilities	Access Rights
View Devices and **Device Groups**	**Read Allow, Write Deny** on the **Device Groups** top node,
Manage Devices	**Read Allow** and **Write Allow** on the group *AllYourDevices* and the device called *Your Device* .
Populate Device Groups	

Modifying an object

To modify the attributes of an object you need the following capabilities and access rights:

- View and manage capabilities of the object type,
- Read and write access on the object.

Exporting an object

To export an object from the console you need the following capabilities and access rights:

- View capability of the object type,
- Read access on the object to be exported.

Importing an object

When you want to import an object you need the following capabilities and access rights:

- View and manage capabilities of the object type,

- Write access on the object under which the new one is imported (created).
  By default the administrator importing the object has read/write/assign access on this new object.

Managing access rights (security) of an object

To be able to modify the security profile of an object you need the following capabilities and access rights:

- View and manage Security Profile capabilities,
- View capability on administrators,
- View capability on the object type,
- Write access on the object for which the access rights are to be modified.

Example

To modify the access rights administrator *France* has on a specific device, the *Master Server* you need the following permissions:

Capabilities	Access Rights
View and **Mange Security Profile**	**Read Allow, Write Deny** on the **Device Groups** top node,
View Administrators	**Read Allow** and **Write Allow** on the group *AllYourDevices* and the device called *Master Server* .
View Devices	

Adding or removing an object to/from a folder

To add an object to or remove an object from a folder you need the following capabilities and access rights:

- View and manage capabilities on the object type,
- Read and write access on the parent object to/from which the child object is to be added /removed and Read access on the child

Example

To add a query *All Devices* to an existing folder, *General Queries* you need:

Capabilities	Access Rights
View Queries	**Read Allow, Write Deny** on the **Queries** top node,
Manage Queries	**Read Allow** and **Write Allow** on the folder *General Queries* and **Read Allow** on the query *All Devices* .

Adding or removing an object to/from a group

To add an object to or remove it from a group you need the following capabilities and access rights:

- View and populate capabilities on the group (parent object type), and view capability on the member (child object type),
- Read and write access on the group (parent object) to/from which the member (child object) is to be added, and read access on the child.

Example

To add a device *Your Device* to an existing device group, *Your Device Group* you need:

Capabilities	Access Rights
View Device Groups	**Read Allow, Write Deny** on the **Device Groups** top node,
Populate Device Groups	**Read Allow** and **Write Allow** on the device group *Your Device Group* and
View Devices	**Read Allow** on the device *Your Device* .

Moving (cutting and pasting) an object

The cut and paste operation on an object is divided into two different actions: the cut action and the paste action, as cut objects, depending on their type, can be pasted under more than one parent object.

- View and manage or populate (for device and user groups) capabilities on the object type
- Read and write access on the old and new parent object, read access on the object to be cut and pasted.

Example

In this example we will cut the *Your Operational Rule* object from its current parent, the *Your Operational Rules* folder and paste it under a new folder called *Test Rules* :

Capabilities	Access Rights
View Operational Rules	**Read Allow, Write Deny** on the **Operational Rules** top node,
Manage Operational Rules	**Read Allow** and **Write Allow** on the objects *Your Operational Rules* and *Test Rules*, as well as **Read Allow** on the object *Your Operational Rule*.

Duplicating (copying and pasting) an object

Similar to the cut and paste operation the copy and paste also is split in two operations. Only administrators, devices, users and device and user groups can be copied from one location to another (be duplicated), as they can be members of more than one group. You can also duplicate members of folders, but in this case the pasted member must be given a new name.

- View and manage or populate (for device and user groups) capabilities of the object type,
- Read and write access on both, the old and new, and read access on the object to be copied,

A duplicating operation on an object requires the exact same permissions regarding capabilities and access rights as the copy and paste operation.

Example

For the following example we want to copy a device, which belongs to a group called *HQ Devices* to another group called *Servers* :

Capabilities	Access Rights
View Device Groups	**Read Allow, Write Deny** on the **Device Groups** top node,
Populate Device Groups	**Read Allow** and **Write Allow** on the groups *HQ Devices* and *Servers* ,
View Devices	as well as **Read Allow** on the device.

Synchronize with a directory server

All groups, including the administrator groups can be synchronized with a directory server in Client Management . For this administrator needs the following capabilities and access rights:

- View, manage and populate capabilities on device/user groups (parent), or view and manage capabilities on administrators (parent),
- View capability on devices/users,
- View and manage capability on directory servers (child)
- Read and Write access on the device/user group (parent), or Read and Assign access on the administrator group (parent)
- Read access on the administrators/device/users and
- Read and Write access on the directory server (child), if it populates a device or user group or Read and Assign access, if it populates an administrator group.

Example 1

For the following example we synchronize our new device group called *MyNewGroup* with an existing directory server, for example called *AllLabClients* :

Capabilities	Access Rights
View Device Groups	**Read Allow, Write Deny** on the **Device Groups** top node,
Manage Device Groups	**Read Allow** and **Write Allow** on the group *MyNewGroup* ,
Populate Device Groups	**Read Allow** and **Write Allow** on the directory server *AllLabClients* ,
View Devices	**Read Allow** on (some) clients of the directory server.
View Directory Servers	
Manage Directory Servers	

The **Manage** capability and **Write** access to the group are necessary, because the group name changes to the name of the directory server group as soon as it is synchronized with the server. The **Manage** capability for the devices is not required, because it is the system which will create the new objects that are added to the group. Therefore you will also not be able to see these new group members, if you do not have at least **Read** access to the children of the synchronized group.

Example 2

For the following example we synchronize an administrator group called *MyNewAdmins* with an existing directory server, for example called *AllLabAdmins* :

Capabilities	Access Rights
View Administrators	**Read Allow** and **Write Allow** on the administrator group *MyNewAdmins* ,
Manage Administrators	**Read Allow** and **Write Allow** on the directory server *AllLabAdmins* ,
View Directory Servers	**Read Allow** on (some) administrators of the directory server.
Manage Directory Servers	

The **Manage** capability and **Write** access to the group are necessary, because the group name changes to the name of the directory server group as soon as it is synchronized with the server.

Related topics

- Assigning or unassigning objects
- Capabilities and access rights reference

Assigning or unassigning objects

When assigning/unassigning an object to/from an object of another type, two basic concepts must be distinguished:

- Assigning or unassigning an object to/from a group
- Assigning or unassigning an object to/from another object

Assigning or unassigning an object to/from a group

To assign/unassign an object to a group that modifies its content (queries, directory servers and compliance rules) you need the following capabilities and access rights. Be aware that administrator groups are handled as usual like folders (see below), not like groups. It causes the contents of the group to change.

- View and populate capabilities for group (parent)
  - if the directory server is to be synchronized as well, not only to be assigned you also need the manage capability
- View capability on the object to be assigned (child),
- Read and write access on the parent and read access on the child.

Example 2

To assign a query *All Servers* to device group *All Servers France* you need the following permissions:

Capabilities	Access Rights
View Device Groups	**Read Allow, Write Deny** on the **Device Groups** top node,
Populate Device Groups	**Read Allow** and **Write Allow** on the group *All Servers France* ,
View Queries	and **Read Allow** on query *All Servers* .

Assigning or unassigning an object to/from another object

To assign/unassign an object to/from another object, such as operational rules, packages, transfer windows, and so on, you need the following capabilities and access rights:

- View and assign capabilities on the target object (parent),
- View and assign capabilities on the object to be assigned (child),
- Read access on the parent and read and assign access on the child.

Example 2

To assign a transfer window *High Speed Downstream* to device *Server France* you need the following permissions:

Capabilities	Access Rights
View Devices	**Read Allow, Write Deny** on the **Transfer Windows** top node,
Assign Devices	**Read Allow** and **Assign Allow** on the device *Server France*
View Transfer Windows	and **Read Allow** on transfer window *High Speed Downstream* .
Assign Transfer Windows	

Capabilities and access rights reference

The following table recapitulates the required capabilities and access rights to manage assignments between the different non-modifying database objects with the understanding that the view capability as well as read access is always required on both the parent and child object:

Parent	Child	Child Capabilities	Parent Access	Child Access
Custom Compliance Rule	Report	Assign Report	Assign	Read
Device	Custom Compliance Rule	Assign Compliance Rule	Assign	Read
Device	Inventory Filter	Assign Filters	Assign	Read
Device	Managed Application	Manage Managed Applications	Assign	Read
Device	Application List	Assign Application Lists	Assign	Read
Device	Licensed Software	Assign Licensed Software	Assign	Read

Parent	Child	Child Capabilities	Parent Access	Child Access
Device	Operational Rule	Assign Operational Rules	Assign	Read
Device	Package	Assign Packages	Assign	Read
Device	Patch Group	Assign Patch Groups	Assign	Read
Device	Patch Job	Assign Patch Jobs	Assign	Read
Device	Rollout	Assign Rollout	Assign	Read
Device	SCAP Job	Assign Compliance Rule	Assign	Read
Device	Task	Assign Task	Assign	Read
Device	Transfer Window	Assign Transfer Windows	Assign	Read
Device Group *	Custom Compliance Rule *	Assign Compliance Rule	Assign	Read
Device Group	Inventory Filter	Assign Filters	Assign	Read
Device Group	Managed Application	Manage Managed Applications	Assign	Read
Device Group	Licensed Software	Assign Licensed Software	Assign	Read
Device Group	Application List	Assign Application Lists	Assign	Read
Device Group	Operational Rule	Assign Operational Rules	Assign	Read
Device Group	Package	Assign Packages	Assign	Read
Device Group	Patch Group	Assign Patch Groups	Assign	Read
Device Group	Patch Job	Assign Patch Jobs	Assign	Read
Device Group	Report	Assign Reports	Assign	Read
Device Group	Rollout	Assign Rollout	Assign	Read
Device Group	SCAP Job	Assign Compliance Rule	Assign	Read
Device Group	Task	Assign Task	Assign	Read
Device Group	Transfer Window	Assign Transfer Windows	Assign	Read
Monitored Applications	Schedule Template	Manage Schedule Templates	Assign	Read
Operational Rule	Task	Assign Task	Assign	Read
Package	Operational Rule	Manage Operational Rules	Write	Write
Patch Group	Package	Manage Patch Groups	Write	Write
Patch Group	Task	Assign Task	Assign	Read
Prohibited Applications	Schedule Template	Manage Schedule Templates	Assign	Read
Query	Sub-Report	Manage Reports	Write	Write
Rollout	Task	Assign Task	Assign	Read
Rollout	User Account	Populate Rollout	Assign	Read
Scan Configuration	Scan	Assign Scan	Assign	Read
Scanner	Scan	Assign Scan	Assign	Read

Parent	Child	Child Capabilities	Parent Access	Child Access
SCAP Job	SCAP Package	Manage Compliance Rules	Write	Read
Target List	Scan	Assign Scan	Assign	Read
User	Operational Rule	Manage Operational Rules	Assign	Read
User Group	Operational Rule	Manage Operational Rules	Assign	Read

- The assignment of a compliance rule to a device group in this case is used by the compliance rule to check the group members for their compliance.

Populating

The following table recapitulates the required capabilities and access rights to manage assignments between the different database objects concerning their population. Same as with the preceding table, the view capability as well as read access is always required on both the parent and child object:

Parent	Child	Parent Capabilities	Parent Access	Child Access
Administrator Group	Directory Server	Manage Administrators	Write	Read
Device Group *	Custom Compliance Rule *	Populate Device Groups	Write	Read
Device Group	Directory Server	Populate Device Groups	Write	Read
Device Group	Query	Populate Device Groups	Write	Read
Rollout	Device Group	Populate Rollouts	Write	Read
Rollout	Target	Populate Rollouts	Write	Read
User Group	Directory Server	Populate User Groups	Write	Read
User Group	Query	Populate User Groups	Write	Read

- The assignment of a compliance rule to a device group here actually populates the device group with the result of its compliance check, that is, the group will contain all compliant devices, all non-compliant devices or those which could not be evaluated.

Scheduling

The following table recapitulates the required capabilities and access rights to schedule the execution of the different database objects. Same as with the preceding table, the view capability as well as read access is always required on the object:

Object	Capabilities	Access
Asset Discovery Scan	Schedule Scans	Write
SCAP Compliance Scan	Schedule Compliance Rules	Write
Operational Rule	Schedule Operational Rules	Write
Rollout	Schedule Rollout	Write

Configuring

The following table recapitulates the required capabilities and access rights to define the basic configuration of CM functionalities:

Functionality	Capabilities	Access
Compliance Management	Configure Compliance Management	Write
Operating System Deployment	Configure Operating System Deployment	Write
Patch Group	Configure Patch Groups	Write
Patch Job	Configure Patch Jobs	Write
Task Management	Configure Task Management	Write

Managing security profiles

The **Security Profile** node provides the possibility to define a specific security profile for each administrator and administrator group in the database. This profile specifies the capabilities of the administrator/administrator group with regards to the different CM objects and to which of the individual objects the administrator/administrator group has access and which type of access.

Parameter	Description
Read Access	Read access provides an administrator/administrator group with the respective rights to display the object in the console. Without read access assigned, write or assign access cannot be granted.
Write Access	This access type allows the administrator/administrator group to manipulate the respective object, such as create children, modify or delete it.
Assign Access	The access type assign provides the possibility to assign the respective object to another object, such as a transfer window to a device. Only those database objects that contain the assign capability are concerned by this right, such as operational rules, packages and transfer windows. It is obsolete for all other database objects.
Direct Access Acknowledgement	This access type provides the possibility to request system credentials when trying to access a device remotely via the **Direct Access** functionality. The default access is **Required** . This type of access is only applicable to devices.
Remote Control Acknowledgement	This access type provides the possibility to request system credentials when trying to access a device remotely via the **Remote Control** functionality. The default access is **Required** . This type of access is only applicable to devices.

These types of access can either be **Allow** , **Deny** or **Inherit** for the base access types or **Required** , **Not Required** , **Inherit** or **Deny** for access requiring system credentials:

Parameter	Description
Allow	This value allows the specified access type. Be aware however, that if access to an object is allowed for an object for one group and denied for another the administrator is a member of the access will be denied, because this value is stronger than allowed.
Deny	This value denies the type of access, it is the strongest value and will prevail in cases of conflict.
Required	This value defines that any user trying to access the device remotely must provide system credentials.

Parameter	Description
Not Required	This value defines that the device can be remotely accessed without credentials. In this case the following two specific situations must be defined additionally. If both options are activated no system credentials are ever required. • **If User Absent**: If this check box is not selected credentials must be provided if the user is absent. • **If Session is Closed**: If this check box is not selected credentials must be provided if the session is closed.
Inherit	This value is neutral, and can be overridden by any other definition. If this setting is specified for an administrator for a specific object access, and the same access is allowed for the group the administrator is a member of, he will inherit the permission to access. The same is valid for denying access.
Respect Windows permissions when accessing files and the Registry	This check box only applies to **Direct Access Acknowledgement** of devices. It defines if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account.

When assigning access rights to the database objects you must differentiate between static and dynamic objects:

Parameter	Description
Static Objects	All objects in the database are static objects. Static in this case means that the access is assigned to the object itself, for reasons of viewing, modification or assignment, and this access will always remain as defined until it is modified manually.
Dynamic Objects	Access to a dynamic object means access not to the object itself, but to its "result", whereby the result might change, either when modifications made to the object as a static object or through changes in the environment the object applies to. All dynamic objects are at the same time static and dynamic, because they must be accessible "directly" to be editable themselves as well.

Be aware that to be able to apply any of these access rights, an administrator/administrator group must also have the respective capabilities assigned, otherwise they will still not be able to view or manipulate the object in any way.

Related topics

- Types of security profiles
- Managing capabilities of a security profiles
- Managing static objects of a security profiles
- Managing dynamic objects of a security profile
- Security Profile Wizard

Types of security profiles

This paragraph will provide you with a number of examples for security scenarios describing the environment in which it is setup, what exactly happens when trying to access and what needs to be defined to ensure the respective scenario works according to definition.

We propose, that you create these profiles not for individual administrators but for administrator groups, thus it is easier to add new admins with the same profile and to make sure there always is at least one administrator of the specific profile. The administrator in these cases will be created with no capabilities and no access rights, all these will be given to him via the groups he is a member of.

Also we assume that the predefined objects were imported, because they contain a number of very useful settings which we refer to in the following scenarios:

- Administrator with system login
- User administrator
- Read-only administrator
- Installer administrator
- Reports administrator
- Compliance management administrator

Administrator with system login

The following scenario describes what happens when an administrator tries to log on to the console:

- that has never before tried to log on, that is not yet created in the BCM database as an administrator but who has a valid local system login.

For this scenario to work, you must however have activated the option to create new administrators via their system login. To make sure this option is activated proceed as follows, as by default it is deactivated:

1. Log on to the console with the predefined admin login.
2. Then go to the **Global Settings** and the **System Variables** node.
3. Select the **Security** tab.
4. Mark the value in the right window pane.
5. Click the **Edit > Properties** menu item.
   The **Properties** pop-up window appears.
6. Check the **Create Default System Administrator** box.
7. Click **OK** to confirm and close the window.
   The required option is now activated.

As the user is not registered in the database, he can only use his local system login to log on to the BMC Client Management console. The following happens:

1. The user logs on with his system login and password.
2. Basic authentication is executed via the HttpProtocolHandler:
   - The HTTP protocol handler verifies with the Host Access module if the requesting client is authorized to connect to the master server. If no modifications were made in the Host Access module since startup the requesting client is authorized.

- Then the HTTP protocol handler verifies with the User Access module if the supplied login and password are authorized. When checking the table of configured users the handler will find an equivalent as system and authorize the login.
- Then the vision64database module will verify with the database if an administrator user exists for this login/password pair, which is not the case. As the login was authorized beforehand, the database module will create a new user with the provided login and password in the access list. However, no capabilities and access rights are assigned at creation time.
- Now the console window appears with a connection to the requested master server, but the displayed contents are very limited:
  - He will only be able to see the following top nodes: **Search** , **Global Settings** , **Device Topology** and **Alerts and Events** . However, he will not be able to view any devices in the **Device Topology** nor will he be able to execute operations on **Global Settings** subnodes.
  - As he has no capabilities assigned either, he will not be able to execute any operations on the visible nodes and objects in the console.

User administrator

The user administrator scenario describes the security settings to be defined for administrators who have quite far reaching rights, similar to the system administrator, that is, they can access all objects and types apart from the actual system settings.

1. Log on to the console with a superadministrator or the admin login.
2. Go to the **Global Settings** > **Administrator Groups** node.
3. Create a new group called *UserAdmins* .
4. Select the following **Security Profile** node and its **Capabilities** tab.
5. Click the **Edit** > **Properties** menu item.
   The **Properties** pop-up window appears.
6. In the **Modify Capabilities** tab select *ALL* capabilities and then clear the following:
   - Both **Administrator** capabilities
   - Both **System Variables** capabilities
   - Both **Security Profile** capabilities
   - Both **License** capabilities
7. Click **OK** to confirm and close the window.
8. Then go to the **Static Objects** tab and via the **Properties** pop-up window select all **Top Nodes** to be added to the static objects with **Read, Write and Assign: Allowed** .
9. In the **Dynamic Objects** tab add all queries which can be found under the folder *BMC Client Management database* apart from the *All Administrators* and *All Administrator Groups* queries with **Read, Write and Assign: Allowed** via the **Properties** pop-up window. These queries ensure, that the administrator has access to all objects of any type that will be created in the future by any other administrator.

Note

We consider administrators and administrator groups part of the system management and therefore have excluded them from the field of activity of the user administrator.

Remarks regarding this configuration:

Read-only administrator

The read-only administrator is somewhat an equivalent of the user administrator without the permission for modification. This type of administrator might be interesting for the head of the IT department to have an overview of the whole system and what goes on in it without active intervention.

1. Log on to the console with a superadministrator or the admin login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Create a new group called *ReadOnly* .
4. Select the following **Security Profile** node and in the **Capabilities** tab.
5. Click the **Edit > Properties** menu item.
   The **Properties** pop-up window appears.
6. In the **Modify Capabilities** tab select *ALL View* capabilities apart from the following:
   - **View Administrators**
   - **View System Variables**
   - **View Security Profile**
   - **View Licenses**
7. Click **OK** to confirm and close the window.
8. Then go to the **Static Objects** tab and via the **Properties** pop-up window select all **Top Nodes** to be added to the static objects with **Read** access **Allowed** , and **Write and Assign** access **Denied** .
9. In the **Dynamic Objects** tab add all queries which can be found under the folder *BMC Client Management database* apart from the *All Administrators* and *All Administrator Groups* queries with **Read** access **Allowed** , and **Write and Assign** access **Denied** via the **Properties** pop-up window. These queries ensure, that the administrator will be able to see all objects of any type that will be created in the future by any other administrator.

Note

We consider administrators and administrator groups part of the system management and therefore have excluded them from the field of activity of the read-only administrator.

Installer administrator

This scenario describes the security settings to be defined for an administrator who only executes agent rollouts across the network.

1. Log on to the console with a superadministrator login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Create a new group called *Installer* .
4. Select the following **Security Profile** node and in the **Capabilities** tab.
5. Click the **Edit > Properties** menu item.

1. In the **Modify Capabilities** tab select the following capabilities:
   - All **Modify Capabilities** capabilities
   - All **Device** capabilities
   - **View** and **Manage Device Groups** capabilities - no **Populate** capability
2. Click **OK** to confirm and close the window.
3. Then go to the **Static Objects** tab and via the **Properties** pop-up window add the following static objects:
   - **Device Groups** top node with **Read and Assign Access: Allow** and **Write Access: Deny**
   - **Rollouts** top node with **Read, Write and Assign Access: Allow**
4. In the **Dynamic Objects** tab add the following dynamic objects via the **Properties** pop-up window:
   - *All Devices* and *All Device Groups* queries with **Read Access: Allow** and **Write and Assign Access: Deny**
   - *All Rollout Folders* and *All Rollouts* queries with **Read, Write and Assign Access: Allow**.

   These queries can be found in the *BMC Client Management database* folder.

Reports administrator

This type of administrator profile is created for users who only create reports, but reports regarding any object in the database.

1. Log on to the console with a superadministrator login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Create a new group called *Reporting* .
4. Select the following **Security Profile** node and in the **Capabilities** tab.
5. Click the **Edit > Properties** menu item.
   The **Properties** pop-up window appears.
6. In the **Modify Capabilities** tab select *ALL View* capabilities apart from the following:
   - **View System Variables**
   - **View Security Profile**
   - **View Agent Configuration**
   - **View Direct Access**
   - **View Remote Control**
7. Then in addition check the following capabilities:
   - **Manage Queries**
   - **Manage** and **Assign Reports**
8. Click **OK** to confirm and close the window.

9. Then go to the **Static Objects** tab and add the following top nodes with the following access rights via the **Properties** pop-up window:
    - **Device Groups** top node with **Read and Assign Access: Allow** and **Write Access: Deny**
    - **Queries** and **Reports** top nodes with **Read, Write and Assign Access: Allow**
10. In the **Dynamic Objects** tab add via the **Properties** pop-up window all queries of the *BMC Client Management database* folder with access rights **Read Access: Allow** and **Write and Assign Access: Deny** apart from the following which will also be added but with different access types:
    - *All Devices* and *All Device Groups* queries with **Read and Assign Access: Allow** and **Write Access: Deny**
    - *All Query Folders* and *All Queries* , as well as *All Report Folders* and *All Reports* queries with **Read, Write and Assign Access: Allow** .

> **Note**
>
> If you have different report creation profiles you can restrict the view to the necessary objects the profiles create reports for. However, ensure that you provide them with the same access as previously to queries and device groups, because reports are based on either one of these object types. If you do not provide access to the device groups, no reports can be generated being assigned to a device group instead of being based on a query.

Compliance management administrator

This type of administrator profile is created for administrators who ensure the compliance of the complete infrastructure, that is, they do not only analyse the current situation of the IT park concerning its compliance but take action to keep it compliant. It can be created in addition to the *Compliance Administrator* that comes with the predefined objects as this profile only allows for the analysis of device compliance.

1. Log on to the console with a superadministrator login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Create a new group called *Compliance Manager* .
4. Select the following **Security Profile** node
5. In the **Capabilities** tab click the **Edit > Properties** menu item.
   The **Properties** pop-up window appears.
6. In the **Modify Capabilities** tab select the following minimum capabilities:
    - **View** and **Manage Devices**
    - **View** and **Manage Device Groups**
    - **View** , **Manage** , **Assign** and **Configure Compliance**
7. Following you can see a list of possible capabilities that can be assigned to the administrator, depending on the compliance targets:

- **View** and **Manage Inventory** - to provide access to all inventory criteria
- **View** and **Assign Packages** - if compliance includes specific installed packages as criteria
- **View** and **Schedule Operational Rules** - if compliance includes specific assigned operational rules as criteria
- **View** , **Manage** , **Assign** and **Configure Patch Groups** - if compliance includes specific installed patches as criteria

8. Click **OK** to confirm and close the window.
9. Go to the **Static Objects** tab and add the following top nodes with the following access rights depending on the capabilities you added in the previous tab via the **Properties** pop-up window:
   - **Custom Compliance** , **Operational Rules** , **Packages** and **Patch Management** top node with **Read, Write and Assign Access: Allow**
   - **Device Groups** top node with **Read and Assign Access: Allow** and **Write Access: Deny**
10. The definitions in the **Dynamic Objects** tab of the **Security Profile** node also depends on the selections made in the **Capabilities** tab:
    - *All Patch Groups* , *All Packages* and *All Operational Rules* queries with **Read, Write and Assign Access: Allow** .

Managing capabilities of a security profiles

The **Capabilities** tab provides the list of available capabilities in the right window pane, which are grouped by their functionality type. These capabilities define which of the the CM functionalities administrators and administrator groups can access in the console. A granted access is indicated by symbol, denied access by symbol, and a granted access that is inherited by an administrator from the administrator group by symbol. Be aware, that when an administrator is assigned a capability twice, once directly and once via a group, the group capability "overwrites" the individual one and will also be displayed as such.

Parameter	Description
Object Type	The fields in this column display all BMC Client Management parts and object types with their symbol and their name for which capabilities can be assigned.
View	This access type is the most restrictive of all and provides administrators with the general access to a specific object type, such as reports or devices. If the **View** capability is not assigned, the main node of the object type will not appear among the nodes in the left console window and no operations of any type can be executed on it. For example, if you do not provide an administrator with the capability to **View Device Groups** , the **Device Groups** node will not be displayed and thus the administrator cannot manage or populate any device groups, because he cannot see them.
Manage	This capability allows administrators to create new objects of the specified type or modify and delete existing ones. For example, the capability **Manage Operational Rules** allows you to create any number of operational rules under the main **Operational Rules** node. You can also delete any existing operational rules or modify them. It also allows for the creation of links between objects (which are not a device or a device group) such as adding and defining the query for a report. However, this capability does not allow you to assign the operational rule to a software distribution for a client device or a user or a group.
Assign	

Parameter	Description
	This capability permits administrators to create the relations between database objects of the specified type and devices/users or device groups/user groups. You only need to have the assign capability for the object being assigned, for example, when assigning an operational rule to a device group you only need the **Assign Operational Rules** capability. Creating links between any type of objects which are not a device or device group, such as adding a package to an operational rule falls under the manage capability.
Populate	This capability is necessary for all operations which might influence the content of the object type, such as assigning a directory server or a query to manage the contents as a dynamic group or finding the targets of a rollout.
Schedule	If an administrator is to be able to actually schedule objects of the respective type, that is, operational rules, rollouts and asset discover scans, this capability must be assigned. If the administrator is to schedule packages and patch packages, this operational rule capability also must be assigned, because the execution/installation of packages and patch packages is based on the execution of operational rules.
Configure	If an administrator is to be able to configure a functionality such as **Patch Management** or **Operating System Deployment** , this capability must be assigned. If an administrator does not have this capability for these functionalities the respective **Configuration** node will not be accessible for these features.

Assigning capabilities to a security profile

To assign a capability to an administrator or administrator group, proceed as follows:

1. Select the administrator or administrator group for whom one or more capabilities are to be assigned either as the node in the left window pane or as the entry in the table in the right window pane and then select the **Capabilities** tab of the **Security Profile** node.
2. Click **Edit > Properties** .
   The **Properties** dialog box appears. It has the following tabs about the capabilities which are grouped by their functionality type:

Modify Capabilities	In this tab you can add or remove capabilities to/from the selected administrator or administrator group. You will see, that capabilities which are inherited via an admin's group are dimmed. To do so check or clear the boxes next to the respective capability. A capability that was already assigned via group does not need to be added again. If you want to assign all capabilities to this administrator you can click the **Select All Capabilities** button at the bottom of the list.
Inherited Capabilities	This tab is only available for administrators and displays the list of all capabilities the administrators inherited through their group membership. This tab is only for information, you cannot make any modifications in it.

3. Click **OK** to assign the selected capabilities to the administrators and to close the window.

Managing static objects of a security profiles

The following topics are provided:

- Adding a static object
- Modifying access rights of a static object
- Removing an object

The **Static Objects** tab enables defining which of all existing database object types and objects an administrator is to be able to access and in which way. Be aware, that to access an individual object the administrator must be assigned at least read access to the respective top node. For example, the administrator must have at least view access to the **Reports** top node, to access a specific report.

By default this tab will always contain one entry, the respective administrator himself. When an administrator is created he will automatically be added here to provide him with the possibility to check his access rights. The default access defined at creation time is **Read Access** access allowed, any other access denied.

Parameter	Description
Name	Displays the name of the object for which the right is assigned, for example, Hardware Inventory Report or All Devices for a query.
Object Type	This column displays the object type of the selected object, such as **Query** or **Report** .
Via Administrator Group	This field shows if the access right to the object is directly assigned to the administrator or if it is inherited through a group membership. The field is empty if it is directly assigned or it will contain the name of the group or groups from which the administrator inherits.
Read Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. In this case the administrator will not be able to see this object in his console nor any of its children.
Write Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. The administrator must have read access granted on the respective object to be able to be assigned write access.
Assign Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. This type of access is only of importance for objects that also have an **Assign Access** capability. In these cases the **Assign Access** capability for this object type is a prerequisite. If it is not assigned this access right is ignored. The database objects concerned by this are operational rules, packages and transfer windows.
Direct Access Acknowledgement	This access type defines if system credentials are required when trying to access a device remotely via the **Direct Access** functionality. Possible values are: • **Required** , for *yes* , system credentials must be provided to access, • **Not Required** , for *no* , no credentials are required with the specification on when they are not required, for an absent user or a closed session or both, • **Inherit** , if the access definition is defined through the group membership, or • **Deny** , if the access to a specific device of a group, such as for example the master is to be refused, even though the administrator is able to access all other group members. The default access is **Required** . This type of access is only applicable to devices.
Remote Control Acknowledgement	This access type defines if system credentials are required when trying to access a device remotely via the **Remote Control** functionality. Possible values are: • **Required** , for *yes* , system credentials must be provided to access, • **Not Required** , for *no* , no credentials are required with the specification on when they are not required, for an absent user or a closed session or both, • **Inherit** , if the access definition is defined through the group membership, or • **Deny** , if the access to a specific device of a group, such as for example the master is to be refused, even though the administrator is able to access all other group members. The default access is **Required** . This type of access is only applicable to devices.
Real User Rights	

Parameter	Description
	This field shows if the administrator is accessing the local files and Windows Registry of a device with the access rights a system account or only those of the local account. It displays **Yes** , to limit to local account access, for complete system access this field remains empty. This parameter is only applicable to devices.

Adding a static object

When adding objects to the security profile, be careful to always include the complete hierarchy to the target object including the object's top node, otherwise the administrators might still not be able to access the object. To add a database object, proceed as follows:

1. Click **Edit> Add Object** .
   The **Select Static Objects** dialog box appears on the screen.
2. In the drop-down box **Object Type** select the type of the database object to add.
   This list is pre-filtered according to your licenses.
3. The box to the left will now display the options in the form of icons, according to which you can select static objects, that is, you can chose between the **Hierarchy** , **All** and **Search** , for devices and groups you also have the option **Topology** . If you selected the option **Top Nodes** the field displays the complete list of all top nodes available in the console, so they can be added directly.
   The contents of the following **Available Objects** list box will change to display the list of all objects of this type.
4. Select one or more objects from this window, or search for specific objects through the **Search** tab.
5. Click **Add** to move the selected objects to the **Selected Objects** box.
   The **Properties** dialog box appears to define the type of access for the selected objects.
6. Select the respective radio buttons and then click **OK**.

> **Note**
>
> Check the option **Respect Windows permissions when accessing files and the Registry** in the **Direct Access Acknowledgement** panel if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account. This option is only applicable to devices.

   The objects will be added to the **Selected Objects** box in which they will be listed with their name and their type.
7. If you would like to add objects of another type as well, repeat the preceding steps.
8. Click **OK** to add all selected objects to the list of security objects of the security profile.

Modifying access rights of a static object

Objects to which access is assigned via a group cannot be modified. To restrict the access further than that assigned thought the group, the object must be assigned individually a second time with new settings. To modify existing access rights for objects, proceed as follows:

1. Select the object for which the access is to be modified in the table in the right window pane.
2. Click the **Edit> Properties** icon.
   The **Properties** dialog box appears.
3. Select the radio buttons for the desired type of access.
4. Click **OK** to confirm the modifications and to close the window.

Removing an object

If the object you are about to remove is a group or a folder make sure it is not a parent to any of the objects still in the list. In this case the administrators cannot be able to access the children anymore. To remove an object from the security profile, proceed as follows:

1. Select the object to be removed from the list of security objects in the right window pane.
2. Click **Edit > Remove Object** .
   A confirmation window appears.
3. Click **OK** to confirm the removal.

Managing dynamic objects of a security profile

The access to the dynamic objects is assigned indirectly though other objects, a query, a device group or a folder. This means, that when dynamic access is assigned, the objects to which the administrator has access might not always be the same.

Query:

A query defines via its target type and its criteria to which objects the administrator has access. These can change either

- when modifications are made to the query itself, such as adding new criteria or modifying one, or
- when changes happen to the environment of the query, which in this case means the target type of the query. For example, a new device that is added to the network complies with the criteria of the query.

For example, administrator *admin1* is given access to query *French* . This query finds all administrators that are located in France, for example, *AdminParis, AdminLyon* and *AdminNantes* . A new administrator, *AdminNice* joins the company at a new location and is added to the database. Because his location is also in *France* , he will be automatically added to the list of administrators *admin1* has access to.

Device Group or **Folder:**

When providing access via a device group or a folder the administrator has access to all direct and indirect members of this group or folder. For example: the administrator *admin* is assigned the device group *Group 1* as a dynamic object. This group has the members *PC1, Group 2* and *Group 3* . *admin* now has access to *PC1* (direct member) as well as all members of *Groups 2* and *3* , that is *PC2* and *PC3* (indirect members). *admin* will also automatically have access to all PCs that are added to either of these groups. If members are removed from one of these groups he will automatically lose access to the removed members.

The **Dynamic Objects** tab displays the following information about the dynamic objects the administrator is given access to:

Parameter	Description
Members of	Displays the name of the object for which the right is assigned, for example, *All Devices* , *All French Clients* or *Patch Job Reports* .
Object Type	This field displays the target type of the object. The possible values for this type are the main objects available in the BCM database , such as **Administrators** or **Devices** .
Via Administrator Group	This field shows if the access right to the object is directly assigned to the administrator or if it is inherited through a group membership. The field is empty if it is directly assigned or it will contain the name of the group or groups from which the administrator inherits.
Read Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. In this case the administrator will not be able to see the objects, which are the result nor any of their children in his console.
Write Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. For this access to be granted, the administrator must also have the read access granted.
Assign Access	Contains **Allow** , for *yes* , grant write access or **Deny** , for *no* , do not grant it. For this access to be granted, the administrator must also have the read access granted.
Direct Access Acknowledgement	This access type defines if system credentials are required when trying to access a device remotely via the **Direct Access** functionality. Possible values are: • **Required** , for *yes* , system credentials must be provided to access, • **Not Required** , for *no* , no credentials are required with the specification on when they are not required, for an absent user or a closed session or both, • **Inherit** , if the access definition is defined through the group membership, or • **Deny** , if the access to a specific device of a group, such as for example the master is to be refused, even though the administrator is able to access all other group members. The default access is **Required** . This type of access is only applicable to devices.
Remote Control Acknowledgement	This access type defines if system credentials are required when trying to access a device remotely via the **Remote Control** functionality. Possible values are: • **Required** , for *yes* , system credentials must be provided to access, • **Not Required** , for *no* , no credentials are required with the specification on when they are not required, for an absent user or a closed session or both, • **Inherit** , if the access definition is defined through the group membership, or • **Deny** , if the access to a specific device of a group, such as for example the master is to be refused, even though the administrator is able to access all other group members. The default access is **Required** . This type of access is only applicable to devices.

Parameter	Description
Real User Rights	This field shows if the administrator is accessing the local files and Windows Registry of a device with the access rights a system account or only those of the local account. It displays **Yes** , to limit to local account access, for complete system access this field remains empty.

Related topics

- Adding the results of a query to the security profile
- Adding the members of a device group to the security profile
- Adding the members of a folder to the security profile
- Modifying the access rights of a dynamic object
- Removing a dynamic object

Adding the results of a query to the security profile

Any query can be added to the security profile of an administrator. In this case it is not the query in itself but the result of the query that defines to which objects the administrator has access.

> **Note**
>
> It is not necessary for the administrator to have read or write access assigned to the query through the query's **Security** tab.

1. Click **Edit > Add Results of Query** .
   The **Select Dynamic Objects** dialog box appears on the screen. The contents of the list box displays the dynamic objects either in the hierarchy of all queries or a list of all existing queries, depending on the icon you click in the left box.
2. In the drop-down box **Object Type** select the type of the database object to add.
   This list is pre-filtered according to your licenses.
3. You can also search for a specific query via the **Search** tab.
4. Click **OK** to confirm the selections.
   The **Properties** dialog box appears to define the type of access for the queries.
5. Select the respective radio buttons.
   The option **Inherited** is only of interest if you are defining this profile for an individual administrator instead of a group. In this case you can select this radio button if the access rights are to be inherited from the administrator group(s) the administrator belongs to. Check the option **Respect Windows permissions when accessing files and the Registry** in the **Direct Access Acknowledgement** panel if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account.
6. Click **OK** to add the queries to the security profile.

Adding the members of a device group to the security profile

Any device group can be added to the dynamic objects of an administrator's security profile. In this case it is, however, not the group in itself that is added but all its direct and indirect members on which the access rights are defined.

> **Note**
>
> It is not necessary for the administrator to have read or write access assigned to the device group through the groups's **Security** tab.

1. Click **Edit > Add Members of Device Group** .
   The **Select Dynamic Objects** dialog box appears on the screen. The contents of the list box displays the available groups either in the hierarchy of all groups or a list of all existing groups, depending on the icon you click in the left box.
2. Select the desired device group.
   You can also search for a specific group via the **Search** tab.
3. Repeat this step until all device groups of which the members are to be assigned to the administrator/administrator group are selected.
   Only select those groups for which the same type of access is to be defined.
4. Click **OK** to confirm the selections.
   The **Properties** dialog box appears to define the type of access for the groups.
5. Select the respective radio buttons and options.
   The option **Inherited** is only of interest if you are defining this profile for an individual administrator instead of a group. In this case you can select this radio button if the access rights are to be inherited from the administrator group(s) the administrator belongs to. As long as the administrator is not a member of a group this option is interpreted as **Deny**.
   Check the option **Respect Windows permissions when accessing files and the Registry** in the **Direct Access Acknowledgement** panel if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account.
6. Click **OK** to add the device groups to the security profile.
7. Repeat the preceding steps to add more groups with different access rights until the access is defined for all required group members.

Adding the members of a folder to the security profile

Any folder can be added to the dynamic objects of an administrator's security profile. In this case it is, however, not the folder in itself that is added but all its direct and indirect members on which the access rights are defined.

> **Notes**

- It is not necessary for the administrator to have read or write access assigned to the folder through the folder's **Security** tab.
- The term *folder* that is used in this context does refer to all BMC Client Management database objects with the exception of *device groups* for which specific access types must be defined.

1. Click **Edit > Add Members of Folder** .
   The **Select Dynamic Objects** dialog box appears on the screen. The contents of the list box displays the dynamic objects either in the hierarchy of all folders or a list of all existing folders, depending on the icon you click in the left box.
2. In the drop-down box **Object Type** select the type of the database object to add.
   This list is pre-filtered according to your licenses.
3. You can also search for a specific folder via the **Search** tab.
4. Click **OK** to confirm the selections.
   The **Properties** dialog box appears to define the type of access for the folders.
5. Select the respective radio buttons.
6. Click **OK** to add the folders to the security profile.

Modifying the access rights of a dynamic object

1. Select the dynamic object for which the access is to be modified in the table in the right window pane.
2. Click **Edit > Properties** .
   The **Properties** dialog box appears.
3. Select the radio buttons for the desired type of access.
4. Click **OK** to confirm the modifications and to close the window.

Removing a dynamic object

When you remove a dynamic object from this list, the administrator will no longer be able to access any of the database objects to which this object gave him access, nor any of their children. To remove a dynamic object from the security profile, proceed as follows:

1. Select the dynamic object to be removed from the list of security objects in the right window pane.
2. Select **Edit > Remove Query** .
   A confirmation window appears.
3. Click **OK** to confirm the removal.

Security Profile Wizard

The Security Profile Wizard wizard guides you thought the creation and definition and scheduling of new administrators or administrator groups.

The wizard is available directly on the main **Wizards** menu from anywhere in the console, and in the specific functionalities of the **Administrators** and **Administrator Groups.**

> **Note**
>
> To create administrators or groups with the maximum possible access rights and capabilities you must preferably be logged on as an administrator with superadmin rights yourself.

At the bottom of the last page of the wizard you will always find an option that moves the focus of the console to the newly created object. Check this box if you want to do so. This option is not explained in the individual windows.

Related topics

- Defining the security profile to create
- Defining the new administrator properties
- Defining the new administrator group properties
- Defining the capabilities of a new administrator or administrator group
- Defining the access via static objects
- Defining the access via dynamic access
- Defining the new administrator group synchronization schedule

Defining the security profile to create

In this first wizard window, **Security Group Type**, you must define which type of profile you want to create. You can either let the system automatically create and synchronize a new group that has all the necessary capabilities and access rights to execute most of the daily tasks, as shown in the wizard window. Or you can create an administrator with the same type of rights. You can also creater either administrator or group and custom configure their profile.

1. Under the first question, **What do you want to create?**, define which type of object you want to create by selecting the corresponding radio button either for the administrator or the administrator group. If you are creating a group, it is by default marked as being synchronized with a directory server. If you do not want to populate the group in this way clear the **From Directory Server** box.
2. Under question **What do you want to create?** define if you want to let CM automatically create a full administrator or group or if you want to configure the object's profile yourself by selecting the corresponding radio button.

> Be aware that any administrator or group that you create with the automatic configuration cannot have more rights than the administrator account with which you are currently logged on. This means that, even though the explanation says

that the new administrator can create, edit and delete all objects, he will not be able to create, modify and delete operational rules, for example, if you do not have these capabilities. Neither will you be able to assign these capabilities to him via the manual configuration.

3. If you are using the automatic creation for all options click **Finish** now.
   The wizard closes and the new administrator or group is immediately created with the maximum rights possible.
4. If you are configuring at least part of the options or synchronizing the group with an active directory server click **Next** to continue with the configuration.

Make sure you made the correct selections in this window, because once you clicked the Next button you cannot come back to it. If you want to change your selection you must cancel with wizard and start again.

Defining the new administrator properties

In this wizard window, **Create Administrator**, you can define specific properties of the new administrator.

1. Enter the login name with which the new administrator is to log on to the console into the **Login** box.
2. *Optional:* Enter the first name of the new administrator into the **First Name** box.
3. *Optional:* Enter the family name of the new administrator into the **Last Name** box.
4. *Optional:* Enter the office phone number of the new administrator into the **Office Phone** box.
5. *Optional:* Enter the home phone number of the new administrator into the **Home Phone** box, if available.
6. *Optional:* Enter the mobile phone number of the new administrator into the **Mobile Phone** box, if available.
7. Optional: Enter the email address of the new administrator into the **Email** box.
8. Optional: Enter the company name the new administrator works for into the **Company** box.
9. *Optional:* Enter the department name or ID in which the new administrator works into the **Department** box.
10. *Optional:* Enter the job title of the new administrator into the **Title** box.
11. *Optional:* Enter the employee ID of the new administrator into the **Employee ID** box.
12. *Optional:* Enter the office or town or country in which the new administrator is based into the **Location** box.
13. *Optional:* If the administrator should only be created but not yet activated, clear the **Account Enabled** box. In this case the administrator will be created but he cannot yet log on to the console and the database In this case the icon of the administrator will appear dimmed in the console.

14. *Optional:* If the new administrator should be able to modify part of the personal data of his account, such as the optional items above, even though he does not have write access to his account check the **Modify Personal Information** box.
15. Optional: Enter some additional explanation into the **Notes** box.
16. Optional: If you do not want the focus of the console to move to the newly created administrator clear the **Go to the new administrator** after clicking the **Finish** button box.
17. If you are using the automatic creation for this administrator click **Finish** now.
    The wizard closes and the new administrator is immediately created with the maximum rights possible.
18. If you are configuring at least part of the options click **Next** to continue with the configuration.

Defining the new administrator group properties

In this wizard window, **Create Administrator Group**, you can define specific properties of the new administrator group.

1. Enter the name for the new group into the **Name** box.

   > If you are synchronizing the new group with a directory server this text box is dimmed, as the name of the group is automatically updated with the name of the selected OU.

2. *Optional:* Enter some additional explanation into the **Notes** box.
3. If you are using the automatic creation for this administrator group without synchronization click **Finish** now.
   The wizard closes and the new administrator group is immediately created with the maximum rights possible.
4. For synchronization you need to enter the DN entry of the directory server with which to synchronize into the **Group Entry DN** box, click **Select a Directory Server**.
   The **Select a Directory Server** window appears.
   The dialog box lists all available directory servers with their organizational units (all available user groups).
5. If the directory server you want to synchronize with is not displayed in this list, that is, it has not yet been created in CM, you can directly create it from here as follows:
   a. Click the **Create and connect to a new directory server** button.
      The **Properties** dialog box appears on the screen.
   b. Enter the required information into the respective boxes (see topic Creating a Directory Server for more information).
   c. Click **OK** to confirm the new directory server.
      The window closes and the new directory server is added to the list of available servers in the **Select a Directory Server** dialog box.
6. Select an entry from the list, you can either select the directory server itself or one of its children. You have the following options:

- *(Optional)* Select a directory server root and the check the box **Synchronize All Administrators** to synchronize all administrators of this active directory server.
- Select an OU of a listed server to synchronize all administrators below this OU, including all those of existing sub-OUs.
- *(Optional)* Check the **Include Users with Specific Primary Group** box to include all user for which the default primary group was modified.

> - Be aware that this type of synchronization does not recreate the directory structure of the OUs in CM, it will import all administrators in a flat list into the new group (contrary to the other types of groups in CM administrator groups cannot have subgroups).

7. Click **OK** to confirm.
   The **Properties** window appears.
8. Select the authentication type from the **Authentication** list and the login type from the **Login Type** list.
9. Click **OK.**
   The window closes and the group name above is automatically updated to the name of the selected OU of the server.
10. Click **Next.**

Defining the capabilities of a new administrator or administrator group

The **Capabilities** step provides the list of available capabilities, which are grouped by their functionality type. These capabilities define which of the the CM functionalities administrators and administrator groups can access in the console. A granted access is indicated via a green check symbol , refused access via a red , and granted access that is inherited via a group an administrator is a member of with this symbol .

> Be aware, that when an administrator is assigned a capability twice, once directly and once via a group, the group capability "overwrites" the individual one.

1. To assign the new administrator or group a specific capability mark the respective check box.

> Checking the **Manage** capability automatically also checks the **View** capability.
> For more information about the individual capabilities and what type of access they provide see topic The Capabilities node of Security Profiles.

2. *Optional:* Click **Select All Capabilities** to assign the new object all available capabilities.

3. Click **Next.**

Defining the access via static objects

This window enables defining which of all existing database object types and objects an administrator is to be able to access and in which way. Be aware, that to access an individual object the administrator must be assigned at least read access to the respective top node. For example, the administrator must be have at least view access to the **Reports** top node, to access a specific report.

By default this tab will always contain one entry, the respective administrator himself. When an administrator is created he will automatically be added here to provide him with the possibility to check his access rights. The default access defined at creation time is **Read Access** access allowed, any other access denied.

> **Note**
>
> When adding objects to the security profile, be careful to always include the complete hierarchy to the target object including the object's top node, otherwise the administrators might still not be able to access the object.

To add a database object, proceed as follows:

1. Click **Add Object** .
   The **Select Static Objects** dialog box appears on the screen.
2. In the drop-down box **Object Type** select the type of the database object to add.

   > This list is pre-filtered according to your licenses.

3. The box to the left will now display the options in the form of icons, according to which you can select static objects, that is, you can chose between the **Hierarchy, All** and **Search,** for devices and groups you also have the option **Topology.** If you selected the option Top Nodes the field displays the complete list of all top nodes available in the console, so they can be added directly.
   The contents of the following **Available Objects** list box will change to display the list of all objects of this type.
4. Select one or more objects from this window, or search for specific objects through the **Search** tab.
5. Click **Add** to move the selected objects to the Selected Objects box.
   The **Properties** dialog box appears to define the type of access for the selected objects.
6. Select the respective radio buttons and then click **OK.**

> Check the option **Respect Windows permissions** when accessing files and the **Registry** in the **Direct Access Acknowledgement** panel if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account.
> This option is only applicable to devices.

The objects will be added to the **Selected Objects** box in which they will be listed with their name and their type.

7. If you would like to add objects of another type as well, repeat the preceding steps.
8. Click **OK** to add all selected objects to the list of security objects of the security profile.
9. Click **Next.**

Defining the access via dynamic access

The access to the dynamic objects is assigned indirectly though other objects, a query, a device group or a folder. This means, that when dynamic access is assigned, the objects to which the administrator has access might not always be the same.

Query:

A query defines via its target type and its criteria to which objects the administrator has access. These can change either

- when modifications are made to the query itself, such as adding new criteria or modifying one, or
- when changes happen to the environment of the query, which in this case means the target type of the query. For example, a new device that is added to the network complies with the criteria of the query.

For example, administrator *admin1* is given access to query French. This query finds all administrators that are located in France, for example, *AdminParis*, *AdminLyon* and *AdminNantes*. A new administrator, *AdminNice* joins the company at a new location and is added to the database. Because his location is also in France, he will be automatically added to the list of administrators *admin1* has access to.

Device Group or Folder:

When providing access via a device group or a folder the administrator has access to all direct and indirect members of this group or folder. For example: the administrator *admin* is assigned the device group *Group 1* as a dynamic object. This group has the members *PC1*, *Group 2* and *Group 3*. *admin* now has access to *PC1* (direct member) as well as all members of *Groups 2* and *3*, that is *PC2* and *PC3* (indirect members). admin will also automatically have access to all PCs that are added to either of these groups. If members are removed from one of these groups he will automatically lose access to the removed members.

For more information, see the following topics:

- Adding the results of a query to the security profile
- Adding the members of a device group to the security
- Adding the members of a folder to the security profile

Defining the new administrator group synchronization schedule

It is possible to only synchronize the group once initially, but you can also schedule regular synchronizations at specific times.

1. Select from the first list, **When do you want this group to be synchronized with the directory server?**, when you want to schedule the synchronization.
   Depending on your choice, the window content below this box changes.
2. Define the synchronization schedule by selecting the desired values from the boxes below.
   Depending on the choices you make, the window content below changes.
   The text in blue on top of the window updates with the selections and changes you make and explains the scheduling choices you made in more detailed form.
3. Check **Run a first synchronization immediately** box, if you want to run a first synchronization right now before the defined schedule is applied.
4. Click **Finish** when your schedule is defined.
   The wizard closes, the synchronization information is sent and is then executed according to the defined schedule.
   If you are synchronizing immediately you can follow the synchronization process on the Members tab of the new group as it populates.

Managing predefined administrator groups

The predefined objects also contain a number of further administrator groups for the following specific security scenarios:

- *Application Administrators*
- *Compliance Administrators*
- *Helpdesk Administrators*
- *Inventory Administrators*
- *Patch Administrators*
- *Reporting Portal*
- *Super Administrators*
- *Software Distributors*

- *Software Packagers*

However, these objects only provide the initial profile for these types of administrators. To be operable, they still need to be assigned their static and dynamic objects with the respective access rights as well as their members. The following topics guide you through the steps that are necessary to adapt some of these profiles to the policies of your company and your IT environment and to populated them:

- Super administrators synchronized with active directory
- Helpdesk administrators group

Super administrators synchronized with active directory

In this first example we will make the predefined super administrator group profile operable and populate it via Active Directory. For this task we have to execute the following steps:

- Defining the super administrator group
- Populating the group via active directory

Defining the super administrator group

Before starting this procedure make sure your directory server is properly configured in CM . You will find information about how to do so in the section dedicated to Directory Servers .

This super administrator profile is an almost exact copy of the predefined *admin* administrator, with the only difference that it can be edited and modified. This new super administrator thus has full read and write access to all already existing objects as well as any objects that will be created in the BCM database .

1. Log on to the console with a super administrator or the admin login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Select the group called *Super Administrators* .
4. Go to the **Static Objects** tab.
5. Click the **Edit > Add Object** menu item.
   The **Select Static Objects** pop-up window appears.
6. Select all **Top Nodes** in the left box.
7. Click **Add** .
   The **Properties** pop-up window appears.
8. Leave all selections as they are, that is **Read, Write and Assign** access **Allowed** and click **OK** .
9. Click **OK** to confirm the selected static objects.
10. Go to the **Dynamic Objects** tab.
11. Click the **Edit > Add Results of Query** menu item.
    The **Select Dynamic Objects** pop-up window appears displaying queries that currently exist in the BCM database .

12. Open the folder *BMC Client Management database* and select all the queries it contains. These queries ensure that the super administrator will be able to see all existing objects of any type as well as those that will be created in the future by any other administrator.
13. Click **OK** .
    The **Properties** pop-up window appears.
14. Leave the **Read, Write and Assign** access as they are, that is **Allowed** , and modify the *Direct Access Acknowledgement* and *Remote Control Acknowledgement* access to *Not Required* .
15. Click **OK** to confirm the access rights for the selected queries.

The administrator group, that is, the specific profile for this type of administrator is now defined and can be populated.

Populating the group via active directory

This super administrator profile is an almost exact copy of the predefined *admin* administrator, with the only difference that it can be edited and modified. This new super administrator thus has full read and write access to all already existing objects as well as any objects that will be created in the BCM database .

1. Select the subnode **Dynamic Population** of the *Super Administrators* in the left window pane.
2. Select the subnode **Directory Server** in the left window pane.
3. Select **Edit > Assign Server**
   The **Select a Directory Server** dialog box appears on the screen. The dialog box lists all available directory servers with their organizational units depending on the base object, that is, in this case it will only display all available user groups.
4. Select an entry from the list.
   You can either select the directory server itself or one of its children.
5. Click **OK** to confirm.
   The **Properties** dialog box appears on the screen. Here you can specify if all administrators are to be synchronized or you can synchronize with a specific user group by selecting it from the *Users* sub-node of the directory server.
6. Select the respective option from the list.
7. Click **OK** to confirm.
   A confirmation window appears.
8. Click **OK** to synchronize now.
   The connection with the directory server is established and all members of the selected entry are added to your current group. The **Directory Server Synchronisation** window appears as a confirmation listing all objects that were added with their status which in this case will either be *New Object* or *Error* . If more than 3000 elements are synchronized this window will be replaced by a simple confirmation message.
9. Click **OK** to close this window.

The name of your group will be changed to the name of the directory server entry followed by the full name of the server in dotted notation. In this case, if you synchronized it with an organizational unit called *Relay Servers* , our group will now were changed from *Super Administrators* to *Relay Servers.Full.Directory.Name* . If the selected group has subunits these will also be synchronized and added to the group as *subunit.group.server name* . The elements will be added to this group in a flat list ignoring any hierarchy they might were located in on the directory server.

Defining the Super Administrator Group

Before starting this procedure make sure your directory server is properly configured in CM . You will find information about how to do so in the section dedicated to Directory Servers .

This super administrator profile is an almost exact copy of the predefined *admin* administrator, with the only difference that it can be edited and modified. This new super administrator thus has full read and write access to all already existing objects as well as any objects that will be created in the BCM database .

1. Log on to the console with a super administrator or the admin login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Select the group called *Super Administrators* .
4. Go to the **Static Objects** tab.
5. Click the **Edit > Add Object** menu item.
   The **Select Static Objects** pop-up window appears.
6. Select all **Top Nodes** in the left box.
7. Click **Add** .
   The **Properties** pop-up window appears.
8. Leave all selections as they are, that is **Read, Write and Assign** access **Allowed** and click **OK** .
9. Click **OK** to confirm the selected static objects.
10. Go to the **Dynamic Objects** tab.
11. Click the **Edit > Add Results of Query** menu item.
    The **Select Dynamic Objects** pop-up window appears displaying queries that currently exist in the BCM database .
12. Open the folder *BMC Client Management database* and select all the queries it contains.

    > These queries ensure that the super administrator will be able to see all existing objects of any type as well as those that will be created in the future by any other administrator.

13. Click **OK** .
    The **Properties** pop-up window appears.

14. Leave the **Read, Write and Assign** access as they are, that is **Allowed** , and modify the *Direct Access Acknowledgement* and *Remote Control Acknowledgement* access to *Not Required* .
15. Click **OK** to confirm the access rights for the selected queries.

The administrator group, that is, the specific profile for this type of administrator is now defined and can be populated.

Populating the Group via Active Directory

This super administrator profile is an almost exact copy of the predefined *admin* administrator, with the only difference that it can be edited and modified. This new super administrator thus has full read and write access to all already existing objects as well as any objects that will be created in the BCM database .

1. Select the subnode **Dynamic Population** of the *Super Administrators* in the left window pane.
2. Select the subnode **Directory Server** in the left window pane.
3. Select **Edit > Assign Server**
   The **Select a Directory Server** dialog box appears on the screen. The dialog box lists all available directory servers with their organizational units depending on the base object, that is, in this case it will only display all available user groups.
4. Select an entry from the list.

   > You can either select the directory server itself or one of its children.

5. Click **OK** to confirm.
   The **Properties** dialog box appears on the screen. Here you can specify if all administrators are to be synchronized or you can synchronize with a specific user group by selecting it from the *Users* sub-node of the directory server.
6. Select the respective option from the list.
7. Click **OK** to confirm.
   A confirmation window appears.
8. Click **OK** to synchronize now.
   The connection with the directory server is established and all members of the selected entry are added to your current group. The **Directory Server Synchronisation** window appears as a confirmation listing all objects that were added with their status which in this case will either be *New Object* or *Error* . If more than 3000 elements are synchronized this window will be replaced by a simple confirmation message.
9. Click **OK** to close this window.

The name of your group will be changed to the name of the directory server entry followed by the full name of the server in dotted notation. In this case, if you synchronized it with an organizational unit called *Relay Servers* , our group will now were changed from *Super Administrators* to *Relay*

Servers.Full.Directory.Name . If the selected group has subunits these will also be synchronized and added to the group as *subunit.group.server name* . The elements will be added to this group in a flat list ignoring any hierarchy they might were located in on the directory server.

Helpdesk administrators group

This administrator requires access to all devices, either via the device groups or the device topology.

1. Log on to the console with a super administrator or the admin login.
2. Then go to the **Global Settings** and the **Administrator Groups** node.
3. Select the group called *Helpdesk Administrators* .
4. Go to the **Static Objects** tab.
5. Click the **Edit > Add Object** menu item.
   The **Select Static Objects** pop-up window appears.
6. Under the **Top Nodes** select the **Device Groups** entry.
7. Click **Add** .
   The **Properties** pop-up window appears.
8. Leave all selections as they are, that is **Read** access **Allowed** , and **Write and Assign** access **Denied** , and click **OK** .
9. Click **OK** to confirm the selected static objects.
10. Go to the **Dynamic Objects** tab.
11. Click the **Edit > Add Results of Query** menu item.
    The **Select Dynamic Objects** pop-up window appears displaying queries that currently exist in the BCM database .
12. Open the folder *BMC Client Management database* and select the queries *All Devices* and *All Device Groups*.
    These queries ensure, that the administrator will be able to see all existing devices and devices as well as those that will be created in the future by any other administrator.
13. Click **OK** .
    The **Properties** pop-up window appears.
14. Leave the **Read, Write and Assign** access as they are, that is **Allowed** .
15. For the **Direct Access Acknowledgement** and **Remote Control Acknowledgement** you have the following possibilities, make your selections according to your company policies:
    a. **Direct Access Acknowledgement**
       - **Required**
         Select this radio button if system credentials must be provided to access the remote devices.
       - **Not Required**
         Select this radio button if no system credentials are required to access the remote devices.
       - **Respect Windows permissions when accessing files and the Registry**
         Check this box if the access rights to the local files and the Windows Registry are to be restricted to those those of the local account.

b. **Remote Control Acknowledgement**
   - **Required**
     Select this radio button if system credentials must be provided to access the remote devices in any case.
   - **Not Required**
     Select this radio button if no credentials are required and then define for which case this selection is applicable: **If User Absent** , **If Session is Closed** or both.

> The **Inherited** option is only of interest if you are defining this profile for an individual administrator instead of a group. In this case you can select this radio button if the access rights are to be inherited from the administrator group(s) the administrator belongs to. As long as the administrator is not a member of a group this option is interpreted as **Deny**.

16. Click **OK** to confirm the access rights for the selected queries.
17. The administrator group, that is the specific profile, for this type of administrator is now defined and can be used. It now only remains to add the administrators that are to be equipped with these types of rights.
18. Click **Add Administrator** .

> **Note**
>
> If no administrators are created yet you can also create them directly here by clicking **Create Administrator** instead.

The **Select an Administrator** pop-up window appears.

19. Select the administrator(s) to add to the group.

> **Note**
>
> Be aware, that if this administrator is also a member of a group with more extensive access rights, he will ONLY have the rights of this more restrictive group, because the denied right always overwrites the allowed right.

20. Click **OK** .
    The administrator is now added to the group and assigned with all capabilities and rights accorded to the group and displays in its **Members** tab.

You can now log off the console and log on again with the administrator login that is a member of this *Helpdesk Administrators* group and execute the required operations.

Managing access rights and capabilities for specific cases

While for most objects of the BMC Client Management database security on the capabilities and access levels can be defined in the same way, there are some exceptions to the rule, which are detailed as follows:

- Managing administrator capabilities
- Managing device topology access
- Managing devices and device group capabilities
- Managing access rights and capabilities for asset discovery

Managing administrator capabilities

The administrators, their groups and their capabilities have specific requirements regarding their security settings for both the capabilities as well as in the definition of their access.

The following topics are provided:

- Capabilities
- Access Rights
- Modifying administrator rights

Capabilities

The capabilities defined for the operation with administrators, administrator groups and capabilities are the same. This means, that there is no distinction between working on an individual administrator or on working with a group. It also includes working on the capabilities through their specific node. For example, if an administrator is assigned the capability to manage administrators, he will also be able to create administrator groups and he can also modify or delete these groups as well as modify their capabilities, through the **Capabilities** tab or through the **Capabilities** node.

Access Rights

As you can see on the console neither the **Administrators** nor the **Administrator Groups** node have a **Security** tab. Access rights must therefore be defined individually through the **Security Profile** node or the **Security** tab of the respective administrator or administrator group.

Modifying administrator rights

When a new administrator is created in the database, he is automatically added to his own **Security** tab with the following access rights defined: *Read Allow* and *Write Deny* . Through this the newly created administrator is able to see himself in the console and to check his capabilities, for example, but he cannot make modifications to any of his settings.

When an administrator is to modify access rights to a specific object he must have the following capabilities and rights:

Capabilities

- View Administrators
- View Security
- Manage Security
- View Object Type
- Manage Object Type

Access Rights

- Read and write access on the object itself.

It is strongly recommended to *not* provide the general administrators with the possibility to modify their security settings, only the superadministrator should have this option. If administrators can modify their own settings they might gain access to objects, to which they should not.

Managing device topology access

The **Device Topology** node is not an object in the database and as such does not have a specific **Security** tab defining its accessibility and it cannot be included in the **Security Profile** either. It will thus always be part of the directory tree of every administrator, even if some of them cannot see anything under the top node. To view devices under this node:

- The administrator has at least the **View Devices** capability. The administrator must have at least read access to the devices. Be aware that he needs read access to the complete hierarchy to these devices, that is, to the master as well as all the relay hierarchy under which the devices are located.

To provide your administrator with read access to all devices in the system in the **Device Topology** node, the following steps must be executed:

- Creating the query
- Defining the security access
- Verifying the assignment and access rights

Creating the query

For the first step, how to create a query. For more information, see Managing queries. The query *All Devices* was imported with the predefined objects.

Defining the security access

The action which remains to be done is to create the appropriate access rights for the administrator to be able to see them in the topology.

1. Connect as the superadministrator *admin* to the console.
2. Go to the administrator's node, and select its **Security Profile** node.
   The **Capabilities** tab will be displayed.

3. Select a row in the table and then click **Edit> Properties** .
   The **Properties** dialog box appears.
4. Check at least the *View* capability for devices, then click the **OK** button to confirm.
5. Select the **Dynamic Objects** tab.
6. Click **Edit> Add Results of Query** .
   The **Select Dynamic Objects** dialog box appears, displaying all queries.
7. Select again the *All Devices* query from the list.
8. In the **Properties** dialog box leave the **Allow** radio button for **Read** , **Write** and **Assign Access** selected.
   Remember here you are not assigning access to the query itself, but to its result, that is, the devices it will collect.
9. Click **OK** to add the object and close the dialog box.

Verifying the assignment and access rights

Now to check if everything works as intended proceed as follows:

1. Log off the console.
2. Re-logon to the console as the new administrator.
   When the console opens on your screen, you should see at least the following top nodes, depending on which capabilities you assigned additionally:
   - Search
   - Global Settings
   - Device Topology
3. Now select the **Device Topology** node.
4. In its **Members** tab you can see the same list of devices as in the group.
5. If you select the **Graph** tab, you will see all your devices in the form of the graph.

Having executed all these operations your administrator can see all managed devices in your system. However, this complete view can be limited by removing access to all devices which he is not supposed to see. This can be done via the query through more restrictive criteria.

Managing devices and device group capabilities

Devices and device groups are a specific case, because devices cannot be seen or accessed in any way if the corresponding permissions, capabilities and access rights, have not been accorded to the device groups they are a member of.

Capabilities

Contrary to the administrators and their groups, devices and device groups have separate capabilities which must be assigned. Assigning the capabilities for device groups follows the general rules, but if devices are to be viewed/managed as well you need to specify these

capabilities separately as well. Device groups also have an extra capability, **Populate** , which must be defined when the content of the group is concerned, such as when you manually add or remove a device from a group or when the group is to be dynamically managed through a query or a directory server.

Access Rights

Devices can be accessed under two different nodes: the **Device Topology** and the **Device Groups** nodes. How to define the access to the devices in the **Device Topology** is explained in the following paragraph, and can be sufficient for a specific type of administrator. However, in other cases, it might be useful for administrators to be able to access their devices via the **Device Groups** node. For this to be possible, you need to assign at least read access to the **Device Groups** top node as well as any other device group (including its hierarchy structure to access the respective group) the administrator needs to access.

Managing access rights and capabilities for asset discovery

The **Asset Discovery** presents the following specific situations:

- Wizards
- Scan targets
- Scanners

Wizards

To be able to launch the scanning wizard an administrator needs to have the **Asset Discovery** view capabilities on scan configurations, target lists and devices as well as the manage and assign capability on scan configurations.

The wizard can either use existing objects to execute or they can create new ones. Be aware, that to create new objects you need the manage capability for the top node of the respective object or at least one of its folders. By default objects created with the wizard will be located directly under the object‘s top node. If you do not have access to this node the new object will be created in the first folder for which you do have access rights. Otherwise, that is, if you do not have access to any of the objects of the type the object created via the wizard will be stored under the **Lost and Found** node.

Scan targets

Target lists in **Asset Discovery** can consist of devices known to the database, thus with defined security and devices without CM agent . Once a scan is executed on a target list the vulnerability inventory will be available via the console and the administrator, who created the scan can see the inventory for all the devices he was not expressly forbidden the access. As yet unknown devices without CM agent will be added to the database now with the status 'scanned' and no security defined, and any administrator with read access on the respective target list and thus the target devices can view the scan results.

Scanners

To define a device as a scanner or remove it from this functionality the *Manage* capability as well as *Write* access rights one the respective device are required.

As scans are assigned to their scanner and not to a top node of this type, when removing a device as a scanner all scans assigned to this scanner will also be removed. The administrator therefore also must have the capability *Scan - Manage* , as well as the *Write* access rights to all scans and folders defined under the respective scanner.

Using BMC Client Management tools

BMC Client Management provides a number of tools that help you with administering the BMC Client management. You can access these tools from the **Tools** menu.

- Sending an email
- Importing Out-of-the-Box objects
- Importing report templates
- Creating upgrade packages
- Cleaning up old packages

Sending an email

Before you can send a mail to an administrator or an administrator group you must ensure that the following settings were defined:

- Under **Global Settings > System Variables > Mail** , the **Mail Server Name** and **Mail Port Number** must be specified.
- Under **Administrators** , the **Email** box in the **General** tab of the administrators in question must be filled out.

CM allows you to directly send the contents of a console window as a report in html format to any recipient. This is done by selecting the console window to be sent and using the **Tools > Send a Mail** menu option and its **Define Mail** dialog box.

Proceed as follows to send an email containing the contents of a console window to another person:

1. Go to the console window which is to be sent as a report in html format.
2. Select **Tools > Send a Mail** and the **Define Mail** dialog box appears on the screen.

> To specify the recipients as direct recipients, copy recipients and blind copy recipients, you proceed in the same way.
> To enter recipients click **To** / **CC** / **BCC** and the **Select an Address** dialog box appears on the screen.

- To select an administrator or administrator group from the list select the **Select from List** radio button and then select the following recipient(s). You can specify an administrator group as the recipient, in this case the mail will be sent to all members of this group that have a valid email address entered into their general data tab.
- Or you can select the **Select Manually** radio button and enter any valid email address into the following text box. You can also enter more than one address by separating these through a semi-colon, for example, `scotty@enterprise.com; kirk@enterprise.com` .

3. Then you can change the **Subject** of the mail, by default when you open the dialog box the subject is BMC Client Management .

> The **Subject** box contains the name of the report which is being sent, which is always *report.html* . This box is not editable.

4. Below the **Subject** box you can see a free text box into which you can enter a message to the addressees. When the window first opens it contains a standard message informing the recipients that the mail contains a report of a CM Console view displaying the tab and node name of the right window pane, that the report was created from.
5. Click **OK** to confirm the mail and to send it.

The email is sent.

Importing Out-of-the-Box objects

It is possible to import the predefined objects (out-of-the-box objects) later on if you have not done so during the master setup, or to import a later version than the one you have.

To import out-of-the-box objects, proceed as follows:

1. Select **Tools > Import Out-of-the-Box Objects** .
   The **Out-of-the-Box Object Import** window opens on the screen.
2. Select the language of the predefined objects from the drop-down box.

> If no predefined objects have previously been imported, the import process will be launched directly and you can continue directly with step 5. Otherwise the **Import Results** window opens on the screen if you already imported an earlier version of this file. It lists all predefined objects that are contained in this new file with their object type.

3. Select all objects that are to be added or updated by marking the respective check box in the **Update** column.
4. To update all objects select **Select All Objects** .
5. Click **OK** to confirm the import and close the window.

The predefined objects will now be imported. The selected new ones will be added, those that already exist will be updated to their newest version.

Importing report templates

Report models can be imported into CM at any time. After their templates are created and put in the proper location on the master, they can be directly imported in the console.

To import report templates, proceed as follows:

1. Put the template files (.xml) in the the following directory: `[BMC Installation Directory]/data/Vision64Database/reporttemplates`
2. Click **Tools > Import Report Templates**  .
   The **Schedule Report Template Import** window appears.
3. Specify in this window if you want to import the template immediately or if you want to set a date and time for the import.
4. Click **OK** to proceed.

The import of new report templates is launched at the specified moment.

Creating upgrade packages

The installed CM agents can be upgraded very easily via an automatic upgrade which is executed through an operational rule from any earlier version to the most recent version. When the master agent is upgraded to the newest version, the required files for all supported operating systems will be automatically stored in a specific directory on the master, **<InstallDir>/Master/upgrade/packages/** , in .zip format. At master agent startup, the upgrade packages will automatically be created and thus published on the master, associated with the respective operational rule in a new directory called Client Management Upgrade . The only remaining manual operation during the upgrade process is the assignment of the target devices to the upgrade package. This upgrade process can be used to directly upgrade from any previous agent version to the most recent version.

If you are using the standard upgrade packages you do not need to use this option, all packages for all operating systems are automatically created. However, if you want to create and use your own upgrade packages you need to proceed as follows:

1. Copy your customized upgrade files to the **<InstallDir>/Master/upgrade/packages/** directory.
2. Log on to the console with a super administrator login or equivalent rights.
3. In the console window select **Tools > Create Upgrade Packages**  .

One custom package (.cst) per .zip file will be created in the same location together with its respective operational rule and placed in **Client Management Upgrade** directory under the **Packages** / **Operational Rules** top nodes.

The operational rule created to install the upgrade package contains in its comment box the version to which the agent will be upgraded. The operational rule will automatically contain as its first step the **Check Operating System** step, to ensure that the packages are distributed to the right target devices, and the necessary steps for package installation and to restart the agent after the install.

After the package is created, the .zip files will be deleted from their directory, thus making sure that the upgrade procedure will only be repeated when upgrading to the next version.

To upgrade the agents, the only remaining task to be done is to assign the devices or device groups to the respective packages and activate the rules.

Cleaning up old packages

This menu item of the **Tools** menu allows you to delete old packages of any type from its storing location (data/Vision64Database/packages) when a new version of the same package displays, that is, when a package was modified and republished. If you have activated the RemoveOldPackages option in the database configuration (Vision64Database.ini) file this operation will automatically be executed, that is, a package will automatically be deleted when a new version of it is published.

To clean up all obsolete packages, proceed as follows:

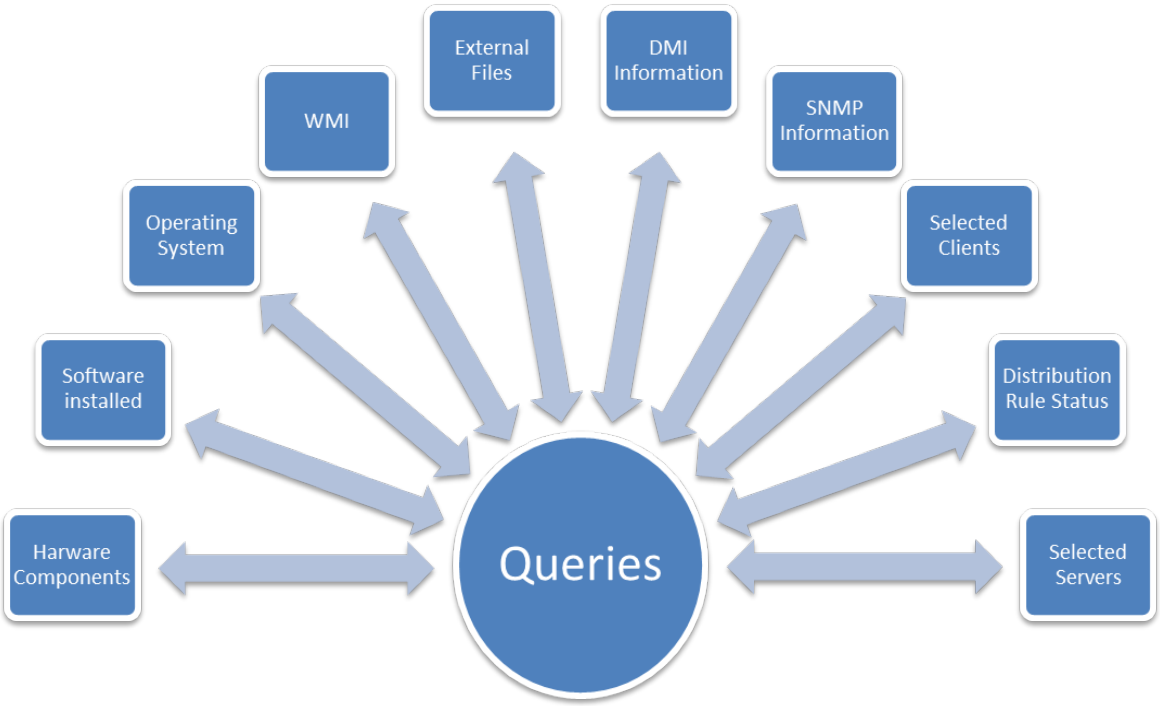
1. Anywhere in the console select the **Tools > Clean-up Old Packages** menu item.
   The obsolete packages will be automatically deleted.

Managing queries

Queries allow the dynamic grouping of clients based on administrator-defined criteria. One of the most common but also most cumbersome tasks has thus been automated.

If you want to know just exactly how many devices have 8 MB of RAM and a German keyboard layout, all you need to do is taking a look at your BMC Client Management console. If another twenty devices were added to your network with these characteristics, they will be automatically added to the device group representing those parameters. Of course you do not have to settle for RAM or keyboard layout - there are between 800 and 2000 variables to choose from, depending on the client's operating system.

Queries can be carried out on all BMC Client Management object types and objects (for example, operational rules, administrators, devices, etc.) and are either based on a single or multiple criteria and their values defined by the administrator. Query folders can be used as organisational containers for different types of queries. They can contain any number of predefined or custom-made queries or further query folders for the management of the client system. The following diagram provides an overview of queries:



Related topics

- Understanding types of queries
- Performing basic query tasks
- Performing advanced query tasks

Understanding types of queries

There are two types of queries in BMC Client Management:

- Predefined, criteria-based queries
- Free SQL queries

Predefined, criteria-based queries

Queries are composed of criteria which tell the agent on the target devices what to check for. The criteria available to the query depend on the type of the query, thus not all existing criteria are available all the time. The **Criteria** tab displays information about the criteria of the selected query and is only visible if the selected query is a criteria-based query.

The following table explains the different elements of the **Criteria** tab:

Name	Description
Query Status	This field displays the status of the query. When a query is newly created it will automatically become *active* . When a query is modified in any way, that is, criteria are added, removed or modified, the **Query Operator** is changed or the **Reverse Query Result** parameter is checked or unchecked, the query automatically becomes *inactive* . This means that all groups, device and user, to which the query is currently assigned will not re-evaluate their members anymore. This also means that any report of which at least one subreport is based on this query, or which is assigned to a group with this query will not be executed. After the query modification finished you must manually reactivate the query by selecting **active** from the list.
Query Operator	The boolean operator is active only in case of a multiple selection and defines the relationship between the individual criteria selected for the query. All criteria of a query are connected with the same operator. Possible values are: • *AND* When selecting this operator, the result of the query will provide you with objects that fulfil ALL criteria defined for the query. For the *AND* operator an INNER JOIN is used. for example, the criteria defined are: Device Name contains 1 *AND* Device Name contains 2. The result will only display devices of which the name contains either the number combination 12 or 21, such as France 123 or UK 210. Devices with a name like French 1 and French 2 will not be included. This option is the default value. • *OR* This operator defines a query where only one of all criteria defined must be fulfilled to be part of the result. For the *OR* operator a LEFT OUTER JOIN is used. The result for the same example as mentioned in the preceding paragraph with the *OR* operator would contain devices with names such as France 1, France 2, Device 12 and Device632.
Reverse Query Result	Check this box, to display the reversed results of the query. In this case the result will contain all objects which do *not* correspond to the selected criteria.
Category	The fields in this column display the category to which the selected criterion belongs to. The existing categories are the same as the query types.
Attribute	This field displays the name of the criterion. The Parent Name attribute returns the devices which are directly below the respective parent. If your hierarchy contains several cascading relay levels a Parent Name attribute/criterion must be added for each relay, to take into account all devices. For this case select *OR* as the operator.
Operator	The fields in this column display the selected operator, which may be one of the following: **Contains** , **Ends with** , **Equal to** , **Greater than** , **Greater than or equal** , **Less than** , **Less than or equal** , **Like (SQL)** , **Not equal to** , **Not like (SQL)** , **Starts with** , **Is Null** and **Is Not Null** .
Value	This field displays the value defined for the attribute.
Reverse Criterion Result	If the result of the criterion definition is to be reversed this field indicates ***Yes*** .If the criterion defines for example to find all devices on which Microsoft IE is installed and this option is activated, the final result of this criterion will be all devices on which IE is *not* installed.

Free SQL queries

Free SQL queries can be entirely freely composed of SQL syntax according to your requirements. It can be assigned to populate device groups and be used as the base for subreports, also they can be selected as static and dynamic objects within administrator or group security profiles. Contrary to criteria-based queries this type of query is always *active*. The **SQL** tab displays information about the selected query and is only visible if the selected query is a free SQL query.

The following table explains the different elements of the **SQL** tab:

Name	Description
Query Status	This field displays the status of the query. When a query is newly created it will automatically become *active* . When a query is modified in any way the query automatically becomes_inactive_ . This means that all groups, device and user, to which the query is currently assigned will not re-evaluate their members anymore. This also means that any report of which at least one subreport is based on this query, or which is assigned to a group with this query will not be executed. After the query modification finished you must manually reactivate the query by selecting **active** from the list.
SQL Query	You can directly enter into this text box your SQL query. **Note:** Be aware of the following specifications when creating your free SQL query: The query must start with ***SELECT***. The ***FROM*** must include the base table linked to the query type: if the type is *Device* , the query need to include the *Device* table. The query cannot include the following operators: ***COUNT***, ***SUM***, ***AVERAGE***, ***MAX***, ***MIN***, and SQL commands such as ***UNION***, ***INTERSECT***, ***EXCEPT***, ***MINUS***, and so on.
SQL Result	This text box displays the result of the query syntax verification.

Performing basic query tasks

The basic tasks for queries include:

- Creating a query
- Creating a query folder
- Modifying a query
- Deleting a query or a query folder

Creating a query

1. Select **Queries** in the left window pane.
   If you want to create the new query within a query folder, select the respective query folder before continuing with step 2.
2. Select **Edit> Create Query** .
   The **Properties** dialog box appears.
3. Enter the desired data in the respective boxes.
4. Click **OK** at the bottom of the window to confirm the data for the new query.
   A new query was created. It directly displays in the table in the right window pane.

Creating a query folder

1. Select **Queries** in the left window pane.
2. Select **Edit > Create Query Folder** .
   The **Properties** dialog box appears.
3. Enter the desired data in the respective boxes.

4. Click **OK** at the bottom of the window to confirm the data for the new query folder.
   A new query folder with the specified properties has been created.

Modifying a query

1. Select **Queries** in the left window pane.
2. Select the query to change to a free query in the table in the right window pane.
3. Select **Edit > Properties** .
   The **Properties** dialog box appears.
4. Check the **Free Query** box.
   A confirmation window appears.
5. Click **OK** to confirm the modification.
   The modification of the query comes into operation.

> **Note**
>
> You can change the query type only in one direction: from a criterion query to an SQL query. SQL queries cannot be converted to criterion queries. When a criterion query is converted, the SQL syntax of its criteria will be displayed in the **SQL** tab.

Deleting a query or a query folder

Queries which are assigned to other objects cannot be deleted. If the query folder to be deleted contains any members, they will be moved to **Lost and Found** under **Global Settings**.

> **Note**
>
> When deleting a query you lose all criteria definitions as well.

To delete a query or a query folder,

1. Select **Queries** in the left window pane.
2. Select the query or query folder to delete in the right window pane.
3. Select **Edit > Delete** .
   The selected object will be deleted immediately.

Performing advanced query tasks

The advanced tasks for queries include:

- Adding criterion to a query
- Modifying criterion of a query
- Modifying a free SQL query

- Removing criterion from a query
- Creating groups from a query

> **Note**
>
> When you add, modify, or remove a criterion, the query becomes *inactive (*all the groups to which it is assigned, will not re-evaluate their members anymore). You need to reactivate the corresponding query after adding, modifying, or removing a criterion.

Adding criterion to a query

1. Select **Queries** in the left window pane.
2. Select the query to which the new criterion is to be added in the left window pane.
3. Select the **Criteria** tab in the right window pane.
4. Select **Edit> Add Criterion** .
   The **Select Criterion** dialog box appears on the screen, displaying a list of available criteria.
5. Select the desired criterion.
   This will define the contents of the drop-down lists in the **Criterion Description** box of the same dialog box.
6. Define the operator by selecting the desired entry from the **Operator** list.
7. Define a value in the **Value** box by either entering the desired value directly or:
   If the value is not a free text value but must be chosen from values registered in the database, such as the inventory type, this box is dimmed and the method described below must be used to enter the value.
   a. Click **Find** next to the **Value** box.
      The **Search Criteria** dialog box appears on the screen.
   b. Select the operator according to which you want to launch the search from the **Operator** list.
   c. Enter the characters for the search into the **Value** box.
      If you are looking for a specific software, select **Contains** as the operator and enter the name completely or partially into the **Value** box.
      For example, if `Contains Maker` is defined, the search can return ***Filemaker*** , ***Framemaker*** , ***Pagemaker*** , and so on.
   d. Select the desired value from the results list.
   e. Click **OK** to continue.
8. If you selected a criterion with a time parameter in step 5, enter the desired time in either the **Value** or the **Timeframe** text box.
   You can simply enter a date and time in the standard user defined format in the **Value** box or find the value via the search functionality described in the second set of substeps of step 7. To enter a dynamic time value, select the newly displayed **Timeframe** radio button. Enter then the desired time value into the text box next to it and select the corresponding unit from the drop down list to the right.

9. If the result of the criterion definition is to be reversed, check the **Reverse Criterion Result** box.
   If the criterion defines for example to find all devices on which Microsoft IE is installed and this option is activated, the final result of this criterion will be all devices on which IE is *not* installed.
10. Click **Add** to add the defined criterion to the **Selected Criteria** list.

> **Note**
>
> You can add further criteria by repeating steps 5-9.

11. Click **OK** to add all selected criteria to the query.
12. Select **active** from the **Query Status** list.
    The selected criteria were added to the query selected in step 2 and the query was reactivated.

Modifying criterion of a query

1. Select **Queries** in the left window pane.
2. Select the desired free SQL query in the left window pane.
3. Select the **Criteria** tab in the right window pane.
4. Select the criterion to be modified in the table in the right window pane.
5. Select **Edit > Properties** .
   The **Select Criterion** dialog box appears.
6. Make the desired modifications in the **Operator** or **Value** boxes.
7. Click **OK** to confirm.
8. Select **active** from the **Query Status** list.
   The modifications of the criterion were saved and the query was reactivated.

Modifying a free SQL query

1. Select **Queries** in the left window pane.
2. Select the desired free SQL query in the left window pane.
3. Select the **SQL** tab in the right window pane.
4. Enter the your SQL query in the **SQL Query** field.

> **Note**
>
> Be aware of the following specifications when creating your free SQL query:
> - The query must start with ***SELECT*** .
> - The ***FROM*** must include the base table linked to the query type: if the type is *Device*, the query need to include the *Device* table.

- The query cannot include the following operators: ***COUNT***, ***SUM***, ***AVERAGE*** , ***MAX***, ***MIN***, and SQL commands such as ***UNION***, ***INTERSECT***, ***EXCEPT***, ***MINUS***, and so on.

5. Select **Edit> Verify SQL** .
   The database will verify your syntax and display the result in the following **SQL Result** . It will provide information about any errors it found, the detail level of which is based on your database system.
6. Select **Edit> Save Query** .
   The modifications of selected free SQL query are now saved.

Removing criterion from a query

1. Select **Queries** in the left window pane.
2. Select the desired free SQL query in the left window pane.
3. Select the **Criteria** tab in the right window pane.
4. Select the criterion to be removed in the table in the right window pane.
5. Select **Edit> Remove Criterion** .
   A **Confirmation** dialog box appears.
6. Click **OK** to confirm.
7. Select **active** from the **Query Status** list.
   The selected criterion was removed and the query was reactivated.

Creating groups from a query

From a query, you can create the following groups:

- Device group
- Patch group
- User group

To create a group, to which a query is assigned, the type of the query has to be *Device*, *Patch*, or *User*, respectively.

1. Select **Queries** in the left window pane.
2. Select the query for which you want to create a group in the right window pane.
3. Go to **Edit** and select one of the following to create corresponding group:
   - **Create Device Group** .
   - **Create Patch Group** .
   - **Create User Group** .

The new group will be created with the same name as that of the query, directly under **Device Groups**, **Patch Management**, or **User Groups** respectively, in the left window pane. The query assigned to it has the status: *active*.

Managing reports

BMC Client Management's design is based on a client-server model where the master includes the database which provides storage for all objects of your system, providing therefore a wide range of information about your devices and objects, even if a device is powered-off or contact is lost. But while this information about all objects resides in the database, it serves no purpose to you unless it is retrieved and displayed in a report, thus guiding you through the history of your system. These reports can then help you to gain a better understanding of what happened in your system. Through a good understanding of past performance, you can prevent issues in the future and continue efficient operations.

BMC Client Management provides customizable reporting capabilities that present database information in the form of reports in a user-specified order and format. Predefined reports are available. For example, inventory and software distribution reports. You can also create your own reports on any object in the database. Reports can be presented in different formats, such as a table or a customizable graph and, depending on their type, they can be formatted as HTML, XML or PDF.

When selecting the report style and format, think of what kind of system information you need to have in your hand at the end of the day, week, or month. Define what you want that information to look like. Keep in mind that these reports can be very useful as status reports to management for strategic decision making, thus they can be sent to specific locations where associates with the respective access rights can read them, or for yourself to perform trend analysis, for example.

The population on which the report is to be executed can be defined either through queries or via assigned groups. Queries define the target population per subreport. A report consisting of several subreports can contain information about different objects of the population - one subreport might be limited to devices and a second one to rollouts executed on the entirety of this object type. If you assign one or more groups to your report, these are applicable to all subreport of this report and they are executed on the respective groups only, that is, with assigned device groups you can only produce reports which contain data on objects of type device.

Reports are created and generated via the console. They can be sent to specifically defined people by email or they can be exported in predefined formats or put at the disposal of a larger group of users via the **Report Portal** of the agent interface.

The main **Reports** node is a full-featured reporting tool, designed to help you create reports about all objects in your system. With this report generator, you can generate different reports, such as inventory, device group, events or other statistical reports. In addition, report folders can be created as organizational containers for different types of reports. They can contain any number of reports and further predefined or custom-made report folders for the management of the client system.

The **Reports** node has the following subnodes:

- One for each report folder

- One for each report

BMC Client Management comes with a number of predefined reports for its different functionalities that are imported at the time of installation. These reports are available in all supported languages and can be found directly under the **Reports** top node and in their respective directories. Therefore, before creating a new report, check if there is a predefined report or an already existing one for the version of the report you want which can be duplicated.

Related topics

- Understanding types of reports
- Creating a report
- Creating a reports folders
- Deleting a report or a reports folder
- Managing report options
- Adding a pie chart to an existing report
- Managing subreports
- Previewing a report
- Scheduling report generation
- Assigning a report
- Generating a report
- Viewing report results
- Publishing a report
- Setting up email for mailing reports
- Managing Report Portal
- Importing new report templates
- Report creation wizard

Understanding types of reports

The BMC Client Management console provides two different types of reports:

- Style-based Reports
- Template-based Reports

For both these types, you can preview the defined report before you schedule it to either run only once at a specific time or to have it executed periodically and put at the disposal of specific members of your company.

Style-based Reports

Style-based reports are composed of subreports, of which each can have a different style, that is, it can have a different display format, such as a table, a pie or a bar chart. They are based on a layout type that defines the number of subreports the report contains and how these subreports are ordered on the displayed or printed page. 12 different layout styles are available. The subreport

appearance is based on a css style sheet. These reports are individually customizable through the report formatting tab which permits the configuration of the display output of a report in various formats. Style-based reports base their generated data on the results of a query, on the members of a device group or both. Style-based reports can only be generated in HTML format.

Template-based Reports

Template-based reports are not available for all CM object types and functionalities, they are available only for patch, power and application management, asset discovery, virtual devices, security products, diagnostic tools as well as for licensed applications and custom and SCAP compliance. These types of report are completely predefined, that is they cannot be modified, but for specific reports you do have a number of options that can be defined. The can be generated in HTML, XML and PDF format. You can also create your own report templates and import them.

Creating a report

1. Select **Reports** in the left window pane.
   If you want to create the new report within a reports folder, select the respective reports folder before continuing with step 2.
2. Select **Edit > Create Report**
   The **Properties** dialog box appears on the screen. For more information, see General reports data.
3. Enter the desired data in the respective boxes.
4. Click **OK** at the bottom of the window to confirm the data for the new report.

A new report was created. It directly displays in the table in the right window pane.

General reports data

The **General** tab presents in the right window pane the general information available for the selected report:

Name	Description
Name	Displays the name of the report.
Report Title	The title of the report, that is, the heading that will be displayed at the top of the report.
Report Type	The type of the report, that is, if it is style- or template-based.
Report Style	The general layout of the report. This defines into how many subreports the report is divided into. This parameter is only available for style-based reports.
Subreport Count	The number of subreports contained in the report. This number is defined by the report style.
Font Size	Defines the font size for this report. This may be a number between 8 and 18.
Font Type	Defines the font type family for this report. This is also the font type used for the PDF generation.

Name	Description
Style Sheet	Defines the style sheet to use when displaying the report.
Logo	Defines if the default company logo or a custom defined one is to be included in the report output.
Time Zone	Defines the time zone which is to be used for the date shown in the generated report: Possible values are: • **Greenwitch** : The time is to be calculated on GMT • **Master** : The time preferences of the master server are to be applied • **Administrator** : Applies the time zone chosen in the user preferences by the administrator requesting the report generation.
Date Format	Defines if the execution date and time of the report is displayed on the page and in which format. The date is always located on top to the right of the page. You may select not to format the date by selecting None, in this case the date is displayed in the default format of MM/DD/YYYY hh:mm:ss.
Language	Defines the language in which the report output is to be generated. All console languages are available for this choice.
Encoding	Defines the encoding to be used for report generation.
Report File Name	Defines the file name of the published report. If this field is empty, the file name of the report is generated with the date and time of its generation.
Public Report	Defines if the report is to be generally accessible via the **Report Portal** .

Creating a reports folders

1. Select **Reports** in the left window pane.
2. Select **Edit > Create Reports Folder**  .
   The **Properties** dialog box appears.
3. Enter the desired data in the respective boxes.
4. Click **OK** at the bottom of the window to confirm the data for the new reports folder.

A new reports folder with the specified properties has been created.

Deleting a report or a reports folder

If the report folder to be deleted contains any members they will be moved to **Lost and Found** under **Global Settings**.

> **Note**
>
> When deleting a report you lose all its definitions as well.

To delete a report or a reports folder , proceed as follows:

1. Select **Reports** in the left window pane.

2. Select the report or reports folder to delete in the right window pane.
3. Select **Edit > Delete** .

The selected object will be delete immediately.

Managing report options

This tab displays the generation options that are activated and defined for the respective report. The table only displays the defined parameters not all available parameters. For more information on modifying the report options, see Modifying report options.

Depending on the report object type no or only a limited number of options are available:

Asset Discovery

Name	Description
Hardware Inventory	Adds a hardware inventory summary to the report.
Software Inventory	Adds a software inventory summary to the report.
Security Settings Inventory	Adds a security settings inventory summary to the report.

Under the **Options** tab you can define specific parameters for the predefined report. Depending on the target object type different option parameters are available:

Custom Compliance

No options are available for reports on this object type.

Diagnostic Tool

No options are available for reports on this object type.

Software License Management

No options are available for reports on this object type.

Application Management

Name	Description
Export Format	Defines the format in which the report is to be exported and/or attached to the email to be sent. Depending on the report type (style or template based) different export formats are available. For template based reports, if the selected format is HTML, the file is exported with an *.HTML.XML* extension.

Patch Management

Name	Description
Critical Severity	Check this box to include all patches of critical serverity into the report.
Important Severity	Check this box to include all patches of important serverity into the report.

Name	Description
Moderate Severity	Check this box to include all patches of moderate serverity into the report.
Low Severity	Check this box to include all patches of low serverity into the report.
Unrated Severity	Check this box to include all patches of unrated serverity into the report.

Power Management

Name	Description
Start Date	Check this box if the report is to be generated for a specific time frame. The field to the right becomes available and displays a calendar when clicked on. Select the desired start date from the calendar. If the report is to be generated from the beginning of the collection up to a certain time, leave the box unchecked.
End Date	Check this box if the report is to be generated for a specific time frame. The field to the right becomes available and displays a calendar when clicked on. Select the desired end date from the calendar. If the report is to be generated from a specific date onwards until now leave the box unchecked.
Details by Device	Check this box to include the data split by individual device in addition to the collective data display.
Group by	Defines the distribution of the charts, **Status** in this case displays all device status values in one single graph. The report may also be grouped by **Hours of the Week, Day, Week, Month** and **Year** .
Unit	Defines in which unit the values provided in the graph are displayed. Depending on this choice some of the fields below becomes available or unavailable.
Use same scale for all devices	Check this box to use the same scale for all devices that are part of the report.
Device Consumption (Watt)	Defines the medium consumption of a device. This is currently between 300 and 500 watts, depending on the equipment of the device. Enter the corresponding value. This value is applicable if **CO2 Emission, Energy** or **Price** are selected as the unit.
Kilowatt Hour Rate	Defines the price of the kilowatt hour. This varies greatly depending on the different countries, therefore no default values have been provided. Enter the value corresponding to your electricity bill. This value is applicable if **Price** is selected as the unit.
Currency	Enter the currency in which the kilowatt hour price is defined above, for example, *GP* or *$* . This value is applicable if **Price** is selected as the unit.
CO2 Emission (g /kWh)	Defines the amount of CO2 in grams per kWh that is dispensed into the atmosphere while generating the energy required to run a computer. This value is applicable if **CO2 Emission** is selected as Unit.

Security Products

No options are available for reports on this object type.

Modifying report options

To activate and/or modify any or all of the available report generation options proceed as follows:

1. Click **Edit > Properties** .

Alternatively you can double-click the parameter.

The **Report Options** window appears providing access to the parameters.

2. Edit the parameters as required.
3. Click **OK** to confirm.

Adding a pie chart to an existing report

This example adds a pie chart to an existing report, displaying the same data that the report already shows in tabular format also in the form of a pie chart.

> **Note**
>
> You can either directly modify this report or first duplicate it and then modify the new report.

1. Select the **Reports > Global Software List** node in the left tree hierarchy.
2. Double-click an entry in the right window pane.
   The **Properties** window appears.
3. Select **Style5** in the **Report Style** drop-down list.
4. Click **OK** .
   The following **Subreport Count** box will change from 1 to 2 and the node in the left window pane will now display two subnodes
5. Go to **Subreport 1** in the left tree hierarchy.
6. Right-click the mouse and select the pop-up menu item **Copy** , as we displays the same data in the pie chart of the second subreport.
7. Now select **Subreport 2**
8. Right-click the mouse and select the pop-up menu item **Replace**
   The list of columns of the first subreport is now duplicated to the second subreport.

> **Note**
>
> Make sure that one attribute, the one according to which all entries are sorted, exist twice: once with an **Operator** , for example **Count** , and once as usual without operator but grouped by. This is absolutely obligatory for any type of graphical display otherwise the data can only be displayed in the form of a table.

9. Now select the **Format** tab to customize your pie chart.
10. From the **Subreport Format** drop-down list select the value **Pie Chart** .
    The following list now shows all available attributes for pie charts.

11. Double-click an entry in the right window pane.
    The **Properties** window appears.
12. Make the following modifications to enlarge and enhance the chart:
    - Check the **Value Labels** box.
    - Increase the **Chart Width** to 800.
    - Increase the **Chart Height** to 400.
    - Check the **Percent Labels** box.
    - Increase the **Maximum number of values** to 20.
13. Click **OK** .
14. To have a preview of the newly created subreport click the following **Subreport Preview** button.
    A new browser tab opens in which you can see how this subreport will appear in the final report.
15. Select the *Global Software List* report in the left tree hierarchy.
16. Click **View Last Result** .
17. Click **Yes** in the appearing pop-up window.
    A new browser window or tab opens and displays the report.
18. If the global software list is very long, you should use the pie chart subreport as the first one. To do so select the **Subreports** node in the left tree hierarchy.
19. Select the first subreport in the table to the right.
20. Click **Move Down** .
21. Then regenerate the report by clicking **View Last Result** .
22. Click **Yes** in the appearing pop-up window.

A new browser window or tab opens and displays the newest version of the report.

Managing subreports

Reports are made up of individual subreports, each of which provide a specific topic on your system. This topic can be defined through the query to which the subreport is associated and it can be further specialized by selecting specific attributes through the columns. The results of the subreport will in this case be limited by the selected query.

This option allows you to define reports on any object and its parameters in the database. You can also define subreports of which the results are limited through the population of a device group by assigning the report to a device group. The subreport can thus be configured exactly to your needs and specifications and be displayed in a format specifically adapted to the situation for which it is created and most adapted to the collected data.

Each subreport of the general report layout must be individually configured by selecting the columns, which displays the data of the report and the format in which the data will appear. The overall appearance of the subreports is defined by the css style sheet chosen for the report and is the same for all subreports.

This section includes:

Replacing a subreport

Individual subreports cannot be copied and pasted, because all subreports that a report might have, are directly created when the layout of a new report is chosen. However, it is possible to replace a subreport with another, already existing subreport. When you create a new report with several subreports, and one of these is to be identical to an already existing subreport of another report, you can replace this subreport with an existing one.

1. Select **Reports** in the left window pane.
2. Select the report you want to copy a subreport from in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be copied in the right window pane.
5. Select **Edit > Copy** .
   The subreport was copied to the clipboard.
6. Select the report you want to replace a subreport of in the left window pane.
7. Select its **Subreports** subnode in the left window pane.
8. Select the subreport to be replaced in the right window pane.
9. Select **Edit > Replace** .

The subreport selected in step 8 has now been replaced by the subreport from the clipboard. Its predefined column and format definitions were overwritten with those of the subreport from the clipboard.

Changing the order of subreports

By moving the subreports of a report up or down you can change their order within the report.

To change the order of subreports, proceed as follows:

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be moved in the right window pane.
5. Select **Edit > Move Up** or **Move Down** .

The selected subreport was moved up or down in the list of subreports.

Repeat step 5 until the report is at the desired position.

Managing columns of a subport

The columns contain the selected data that will be displayed in the subreport. The list of available columns is linked to the type of the associated query if one is selected, otherwise the available columns are those of type *Device* . Columns can be sorted and an operator can be applied based on the data type (**Sum** , **Count** , **Average** , **Minimum** , etc.).

> **Note:**
>
> When assigning a device group to the report to which the subreport belongs, the query, if you chose one in this tab, will be ignored when generating the report and all columns defined for the subreport will be deleted.

The following table explains the different elements of the **Columns** tab:

Name	Description
Query Type (list)	Defines the type of the report target, that is, on which type of CM object the report is to be generated.
Query Name (list)	Displays which query is assigned to the subreport. This list displays all queries to which the current user has access rights and which are available for the previously selected type. If you intend to assign the report to a device group and selected a query here, the report result will contain the data of the assigned group's members which are returned by the query. The subreport has the same number of lines as the query result. If part of the requested data were not provided by the object in question one or more lines or fields then stay empty in the subreport.
Object	The object is the database object on which the query is executed upon, for example, device for a query that is executed on device groups.
Attribute	Displays the attribute of the object for the column, such as HTTP Port, email address, and so on.
Operator	Displays the type of operator which is run on the values of the selected attribute, such as **Count** , **Average** , **None** , and so on. The type of operator displayed depends on the attribute selected in the preceding field.
Sort Order	Defines in which order the values are to be sorted, the possible values are **Ascending** , **Descending** or **None** .
Group By	Displays the value according to which the display is grouped, possible values are true for grouped by this attribute and false for not grouped by this attribute. If you select to group by more than one value, these values are aggregated for a more detailed representation of the data. For example, if you select in a report with a query of type *Device* to group by IP Address and HTTP Port, your charts will be shown grouped by the value IP Address: HTTP Port.
Heading	Indicates if the table is broken up in several tables depending on the different values of the selected heading. In this case the selected column is removed from the general table and its values are used as the title for the different tables displaying the values of the other columns. If no such value is selected all data will be shown in one single table.
Default Title	Displays a default title for the object to be displayed in the report. It will only be used if no customized title is defined.
Customized Title	Displays the user customized title for the report. It overrides the title defined by default. If this field is empty the default title will be used.

Related topics

- Changing the query associated with a subreport
- Adding columns to a subreport
- Changing the order of subreport columns
- Removing columns from a subreport

Changing the query associated with a subreport

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the left window pane.
5. Click the **Columns** tab in the right window pane.
6. Make the desired changes in the **Query Type** and **Query Name** boxes.
   When you change the query to one with a different query type, you will loose all columns that you defined for the prior query. The subreport was copied to the clipboard. The change of the query will automatically be saved and applied to the subreport. In case the new query is of a different type than the prior query, you'll now need to add the necessary columns provided by the new query to the subreport.

Adding columns to a subreport

If a query was replaced by one of a different type, its columns were lost, therefore you manually need to add the necessary columns to the new subreport query.

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the left window pane.
5. Click the **Columns** tab in the right window pane.
6. Select **Edit > Add Column**  .
   The **Select Report Columns** is displayed on the screen, displaying the available columns and their attributes for this query.
7. Add the desired columns to the subreport:
   a. Select the desired column from the **Available Columns** list
   b. Set the desired attributes in the **Attribute Description** area.
   c. Click  .
   d. Repeat the substeps a - c to add further columns.
8. Click **OK** to confirm the new columns.

The selected columns were added to the subreport.

Changing the order of subreport columns

By moving the columns of a subreport up or down, you can change their order within the subreport.

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the right window pane.
5. Click the **Columns** tab in the right window pane.
6. Select the column to be moved in the right window pane.
7. Select **Edit > Move Up** or **Move Down** .
   The selected column was moved up or down in the list of columns. Repeat step 7 until the column is at the desired position.

Removing columns from a subreport

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the left window pane.
5. Click the **Columns** tab in the right window pane.
6. Select **Edit > Remove Column** .
   A **Confirmation** dialog box appears.
7. Click **OK** to confirm the removal.

The selected column was removed from the subreport.

Managing format of a subreport

In the **Format** tab you can set up how the respective subreport will look like.

When defining the format of the subreport start with the final outcome of the data in your mind, think about what kind of information you are displaying and for which situation it is used, thereby taking into account the volume of the information as well.

The following table explains the different elements of the **Format** tab:

Name	Description
Subreport Format (list)	Defines in which format the data of the current subreport appears. The possible formats are **Bar Chart** , **Pie Chart** , **Line Chart** and **Table** . The following table lists all possible format options which can be modified.
Attribute	Displays all attributes which can be configured for the selected format. The list of possible options varies according to the chosen format.
Value	Indicates if the attribute is to be used for the formatting of the query data and at which value it is set. To modify any of these values call the **Properties** window through the menu item or the respective icon and execute the necessary modifications.

Name	Description
Notes	Displays a description of the attribute in the form of an explanation.

Related topics

- Changing the format of a subreport
- Modifying the format options of a subreport

Changing the format of a subreport

The format of a subreport defines in which way its data displays. Possible formats are: **Bar Chart** , **Pie Chart** , **Line Chart** and **Table** .

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the right window pane.
5. Click the **Format** tab in the right window pane.
6. Select the desired format from the **Subreport Format** list in the upper part of the right window pane.

The format of the selected subreport has now changed to the specified format.

Modifying the format options of a subreport

The format options define the general outlook of your subreport. You can modify these options to adapt the outlook to your liking.

To modify the format options, proceed as follows:

1. Select **Reports** in the left window pane.
2. Select the report to be modified in the left window pane.
3. Select its **Subreports** subnode the left window pane.
4. Select the subreport to be modified in the right window pane.
5. Click the **Format** tab in the right window pane.
6. Select any row displaying a format option in the table in the right window pane.
7. **Edit > Properties** .
   The **Properties** window displays on the screen, displaying all options available for the selected report format.
8. Make the desired modifications in the respective boxes.
9. Click **OK** to confirm the modification.

The desired modifications were saved and applied to the format of the selected subreport.

Previewing a report

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select **Edit > Preview**  .

A browser window appears displaying a preview of how the eventually generated report will look like.

Scheduling report generation

When a report is created, it is automatically assigned a scheduler. You can modify the schedule for the currently selected report from the **Assigned Schedule** tab of the **Reports** node to define when and at which frequency the report is to run. When it is created, the scheduler is deactivated by default. Initially, when a report is assigned to one or more objects of the same type, the same scheduler is created and applied to all objects. However, this common schedule can be modified for the individual object at their respective assigned reports location. The default settings of the scheduler's timer are to execute the report once a minute until manually stopped. The timer settings can also be modified manually by editing the CronSpec entry in the Timer module of the respective device.

Modifying the schedule of a report

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select the **Assigned Schedule** tab in the right window pane.
4. Select the schedule you want to modify.
5. Select **Edit > Properties**  .
   The **Scheduler** dialog box appears.
6. Make the desired changes the available options.
7. Click **OK** to confirm the modification.

The schedule for the selected report was modified. From now on the new timing is applied.

Note

Be aware, that only the schedules of those assigned objects is modified, that have not yet been individually modified in their respective locations.

Assigning a report

To assign a report to an object proceed as follows:

1. Select the main node containing the object you want to assign a report to in the left window pane.
2. Select the desired object in the left window pane.
3. Select its subnode **Report Results** in the left window pane.
4. Select **Edit > Assign Report** .
   The **Assign a Report** dialog box appears.
5. Select the desired report from the list in the dialog box.
6. Click **OK** to confirm the assignment.
   A confirmation window appears.
7. Click either the
   - **Yes** to immediately generate the newly assigned report.
   - **No** to only add it to the list of assigned reports.

The selected report was assigned to the selected object.

Generating a report

Next to scheduled generation, reports can also be generated on demand.

This section includes:

- Generating and viewing a style-based report
- Generating and viewing a style-based report assigned to a aevice group
- Generating and viewing a template-based report

To generate a report

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select **Edit > Generate Report** .
   A **Confirmation** dialog box, appears on the screen.
4. Click **Yes** to proceed.
   If the report to generate is of a template-based report, this window allows you to select the format in which the report will be generated. You may select HTML, XML, or PDF, or a combination of these. By default, a report is only generated in HTML. The report will be generated directly and put in all the required places according to its settings and assigned groups.

Generating and viewing a style-based report

1. Select the **Reports** node in the left tree hierarchy.
2. Select a report in the table in the left window pane, for example *Disks* .
3. Click **Generate Report** .
4. A confirmation window appears, click the **Yes** to confirm.
   The report will be created immediately using the current data of the database.

5. To view the newly generated report click **View Last Result** .

A new browser window or tab opens and displays the report.

Generating and viewing a style-based report assigned to a aevice group

All style-based reports can be assigned to device groups. This report will then display the same information but limited to the data of the assigned device group.

1. Select the **Reports** node in the left tree hierarchy.
2. Select a style-based report in the table in the left window pane, for example *Disks* .
3. Go to its **Assigned Objects > Device Groups** node.
4. Click **Assign Device Group** .
5. Select a device group from the window.
6. Click **OK** to confirm the assignment and close the window.
   The device group will be added to the table of assigned device groups.
7. Then go back to the report in the left window pane.
8. Click **Generate Report** .
9. A confirmation window appears, click **Yes** to confirm.
   The report will be created immediately using the current data in the database concerning the assigned device group.
10. To view the newly generated report click **View Last Result** .
11. Click **No** in the appearing pop-up window.

A new browser window or tab opens and displays the report.

> **Note:**
>
> The report result which is generated will be put in all the required places according to the reports settings. This means it is available under the **Report Results** node of the report, as well as under that of the device group it is assigned to.

Generating and viewing a template-based report

Template-based reports must be assigned to an object to be generated, for example, patch reports must be assigned to a patch group or a patch job, compliance reports to a compliance group or the power management report to a device group. If the report is already assigned continue directly with *point 6* of this procedure.

1. Select the **Reports** node in the left tree hierarchy.
2. Select a report in the table in the left window pane, for example **Configuration Summary** .
3. Go to its **Assigned Objects > Objects** node.
4. Click the **Assign Object** and select the desired object from the list.
5. Click **OK** to confirm.
6. Reselect the report in the left window pane.

7. Click **Generate Report** .
8. A confirmation window appears, click **OK** to confirm.
   The report will be created immediately using the current data of the database.
9. To view the newly generated report click **View Last Result** .
10. Click **No** in the appearing pop-up window.

A new browser window or tab opens and displays the report.

Viewing report results

Each time a report is generated, a new node is created in the **Report Results** node using the local generation date and time of the computer on which the report is generated for the report as its name. These report results are also automatically sorted into folders if they are generated for a specific objects such as a device group or a compliance rule. Report results are stored in the database indefinitely.

This section include:

- Viewing result of a report
- Viewing the last result of a report
- Viewing the result for a device group report
- Viewing the result of a specific, previously created report

The data on which the report result of a style-based report is based when being generated depends on the definition of the subreports:

- If the report is not assigned to any device group:
  - All subreports must be based on a query. The report result bases its data on the data returned by the queries.
- If the report is assigned to a device group:
  - If none of the subreports of the report are based on a query, the report result contains the data of the group members.
  - If a subreport is assigned to a query, the report result data is based on the group members which are returned by the query.

The results of a template-based report are always based on the data of the assigned object.

A **Report Result** subnode (for example **Reports > Your Report > Report Results > Device Group Results** for device groups) lists all objects that are assigned to this report in its table to the right and allows you to access the reports generated for each of these objects via its subnodes, of which it has one for each assigned object. These objects can be a custom compliance rule, an SCAP job, a patch job, a patch group, a device group or an individual device.

The following general information about a report is displayed:

Name	Description
Name	Displays the name of the report.
Report Title	The title of the report, that is, the heading that will be displayed at the top of the report.
Report Type	The type of the report, that is, if it is style- or template-based.
Report Style	The general layout of the report. This defines into how many subreports the report is divided into. This parameter is only available for style-based reports.
Subreport Count	The number of subreports contained in the report. This number is defined by the report style.
Font Size	Defines the font size for this report. This may be a number between 8 and 18.
Font Type	Defines the font type family for this report. This is also the font type used for the PDF generation.
Style Sheet	Defines the style sheet to use when displaying the report.
Logo	Defines if the default company logo or a custom defined one is to be included in the report output.
Time Zone	Defines the time zone which is to be used for the date shown in the generated report: Possible values are: • **Greenwitch** : The time is to be calculated on GMT • **Master** : The time preferences of the master server are to be applied • **Administrator** : Applies the time zone chosen in the user preferences by the administrator requesting the report generation.
Date Format	Defines if the execution date and time of the report is displayed on the page and in which format. The date is always located on top to the right of the page. You may select not to format the date by selecting None, in this case the date is displayed in the default format of MM/DD/YYYY hh:mm:ss.
Language	Defines the language in which the report output is to be generated. All console languages are available for this choice.
Encoding	Defines the encoding to be used for report generation.
Report File Name	Defines the file name of the published report. If this field is empty, the file name of the report is generated with the date and time of its generation.
Public Report	Defines if the report is to be generally accessible via the **Report Portal** .

Viewing result of a report

To display the report results for an object, proceed as follows:

1. Select the main node containing the object you want to assign a report to in the left window pane.
2. Select the desired object in the left window pane.
3. Select the subnode **Report Results** in the left window pane.
4. Select the desired report result in the right window pane.
5. Select **Edit > View**  .
   A browser window appears displaying the contents of the selected report result.

Viewing the last result of a report

When a report is scheduled to be generated at regular intervals, you can view the last generated report.

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select **Edit > View Last Result** .
   If the report is assigned to more than one group or generated in more than one format, the **Select a Group** window opens on the screen. Here you can specify which report you want to display, that is, select the group and the format which to display. A browser window appears requesting identification for the agent interface.
4. Enter your credentials in the respective boxes.
5. Click **OK** to continue.
   In the browser window, the last generated report appears.

Viewing the result for a device group report

To display the report results for a device group, proceed as follows:

1. Select **Device Groups** in the left window pane.
2. Select the desired device group in the left window pane.
3. Select the subnode **Report Results** in the left window pane.
4. Select the desired report result in the right window pane.
5. Select **Edit> View** .
   A browser window appears displaying the contents of the selected report result.

Viewing the result of a specific, previously created report

For generated reports, you can either view the last generated result or also a specific, previously created result.

To view a specific, previously created result,

1. Select the **Reports** node in the left tree hierarchy.
2. Select the report to view.
3. Select the **Report Results** subnode of the report in the left hierarchy tree.
4. Select from the list of previously generated report results in the table to the right the one to display.
5. Click **View** .

A new browser window or tab opens and displays the report.

Publishing a report

To make the generated reports accessible to other associates within your department or company, you can publish them. Publishing means that each execution will publish the report in a given format (CSV, HTML, or XML) and to a given place provided through a URL. This way, administrators can show reports on any server to other users, who do not have access to BMC Client Management.

To publish a report,

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select **Publish** tab in the right window pane.
4. Select **Edit > Create Export**  .
   The **Properties** dialog box appears on the screen.
5. Enter the required information in the respective boxes:

Parameter	Description
Export Format	Defines the format in which the report is to be exported and/or attached to the email to be sent. Depending on the report type (style or template based) different export formats are available.For template based reports, if the selected format is HTML, the file is exported with an .HTML.XML extension.
Protocol	Select the protocol via which the export file is to be transferred to its target location. If you select http make sure first that your http server accepts to receive files in http format. If you publish via the file protocol you do not need to fill in the following four fields, continue directly with field Path.
User Name	Enter the name of the user login to access the export file in its target location.
Password	Enter the password corresponding to the user login. For security reasons the password is displayed in the form of asterisks (*). This field is not applicable if you have chosen file as your protocol.
Host Name	Enter the name of the host machine on which the file is to be stored. You may enter the name either as its short or complete network name, for example, scotty or scotty.enterprise.com, or as its IP address in dotted notation, for example, 194.45.245.5 or 2001:db8:85a3::8a2e:370:7334. This field is not applicable if you have chosen file as your protocol.FTP: For the ftp protocol the host name is to be entered without the ftp:// prefix. for example, ftp.enterprise.com.HTTP: For the http protocol the host name is to be entered without the http:// prefix. for example, scotty.enterprise.com. You may enter the name either as its short or complete network name, for example, scotty or scotty.enterprise.com, or as its IP address in dotted notation, for example, 194.45.245.5 or 2001:db8:85a3::8a2e:370:7334.
Port	Enter the port number of the target host through which the export file is to be transferred. This field is not applicable if you have chosen file as your protocol.SMB: If no port is entered, the default smb port is used, even if 0 is displayed in the window in this case.
Path	Enter the complete directory path of the export file on the target machine. Do not add a name for the file. The file name is by default the name of the report with the extension corresponding to the chosen file type. SMB: For the smb protocol the path must be the real, complete path on the target device. Only the destination directory (without file name) must be listed here, for example, C:Temp for Windows. For Linux the full path is not required, only the share name needs to be given, for example, if your path is /home /user/ and the name of your share is myshare only myshare needs to be entered into this field.FTP: For the ftp protocol the path must be entered after the home directory of the connected user. If only a dot with

Parameter	Description
	backslash (.) is entered, this indicates the home directory.HTTP: For the http protocol the path must be entered from after the home directory of the connected user. If only a backslash () is entered, this indicates the home directory. For example, if FPAC is entered here in connection with the host name example above the example connects to the URLhttp://scotty.enterprise.com/FPAC.

6. Click **OK** to confirm.
   The export for the desired report was set up. On generation it is exported in the specified format and published to the specified path.

Setting up email for mailing reports

Reports once generated can also be sent to a number of specific recipients in addition to being published and thus made accessible. From the **Mail** tab of each report's node, you can define the format and e-mails which are to be sent once a report is generated. Before you can send a mail to an administrator or an administrator group, you must ensure that the following settings are defined:

- Email is set up for the BMC Client Management. For more information, see Managing email settings.
- Email is specified for each recipient of the email.

As reports can be assigned to several groups, every recipient receives one mail per group, whereby each will refer to the respective group in the subject and the attachment by the following structure:

- Subject: `<subject text> <group name>`
- Attachment: `<report name>.<group name>.<file extention>`

For Example:

Subject: Have a look at this! All Devices with Agent

Attachment: Hardware Summary List.All Devices with Agent.html

To set up the email for mailing reports

1. Select **Reports** in the left window pane.
2. Select the desired report in the left window pane.
3. Select the **Mail** tab in the right window pane.
4. Select **Edit > Add email** 
   The **Define Mail** dialog box appears on the screen.
5. Click **To** , **CC** , **BCC** to add recipients.
   The **Select an Address** dialog box appears on the screen.
6. Select one of the following radio buttons:

a. **Select from List** to select an administrator or an administrator group.
   If you select an administrator group as recipient, the email will be sent to all members having a valid email address specified in their respective **General** tab.
b. **Select Manually** to enter any valid email address into the following text box.
   You can enter more than one email address by using a semicolon as separator. For example: scotty@enterprise.com;kirk@entersprise.com

7. If desired, enter a subject in the **Subject** text box.
   This text box can contain up to 256 characters. If this text box is left empty, the subject of the email will only consist of the Group's name the respective report is assigned to.
8. If desired, enter a message in the following text box.
   This text box can contain up to 2000 characters.
9. Select the format of the attached report from the **Export Format** list.
10. If desired, clear the **Attach Report to Mail** check box.
    If you clear this check box, the email will only contain a link to the storing location of the respective report in the **Report Portal** of the agent interface.
11. Click **OK** to confirm the data for the email and add it to the list.
    The email has successfully been set up and is now ready for use.

Managing Report Portal

The Report Portal is a service provided by the master server, which makes reports available to everybody with required permissions. It provides a list of all generated public reports. By default, these reports are stored indefinitely.

This topic includes:

The list with the generated reports is structured as follows:

- **Name** : Displays the automatically generated name of the report or the name as defined in the **Report File Name** field in the general report definition. On the left of the name you can see the icons representing the generated format (HTML, XML and PDF). If a report is not available in any of these formats, that is, it was not requested to be generated in this format, the respective icon will be dimmed.
- **Report Title** : Displays the title of the report.
- **Create Time** : Displays the date and time at which the report was actually generated..
- **Group Name** : Displays the name of the group or rule if the report is assigned to one. If a report is assigned to more than one group or rule, a separate table entry can be found for each assigned object.

The Report Portal is accessed via a web browser by entering an address with the following structure in the address bar: http://<master name>:<port number>/report

For example: `http://scotty:1611/report`

> **Note**
>
> You can enter the name either as its short or full network name such as *scotty* or *scotty.enterprise.com* , or in the form of its IP address. Be aware that when you use IPv6 you need to put square brackets around the IP address, for example, *[2001:db8:85a3:8d3:1319:8a2e:370:7348]:1611*.

Viewing a report in Report Portal

To view a report in the desired format, proceed as follows:

- Click the icon representing the desired format on the left of the report name:
  -  for XML
  -  for HTML
  -  for PDF

The report will open in a new browser window or tab. If you selected the PDF format but no corresponding browser plug-in is installed, a pop-up menu displays on the screen, proposing you to download the PDF file of the report.

Filtering reports

The reports displayed in the Report Portal can be limited to a specific period. By default, the filter is set to display all reports of the previous year.

To change the filtering criteria,

1. Enter the earliest report date in the **Start Date** field.
   Click in the box to select a date from the appearing calendar or **Clean** to clear the calendar box.
2. Enter the latest report date in the **End Date** field.
3. Click **Filter** to proceed.

Now only the reports that were generated within the defined timeframe are shown.

Importing new report templates

Report models can be imported into CM at any time. After their templates are created and put in the proper location on the master, they can be directly imported in the console.

To import report templates, proceed as follows:

1. Put the template files (.xml) in the the following directory: `[BMC Installation Directory]/data/Vision64Database/reporttemplates`

2. Click **Tools > Import Report Templates** .
   The **Schedule Report Template Import** window appears.
3. Specify in this window if you want to import the template immediately or if you want to set a date and time for the import.
4. Click **OK** to proceed.

The import of new report templates is launched at the specified moment.

Report creation wizard

The definition and generation of the different reports in the network can be done manually by creating the report and then defining all options, or they can be created via the **Report Creation Wizard** .

The **Report Creation Wizard** is the base wizard for all types of reports, style-based and template-based to be created. It can be called from anywhere under the main **Reports** node, and from the **Wizards** menu or the **Dashboard**.

This topic includes:

Defining the report

The first step defines the report base information such as its name, type, style and language.

1. Enter the required information into the respective boxes and make the desired selections.

   > By moving the cursor over a field, a balloon tip displays, explaining the purpose of the respective field.

2. Click **Next** to proceed to the following step of this wizard.

Defining the subreports

This optional step is concerned with the configuration of the subreports and thus not available for template based reports. It provides one tab for each subreport of the report.

1. Define the required parameters in the respective boxes.

2. Click the next **Subreport** tab and define its contents as explained, until all available subreports are defined.
3. Click **Next** to proceed to the following step of this wizard.

Defining the options

This optional wizard step is applicable only to some Patch, Power and Application Management reports. It allows you to activate and specify the predefined report generation parameters. The table only displays the defined parameters not all available parameters.

1. Select the parameter to be modified from the list.
2. Click  .

> Alternatively you can double-click the parameter.

The **Report Options** window appears providing access to the parameters.
3. Edit the parameters as required and then click **OK** .
4. Click **Next** to proceed to the following step of this wizard.

Defining report publishing and mailing

In this wizard step you can set up the publication parameters of the report, that is, its format (CSV, HTML or XML), as well as storage location and email recipients and contents.

1. Enter a file name for the report in the respective text box.
2. Check the **Public Report** box if you want the report to be accessible by non-CM users.
3. Set up the required exports and emails as described.
4. Click **Next** to proceed to the following step of this wizard.

Assigning objects to the report

In this step of the wizard the objects on which the report is to be generated are to be defined. The report target population is either defined by the query selected for the subreport(s) or by one or more target groups, which are assigned in this window. The report target population can also be defined by both, a query and one or more target groups.

1. Assign the desired object to report as explained.
2. Click **Next** to proceed to the following step of this wizard.

Scheduling the report generation

In this last wizard step the schedule for generation is to be set up.

1. Define the date for the actual execution via the **execution** field in the **Validity** tab.
2. If the scan is run on a regular schedule, you need to specify when it is to be executed for the last time in the **Termination** field.

3. Click the **Frequency** tab.
4. Define the actual execution schedule of the scan, that is, at which frequency it is to be executed.

   Depending on your choices other boxes might become available in this tab.

5. Click **Finish** to confirm all the data for the new report.
   A **Confirmation** dialog box appears, giving you the possibility to directly jump to the new report in the console.

The report generation and its schedule are now active.

Example: Creating, generating, and viewing a style-based report

Style-based reports are based on a layout type that defines the number of subreports the report contains and how these subreports are ordered on the displayed or printed page. 12 different layout styles are available. Style-based reports can base their generated data on the results of a query, on the members of a device group, or both.

This example creates a report displaying some hardware inventory data based on query results in the form of a table that will be available on the **MyApps** and it is scheduled to be generated on the first of each month.

1. Select the **Reports** node in the left tree hierarchy.
2. Click **Wizards > Report Creation** to launch the **Report Creation Wizard** .
3. Enter **Hardware Summary** into the **Name** and **Report Title** boxes.
4. Click **Next** .
5. Enter **Hardware Summary List** into the **Subreport Title** box.
6. Select a query in the **Query Name** box, for example, *All Devices* .
7. Click **Add Column** .
8. Once all columns are added click the **Subreport Preview** button below the table.
   A browser window opens on your screen and displays how this subreport will roughly look like.
9. Click **Next** to continue.
10. Select the value **Name** in the **Available Columns** box.
11. Select the value **Ascending** in the **Sort Order** drop-down list.
12. Click **Add** to move the attribute to the list of **Selected Columns** .
13. Now select the value **IP Address** , reselect the value **None** in the **Sort Order** drop-down list and click **Add** .
14. Select the value **MAC Address** and click **Add** .
15. Finally select the value **Operating System** and click **Add** .
16. Click **OK** to close this window.
17. Check the box **Public Report** .

18. Click **Next** .
19. Click **Next** without assigning any device group.
20. Select the **Immediately** radio button in the **Execution Date** panel.
21. Select the **Run Forever** radio button in the **Termination** panel.
22. Go to the **Frequency** tab.
23. In the **By Schedule** panel select the **Day of the Month** radio button.
24. Select from the following list the value 1st day of the month.
25. Go to the **Frequency** panel to the right and select the value **Once daily** in the **Period** box.
26. In the following box, **at** , enter the time at which it is to be generated, for example, at 5 in the morning.
27. Click **Finish** at the bottom of the window.
28. Click **Yes** in the **Confirmation** window.
29. Click **View Last Result** .
30. Click **Yes** in the appearing pop-up window.

A new browser window or tab opens and displays the report.

Example: Creating, generating, and viewing a template-based report

Template-based reports, as the name already indicates, are templates which can be used to create your own reports according to a specific model or template, and they are provided in XML, HTML and PDF format. This report type is only available for **Patch Management** , **Power Management** , **Application Management** , **Compliance Rules** and the **Configuration Summary** and must always be assigned to at least one of the objects of its type.

This example creates a report showing the basic information and possibly basic inventories of all devices that are part of a group. It is to be executed regularly every first of the month:

1. Click **Wizards > Report Creation** to launch the **Report Creation Wizard** .
2. Enter **Configuration Summary** into the **Name** and **Report Title** boxes. The **Template-based** option in the **Report Type** list is already preselected for this guided task.
3. Select from the **Report Template** box the template **Configuration Summary** .
4. Click **Next** .
5. To display the **Security Settings Inventory** in addition to the basic device information click **Properties** above the table.
6. Check the **Security Settings Inventory** box in the appearing **Report Options** window.
7. Click **OK** .
8. Click **Next** .
9. Click **Next** without making any modifications.
10. Click **Assign Device Group** .
11. Select the desired group from the pop-up window, e.g., *All Devices* .
12. Click **OK** to confirm and close the window.
13. Click **Next** to continue.
14. Check the **Immediately** radio button in the **Execution Date** panel.
15. Check the **Run Forever** radio button in the **Termination** panel.

16. Go to the **Frequency** tab.
17. In the **By Schedule** panel select the **Day of the Month** radio button.
18. And select from the following list the value 1st day of the month.
19. Go to the panel to the right and select the value **Once daily** in the **Period** field.
20. In the following field, **at** , enter the time at which it is to be generated, that is, at 5 in the morning.
21. Click **Finish** at the bottom of the window to confirm the new report and immediately generate it.
22. Click **View Last Result** .
23. Click **Yes** in the appearing pop-up window.

A new browser window or tab opens and displays the report.

Managing events and alerts

An event is any significant action or occurrence in the system or in an application detected by a program that requires users to be notified. Managing the events that occur on a client is a key requirement to minimizing downtime of these computers. Event logging starts automatically each time the managed device is started. It permits to visualize the general state of a managed device, the pending alarms and any information regarding the agent installed on this client and the possibility to respond to these events.

In addition to the events BMC Client Management has added the notion of alerts, which are events that the administrator needs to be made aware of immediately. Alerts are a specific type of events, that is, events for which a notification is sent to one or more administrators. The alert displays in the status bar in the form a yellow triangle ⚠ no matter which node the administrator is currently displaying and the number of new alerts are also displayed on the dashboard.

This section includes:

- Event log model list
- Configuring alert notification

The events logged for the activated event log models can be monitored under the main **Alerts and Events** node and under a node of the same name under an individual device or device group. To be displayed in the event logs of a device, the events logged locally by the BMC Client Management agent must be uploaded to the master database. For some modules, this is done automatically, such as for software installations or the different managed applications. For others, such as the logged events for resource monitoring, they must be uploaded via operational rules. The respective rules are explained in the operational rule steps reference.

The **Alerts and Events** node provides the following selection options which can be combined for the display. When opened, the table of this node is empty. Click **Find** to view alerts and events.

Parameter	Description
Model Name	Select from this list the type of event log model for which to display the logged events. Depending in this selection the data displayed in the view will vary.
Status	Select in this box the status value for which the logged events are to be displayed.
Start Date	Select in this box the date from which on the logged events are to be displayed.
End Date	Select in this box the date up to which the logged events are to be displayed.

For more information, see Event log model list.

Filtering alerts and events

1. Select the desired event log model from the **Model Name** drop-down box.
   To filter for a specific status of the current model, do not modify this selection.
2. Select the following criteria to further filter the alerts and events of the selected model:
   - Select a specific status value from the **Status** drop-down box to display only alerts /events of a specific status type.
   - To filter for events of a specific timeframe select the start and end date of the desired timeframe in the calendar boxes.
     You can use only one criteria for filtering or you can use a combination of them.
3. Click **Find** .

The table will refresh and display only those alerts/events that comply with the selected criteria.

Acknowledging alerts

After you access the **Alerts and Events** node, the alert icon in the status bar disappears. However, the status of the alerts themselves has not yet changed.

To acknowledge specific alerts,

1. Mark the alerts to be acknowledged in the table in the right window pane.
2. Select **Edit > Acknowledge Alerts** .
   A confirmation window displays.
3. Select **Yes** to confirm and proceed with the action.

The status of the selected alerts will now be changed from `Unnotified Alerts` to `Acknowledged Alerts`.

Purging alerts and events

Alerts and events can be purged. Be careful when using this operation. All alerts and events of this event log model for the current device/device group will be irrevocably deleted from the database.

1. Click **Purge** .
   A confirmation window appears.
2. Click **Yes** to confirm.
   Another confirmation window appears if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce or BMC FootPrints Service Core .
3. If the incident tickets that were created in BMC Remedyforce should be closed at the same time, click **Yes;** otherwise click **No** .

All alerts and events will be deleted from the database and, if requested, the status of the connected incident ticket(s) in BMC Remedyforce or BMC FootPrints Service Core will be changed to `Closed`.

Deleting individual alerts and events

It is possible to delete individual alerts and events that are no longer required.

1. Select the alert(s)/event(s) to delete in the table to the right.
2. Click **Edit > Delete** .
   A confirmation window appears.
3. Click **Yes** to confirm.
   Another confirmation window appears if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce .
4. If the incident tickets that were created in BMC Remedyforce should be closed at the same time click **Yes** , otherwise click **No** .

All selected alerts and events will be deleted from the database and, if requested, the status of the connected incident ticket(s) in BMC Remedyforce will be changed to `Closed` .

Event log model list

The **List** node displays the list of event log models which are currently defined and are located on the local client. It does not include any models which are in any status of waiting to be assigned to the client.

Parameter	Description
Model Name	The fields of this column list the names of all event models which currently exist in CM . This can either be the name of the model for any predefined models such as the Web History Monitor, or the name of a custom defined model such as a performance counter plus its checksum, for example, Memory_12458942348662. The predefined models are explained in detail in the Available event log models topic.
Category	Provides the category to which the respective model belongs which can be a value such as Resource Monitor or Software Distribution.
Model Note	These fields provide a short description on what the respective model logs.
Activation	The values in these fields define if the respective model is activated, that is, if it stores the generated events. Possible values are **Yes** for events that are stored on local level and then can be uploaded to the master database, and **No** , the model is not activated and events will be deleted right after being generated.

Available event log models

The table displays different information depending on the selected event log model. Depending on the currently selected object type, some or all of these models might be available:

- Alert & Event
- Monitored Applications
- Prohibited Application
- Protected Application
- Software Installations
- Power Management
- Windows Devices

Alert & Event

The **Alert & Event** model logs agent operation events, such as events and alerts generated by operational rules, by the inventory module, security alerts, and so on. It shows the following information for each event:

Parameter	Description
Event Date	The date and time the alert occurred in the default time format.
Device Name	This column is not displayed under the **Alerts and Events** of a device.
Status	Displays the current status of the event. • **Acknowledged Alert** : The administrator received the alert notification and has already acknowledged it. • **Unacknowledged Alert** : The administrator received the alert notification but has not yet acknowledged it. • **Notified Alert** : The alert notification was sent but the alert has not yet been acknowledged. • **Unnotified Alert** : An alert occurred but its notification has not yet been sent. • **Closed** : The problem that caused the alert was resolved and the alert is now closed.
Severity	Defines the severity of the selected alert, **Error, Information** or **Warning** .
Category	Defines the type of event that is being logged.
Sub-category	The alert sub-category to which the alert/event was assigned. This value can be freely defined by the administrator.
Description	Displays the textual description of the alert/event.
Shared	Indicates if this alert is shared with other applications such as BMC Remedyforce or BMC FootPrints Service Core via the external integration. It only appears after the ticket was actually created in the target integration.
Acknowledged by	The name of the administrator who acknowledged the event.
Last Modified By	Displays the name of either the last person that last modified the object or its contents, such as the administrator, or it may be the system that last executed any modifications.
Notes	This free text field can contain additional information concerning the selected object.

Monitored Applications

Logs an event for each application that is monitored.

Parameter	Description
Event Date	The date and time at which the event about the monitored application was logged by the local agent.
Application Name	The name of the monitored application.
Application Version	The version number of the monitored application.
Start Time	The date and time at which the application was started on the local client.
End Time	The date and time at which it was closed again.
Duration (sec)	The time the application was running on the local device in seconds.
Connected User Name	This field displays the name of the user that was connected at the time when the application was launched.
Domain	The name of the domain of the connected user. If the network does not have domains the device name will be displayed here.

Prohibited Application

Logs an event for each prohibited application which was found in the network.

Parameter	Description
Event Date	The date and time at which the event about the prohibited application was logged by the local agent.
Application Name	The name of the prohibited application.
Application Version	The version number of the prohibited application.
Detection Time	The date and time at which the application was found to have started and was stopped on the local client.
Connected User Name	This field displays the name of the user that was connected at the time when the application was launched.
Domain	The name of the domain of the connected user. If the network does not have domains, the device name will be displayed here.

Protected Application

Logs an event for each protected application which was repaired in the network.

Parameter	Description
Event Date	The date and time at which the event about the protected application was logged by the local agent.
Application Name	The name of the protected application.
Application Version	The version number of the protected application.
Fixing Time	The date and time at which the application was repaired on the local client.
Fixed File	The name of the file that was repaired.
Connected User Name	This field displays the name of the user that was connected at the time when the application was repaired.

Parameter	Description
Domain	The name of the domain of the connected user. If the network does not have domains, the device name will be displayed here.

Software Installations

Logs an event for all successfully executed software distributions:

Parameter	Description
Event Date	The date and time at which the event about the successfully installed software was logged by the local agent.
Operational Rule Name	The name of the operational rule that was distributed and installed on the target devices and its status.
Package Type	The type of package, that is, if it is a custom, MSI, RPM or snapshot package.
Compressed Package Size (MB)	The size of the package.
Status	The final installation status of the package.

Power Management

Logs an event for each energy state change of a device:

Parameter	Description
Event Date	The date and time at which the event about the energy state change was logged by the local agent.
Type	This column displays the type of power event, for example, *Sleep* , if the monitor turned into sleep mode, *Login* , if login information were entered to unlock the screen saver, and so on.

Windows Devices

Logs an event for each disabled Windows device:

Parameter	Description
Event Date	The date and time at which the event about the printer monitor was logged by the local agent.
Operation	This column shows the type of operation that was executed on the connected device,that is, **Authorized** if the device was allowed to connect or **Forbidden** otherwise. Each operation for the same key is only listed once and will be updated if a status change occurs, that is, if a forbidden USB key tries to connect several times, only the first connection trial will be logged as the event. If this key is then allowed to connect and tries again, this time successfully, the logged event is updated.
Class Type	This field defines for which type of peripheral device the step is to be defined, for example, USB HUB, USB Scanners, USB Storage Devices, and so on.
Description	This field contains the name of the concerned peripheral device.
Connected User Name	This field displays the name of the user that was connected at the time when the event occurred.
Domain	

Parameter	Description
	The name of the domain of the connected user. If the network does not have domains, the device name will be displayed here.

Configuring alert notification

Alert notification is configured in the **Alert Management** section of the **Preferences** window. Before you can define the alert management, however, you need to define the **Email** settings in the **System Variables** and the email address in your administrator settings.

This topic includes:

- Configuring email address
- Configuring email settings
- Configuring Alert Management user preferences

Configuring email address

To be able to access and define these settings, your account must be enabled with the **Account Enabled** parameter.

1. Select **Options> My User Account** .
   A **Properties** dialog box appears on the screen.
2. Find the **Email** box and enter your e-mail address.
3. Click **OK** to confirm and close the window.

Configuring email settings

In the **Mail** tab of the **System Variables** page, you define the default settings for the e-mail system throughout your network.

1. Select any line in the table in the right window pane of the respective topic.
2. Select **Edit > Properties** .
   The **Assign an Administrator** dialog box appears on the screen.
3. Make the appropriate modifications to the individual values.
4. Click **OK** to confirm the modifications and close the window.

The new settings will be taken into account immediately.

Configuring Alert Management user preferences

As a prerequisite for these options, you must have an email address configured in your administrator account and the email settings in the **System Variables** must be specified.

1. Select the **Preferences** button in the upper right-hand corner.
   The **Preferences** dialog box appears on the screen.
2. Select the **Alert Management** tab.

3. Check the **Send multiple alerts in one email** box, if you prefer to receive collected alerts in one email instead of receiving one email per alert.
   If this is the case, you must then define the timeframe during which the alerts are collected before being sent.
4. Enter the desired value into the **Minute(s)** box.
   This text box defines the frequency at which alert notifications are sent. To deactivate this option enter 0. If this option is activate with e.g., 60 minutes, then the administrator will receive an e-mail every hour, if within that hour new alerts arrived. This e-mail will contain the list of the alerts generated during the last hour and their basic information, such as the device on which it occurred, the severity, the category, and so on.
5. To define for which events you want to receive alerts click the arrow icon next to the event category under the **Notify me when the following alerts occur** panel.
   This will expand the respective section and display all its available events.
6. Check the boxes of the events for which alerts are to be generated and sent. You can select as many events as you want.
7. Click **OK** to confirm and close the window.

Managing update configurations

In this view you can configure the general behavior of the **Update Manager** via its tabs. The **Update Manager** tab of the **Global Settings** > **Update Configuration** page allows you to configure the automatic update of the BMC Client Management modules **Security Products**, **Virtualization,** and **Software Catalog** according to your requirements. Any device with an Internet connection in your infrastructure can be **Update Manager** . By default the master is preselected as such.

This topic includes:

Understanding update status

The **Status** tab displays the current update status of the modules that can be updated by the Update Manager together with the different operating systems on which these modules can exist. It provides the following information:

Parameter	Description
Component	The fields of this column list all components of which the automatic update can be manage by the Update Manager.

Parameter	Description
System	This column displays the operating system for which the respective component is applicable.
Version	This field displays the currently installed version of the respective component.
Status	This field displays the current status of the component, that is, if the component is of the latest available version (Up to Date) or if it needs to be updated (Out of Date). Any type of failed status, such as Download Failed, License expired will be displayed via a red flag. During the update process this field will also display the different stages of the process until all components are up to date.
Available Version	After a check was executed and updates are available for individual components this field will indicate their version number.
Last Update Time	This column displays the date and time at which the component was last updated.

Updating parameter configuration

This view allows you to individually configure the **Update Manager** via the following parameters:

Parameter	Description
Activate Verification for Available Updates	Check this box to activate the automatic verification and application process for available updates. In this case the agent verifies if updates are available, if yes, downloads them and applies them to all concernded devices.
Schedule the Verification for Available Updates	Click the icon to the right to define the schedule via the **Scheduler** window at which the agent is to verify for available updates. If no components are selected below, the agent only verifies for updates without downloading them.
Automatic Download of Security Products and Virtualization v4	Automatic download of OESIS framework v4 updates.
Software Catalog Automatic Download	Check this box to activate the automatic verification and application process for available updates of the software catalog. In this case the agent verifies if updates are available, if yes, downloads them and applies them to all concernded devices.

Updating proxy options

If an **Update Manager** device has a proxy installed, this tab allows you to define its security parameters to access the outside. Be aware that if you are using the device as a patch manager or scanner as well as **Update Manager** , the proxy will also be the same. If the proxy was already defined for the any other functionality and you modify options here, these then also apply to the other functionalities. If you have a proxy that requires specific authorizations, you need to add the following address to the white list:

- http://vmupdater.numarasoftware.com

Changing update manager

If you need to define another device as the Update Manager, proceed as follows:

1. On the **Status** tab, click **Change Update Manager**.
   The **Change Update Manager** window displays.
2. Select the new update manager from the available lists.
3. Click **OK**.
   The selected device is now the new update manager. The focus of the console moves to the update manager view of the device. There you can ensure that it is up to date by checking for later versions and if required updating the components.

Checking for available updates

To verify if updates are available for one or more of the components,

- Click **Check for Update**.
  A verification is launched via the Internet to check for available updates.
  - If none are found only the **Last Verification** date box above the table is updated with the date and time of this operation.
  - If one or more updates are available this information is presented as follows:
    - The icon color of the **Last Verification** box changes to either yellow (update available for at least one component) or red (updates available for all components).
    - The value of the **Status** box of the respective component changes to Out of Date.
    - The color of the **Status** icon changes to yellow or red.

Updating components

After a verification indicated that updates are available for at least one component,

Click the arrow next to **Update all Components** and select the components to update. You can have the following options:

- **Update All Components** to update all components for which an updated version is available.
- **Update Security Products and Virtualization V4** to update only the security products and the virtualization modules.
- **Update Software Catalog** to only update the software catalog.

The update process is launched.

- The available updates for the selected components are downloaded.
- The value of the **Available Version** changes to the version number of the version that was just downloaded.
- The installation process of the components is started.

After the update process is finished, the value of the **Version** box changes to that of the **Available Version**, the status will change to `Up to Date`, the icon turns green again and the Last Update Time changes to the current date and time value. Any type of failed status, such as Download Failed, License expired will be displayed via a red flag. During the update process this box will also display the different stages of the process until all components are up to date.

Viewing local update manager status

To locally verify the status of the Update Manager,

1. Go to the **Device Topology** > **Your Update Manager** > **Agent Configuration** > **Module Configuration** > **Update Management** node.
2. Select the **Update Status** tab.
   This view displays the following information about the current status of the Update Manager:
   - Component
   - Version
   - Status
   - Available Version

Configuring asset discovery

Configuring asset discovery includes:

- Managing scan configurations
- Adding existing devices as targets
- Configuring target lists
- Managing asset discovery scanners

To summarize, the configuration of the **Asset Discovery** functionality of is done in the following different steps:

1. The Scanner must be defined. You can skip this step, if you are using the master as your Scanner as it is predefined as such.
2. Each scanner has a specific configuration, which is to be defined under the scanner's node.
3. The **Asset Discovery** module disposes of a number of parameters defining its general behavior which can be adapted to comply with company policies. It must be configured individually either directly in the **Agent Configuration** node of the respective device or via the respective operational rule for all members of a device group. You can also configure it directly through the respective configuration file (`RemoteInventory.ini`) in the `InstallDir/config directory` .
4. The configuration of the asset discovery objects, such as the scan configurations and target lists are defined directly under the **Asset Discovery > Configuration** node.

Managing scan configurations

The scan configurations define the actual scanning parameters. Depending on your network features, these might vary considerably and you can select the most suitable to scan for your environment or system. Scan configuration folders are created as organizational containers for the different scan configurations. They can contain any number of scan configurations for the execution of asset discovery scans of your system.

Creating a scan configuration

To create a new scan configuration, proceed as follows:

1. Select **Edit> Create Scan Configuration** .
   The **Properties** dialog box opens on the screen.
2. Define the basic settings of the new scan configuration.
3. Click **OK** to add it and close the window.

Managing active protocols

Asset discovery supports the following protocols:

- Windows: Server Message Block - (SMB)
- Linux/Unix: Secure Socket Shell (SSH)
- Network devices: Simple Netowrk Management Protocol (SNMP)
- VMwave Vsphere
- Hyper-V

The **Active Protocols** tab allows you to configure the parameters for the protocols used by the scan. It allows you to define the following settings:

Parameter	Description
Name	The fields in this column display the list of protocols available for scanning.
Activated	The symbol in these fields indicate if the respective protocol is defined for scanning or not.
Description	This field displays the long name of the protocol abbreviation.
User Account	These fields display if user authentication is not required for the scanning of this protocol and the number of user accounts/communities entered as authentication for the respective protocol.

If a Linux device is configured as a scanner, it cannot discover, test or probe windows devices that run Hyper-V. Only a Windows scanner can discover devices running Hyper-V.

Adding existing devices as targets

You can add target device by selecting them from the list of existing devices. To do so, proceed as follows:

1. Click **Add existing devices to the target list** .
   The **Select a Device** window opens on the screen.
2. Select the devices to be added from one of the lists.

> The list of groups and devices provided in this window includes groups and members of synchronized directory servers.

3. Click **OK** to confirm the addition and close the window.

Configuring target lists

Targets are all devices for which an asset discovery is to be executed by the scanner. As the BMC Client Management - Inventory can scan not only devices which have a CM agent installed but also those without, using device groups for target scanning would have been incomplete and the concept of targets or target lists was used instead.

Target list folders are created as organizational containers for the different target lists. They can contain any number of target lists for the execution of asset discovery scans of your system.

This section includes:

- Creating a target list
- Populating targets
- Viewing schedule details

Creating a target list

1. Select **Edit > Create Target List** .
   The **Properties** pop-up menu appears.
2. Enter a name for the target list into the name field.
3. Click **OK** to confirm and close the window.

The new target list will automatically be created and displayed in the right window pane.

Populating targets

After a target list is created, you need to populate targets in the target list. The following are different ways to populate targets:

- Adding targets from lists
- Adding existing device groups as targets
- Adding targets via an address range

Viewing schedule details

You can view detailed information about the schedule of each of the assigned scans from the Schedule Detail :

Parameter	Description
Name	This column displays the list of names of all scans created for the currently selected scanner.
Status	The fields of this column display the status of the each scan.
Last Status Update Time	This time value indicates at which date and time the status previously displayed was updated by the target's agent for the last time.
Activation	This field shows the condition on which the scan will start executing on the targets.
Schedule	The fields of this column display the frequency with which the scan will be executed on the assigned device.
Termination	This field displays when the scan execution is scheduled to be terminated, that is, when the scan is to be run for the definitely last time of the current scheduling cycle.
Time of Assignment	This field displays the date and time at which the assignment between the objects was created in the database.

Adding targets from lists

1. Click **Add new members to the target list from lists**
   The **Select Devices from the List** window appears providing you with different methods to select the targets.
2. To add a device from the list of all autodiscovered devices known to the database proceed as follows:
   The AutoDiscovery module provides a list of all devices of any type found in the network, such as printers or devices with and without the agent installed. However, the list displayed in this case will only show all clients of type *device* and only those with a status of `Verified` or `Learned` , which means that all devices in this list were verified for existence either by the local client or a neighbor client and exist on the network.
   a. Click **AutoDisc Object** in the left menu bar.
      The **Available Devices** window appars and displays the list of all available devices. You will find more information about the list of autodiscovered devices in the main manual.
   b. Select the device/devices to be added as targets from the list.
   c. Click **Add** to move the selected devices to the list of **Selected Devices** .
   d. Click **OK** to confirm the selections and close the window.

3. To add a device from a list of autodiscovered devices by one specific network device proceed as follows:
   The tab **AutoDisc Device** allows you to select your target devices from a list of autodiscovered devices by one specific network device.
   a. Click **AutoDisc Object** in the left menu bar.
      The **Select a Device** window appears and displays the list of all devices with autodiscovery results.
   b. Select the device of which the autodiscovered list is to be used from one of the tabs of the **Select a Device** dialog box.
   c. Click **OK** to confirm the selection and close the window.
      The **Select Devices from the List** dialog box now only displays the devices that were discovered by the selected network device.
   d. Select the device/devices to be added as targets from this list.
   e. Click **Add** to move the selected devices to the list of **Selected Devices** .
   f. Click the **OK** to confirm the selections and close the window.
4. To add a device from the list of your Microsoft network neighborhood proceed as follows:
   a. Click **Network** in the left menu bar.
      The **Microsoft Windows Network Neighborhood** window appears and displays the network structure.
   b. Browse down into the hierarchy and select the devices to add to the target list.
   c. Click the **OK** to confirm the selections and close the window.
5. To add a device from an existing .csv file proceed as follows:
   a. Click **CSV List** in the left menu bar.
      The **Open** window appears.
   b. Navigate to the desired .csv file that contains the device list, select it and click **Open** at the bottom of the window.
      The **Available Devices** displays and displays the list of all devices contained in the selected CSV list.
   c. *(Optional)* Check the **Header** box, if your CSV file has a title line which is to be removed.
   d. Select the devices to be added to the targets from the list in the window.
      You can also select all devices in the list by using **Select All**.
   e. Click the **OK** to confirm the selections and close the window.
6. Click **OK** to confirm the additions and close the window.

Adding existing device groups as targets

You can add target device groups by selecting them from the list of existing groups. To do so, proceed as follows:

1. Click **Add existing device groups to the target list** .
   The **Select a Device Group** window opens on the screen.

2. Select the device groups to be added from one of the lists.
   The list of groups provided in this window includes groups and members of synchronized directory servers.
3. Click **OK** to confirm the addition and close the window.

Adding targets via an address range

You can also add one or more devices by typing their name or address.

> **Note**
>
> When you specify an address range with IPv6 addresses be careful to not add complete subnets, as these are very large and take very long to complete.

1. Click **Add Existing Device** .
   The **Add a Device** dialog box appears on the screen.
2. Enter the name of the device to be added to the list into the respective field. The name can be entered
   - Either as its short or long network name, for example, `scotty` or `scotty.enterprise.com` or as its IP address, IPv4 or IPv6, for example, `159.124.5.10` or `2001:0db8:85a3:0000:0000:8a2e:0370:7334` ,
   - Or as a comma separated list of names or ranges, for example, `scotty; 192.168.4.45-192.168.4.47; 2001:0db8:85a3:0000:0000:8a2e:0370:7334` which includes computers `scotty.enterprise.com` , `192.168.4.45, 192.168.4.46` , `192.168.4.47` and `2001:0db8:85a3:0000:0000:8a2e:0370:7334` .
   - A range can also be entered as CIDR notation in the form of `192.9.205.22/18` or `2001:0db8:85a3:0000:0000:8a2e:0370:218/733` .
3. Click **OK** to add the device and close the window.

Managing asset discovery scanners

Any device in your network can be an *Asset Discovery Scanner.* It only must be declared as such and have the required asset discovery module loaded. A scanner executes scans on individual devices or groups of devices, called targets or target lists. It accesses the targets via different protocols to retrieve all available asset information.

> **Note**
>
> **Limitations:** Scanners running on a Linux operating system cannot scan the hardware inventory of devices running on any type of Windows operating system.

This section includes:

- Defining a scanner
- Configuring asset discovery scanner

This view provides the following information about the defined scanners:

Parameter	Description
Name	The name of the scanner.
IP Address	The IP address of the scanner.
Operating System	The operating system running on the scanner.

After a scanner is declared and configured as such, it will appear in the list of **Scanners** under the **Asset Discovery** node. For each of the scanners listed you can then create the asset scans it is to execute.Do not forget to configure them as explained in paragraph Configure Asset Discovery Scanner of this manual.

Defining a scanner

A scanner is a device of your network that is capable of scanning other devices for their assets. Contrary to the scanned devices the scanner must have a CM agent installed and have the asset discovery module loaded. Any device with a Windows 2003, Windows XP, Windows Vista Business and Ultimate, 64 Bit Windows or Linux Red Hat 9, AS/ES 3 and 4 and SUSE operating system can be defined as a scanner.

A device may be configured as a scanner in the following different locations:

- Designating a device as a scanner
- Add a device as a scanner

Designating a device as a scanner

Any device can be defined as a Scanner either via the Device Topology or the device group node of which the device is a member.

1. Select the **Device Topology** or the **Device Groups** node, of which the desired device is a member in the left window pane.
2. Select the device to become a Scanner.
3. Select **Edit > Properties** .
   The **Properties** pop-up menu appears.
4. Go down to the lower part of the window and check the box next to the **Asset Discovery Scanner** option. For devices which do not have the required operating system, this option is not accessible.
5. Click **OK** to confirm and close the window.

The device will be added to the table of Scanners and it will appear in the list of Scanners under the main **Asset Discovery** node.

Add a device as a scanner

You can directly add a device as a Scanner under the **Scanners** node. Any device that fulfills the predefined requirements can be a scanner in BMC Client Management - Inventory. The master is a scanner by default.

To define a device as a scanner,

1. Select the **Asset Discovery** node and then go to the **Scanners** node in the left window pane.
2. Click **Edit > Add Device** .
   The **Add a Scanner** pop-up menu displays displaying the list of all devices, that can be a scanner because of their operating system.
3. Select the device to be added from one of the list boxes.
4. Click **OK** to confirm and close the window.

The device will be added to the table of Scanners and its configuration parameter will be updated.

Configuring asset discovery scanner

After a scanner is declared and set up as such, it will appear in the list of **Scanners** under the **Asset Discovery** node. For each of the scanners listed, you can then create the scans it is to execute or run autodiscoveries. Before launching any scans, make sure via the **Update** node that your scanner is up to date on all its components.

Configuring the asset discovery scanner includes:

- Configuring Asset Discovery module parameters
- Configuring assigned scans

Configuring Asset Discovery module parameters

The configuration of the **Asset Discovery** module is done via the **Asset Discovery** subnode of the **Agent Configuration > Module Configuration** node, or directly under the defined Scanner's **Module Configuration** node under the main **Asset Discovery** node. It provides the possibility to modify the configuration parameters for the module and adapt its behavior to company policies and requirements. The Module Configuration node has the following tabs:

- Parameters
- Device List
- Credentials

This topic includes:

- Configuring module parameters
- Viewing credentials

For information about Device List tab, see Viewing result of the last scan.

Configuring module parameters

The **General** tab displays the list of parameters that must be defined for the **Asset Discovery** module and its general behavior.

1. In the **General** tab, select any line in the table in the right window pane.
2. Click **Edit> Properties** .
   The **Properties** pop-up menu appears.
3. Make the appropriate modifications to the individual values.
4. Click **OK** to confirm the modifications and close the window.
   The new module settings will be taken into account immediately.

Viewing credentials

You can view the credentials defined for the remote inventory process. These values are defined and assigned via an operational rule. They cannot be added or modified in this view.

The table provides the following information:

Parameter	Description
Protocol	This field displays the protocol for which the account is defined, possible protocols are `smb`, `ssh` and `snmp` .
Login	The login name for the respective protocol. It has either one of the following formats: • `domain name/user logon` • `local host name/user logon` (If the login is for the SNMP protocol, thes field contains the name of the community.)

Configuring assigned scans

You can view detailed information about all scans that are defined and scheduled for the currently selected scanner from the **Assigned Scans** node. Scan folders are created as organisational containers for the different scans. They can contain any number of scans for execution on your system.

This topic includes:

- Creating a scan
- Viewing schedule details

Creating a scan

To create a new scan by individually defining its components, proceed as follows:

1. Go to **Asset Discovery** > **Scanners** > **(your scanner)** > **Assigned Scans**.
2. Click **Edit> Create Scan** .
   The **Properties** dialog box appears.
3. Enter the desired data into the respective boxes.

4. Click **OK** at the bottom of the window to confirm the data for the new scan or click **Cancel** to abandon without modifications and to close the window.
   The new scan will automatically be created and be displayed in the right window pane. By default, the scan is scheduled to run immediately.

Viewing schedule details

After the scan is created, you need to configure the schedule, activate it, and assign or reassign it. You can also control the scan operations. Th **Assigned Schedule** tab provides detailed information about each of the assigned scans:

Parameter	Description
Name	This column displays the list of names of all scans created for the currently selected scanner.
Status	The fields of this column display the status of the each scan.
Last Status Update Time	This time value indicates at which date and time the status previously displayed was updated by the target's agent for the last time.
Activation	This field shows the condition on which the scan will start executing on the targets.
Schedule	The fields of this column display the frequency with which the scan will be executed on the assigned device.
Termination	This field displays when the scan execution is scheduled to be terminated, that is, when the scan is to be run for the definitely last time of the current scheduling cycle.
Time of Assignment	This field displays the date and time at which the assignment between the objects was created in the database.

Configuring Windows Devices for Device Management

The first step when managing the peripherals of Windows devices it to configure the local device management module and make sure it is loaded on all Windows devices.

1. Select the **Operational Rules** top node in the left window pane.
2. Select **Edit > Create Operational Rule**  .
   The **Properties** dialog box appears on the screen.

> **Note:**
>
> If you want to create the new rule in a specific folder instead of under the operational rules top node see Option (a) now.

3. Enter *Device Management Configuration* (or any other desired name) into the **Name** box and click **OK** to confirm.
4. Select the newly created rule and go to the **Steps** tab.

5. Select **Edit > Add Step** .
   The **Select a Step** pop-up window appears.
6. Expand the item **Agent Configuration** and select step **Load/Unload Module** .
7. Click **Add** .
   The **Properties** dialog box appears on the screen.
8. From the drop-down list of the **Module Name** box select the **Windows Device Management** option.
9. Leave all other options as they are.
10. Click **OK** to confirm.
11. Now select the step **Windows Device Management Module Setup** .
12. Click **Add** .
    The **Properties** dialog box appears on the screen.
13. Check the **Log Events** box.
14. Click **OK** to confirm.
15. Click **OK** again to confirm the list of defined steps for the operational rule and to close the window.
    The rule will now be created with the defined steps.
16. Click the **Assigned Objects** , then **Assigned Device Groups** node in the left window pane under your newly created operational rule.
17. Select **Assign Device Group** .
    A confirmation window appears.
18. Click **Yes** to automatically launch the rule.
19. The **Select a Device Group** pop-up window appears.
20. Select the group *All Devices* .
    The device group will be added to the table in the right pane with the status `Activated` .

Once the status of all its members, that you can see under the subnode **All Devices** , displays as `Executed` , the devices are ready for device management.

Configuring device settings for power management

The **Power Management** module is loaded by default at installation time, now it only needs to be configured. Like most other modules, it is configured via the **Agent Configuration** of the respective device. We will do so in this example via an operational rule using the wizards for all devices of your test environment:

1. Select **Wizards > Operational Rule Creation** .
   The left pane of the wizard window appears all available steps of this wizard.
2. Enter *Power Management Configuration* (or any other desired name) into the **Name** field of the **Definition** view.

3. Leave all other parameters as they are, because neither packages will be distributed nor dependencies are required for this rule.
4. Click **Next >** to continue.
   The **Steps** window appears. Here we must define the operations necessary to configure the power management which is done all in one single step:
5. Select **Add Step** on top of the list field.
   The **Select a Step** pop-up menu will be displayed on the screen.
6. Open the **Agent Configuration** folder and select the **Power Management Module Setup** step.
7. Click **Add** to confirm.
8. The **Properties** window appears.
9. Make the following modification to the available parameters:
   - Check the **Log Events** option. This will ensure that the events generated for the power management are logged in the local database.

   > This step configures the event generation for the module, as we have just done, and the default inventory update and upload. By default it is generated and uploaded to the master database every 24 hours. If you want to define a different schedule see Option (a).

10. Click **OK** to add the step to the list and close the window.
11. Click **OK** again to confirm the list of steps for the operational rule and close the window.
12. Click **Finish** to confirm the settings of the new operational rule.
    A confirmation window appears which allows you to directly continue with the **Operational Rule Distribution Wizard**.
13. Click **Yes** to continue directly with the distribution of the new rule.
    The **Operational Rule Distribution Wizard** is displayed on the screen with its first window, **Operational Rule**. The **Name** field is inaccessible as the operational rule to distribute is already preselected, that is, the one we just created.
14. Leave all options as they are.
15. Click **Next >** to continue.

> The operational rule is now created and must be assigned to the devices on which to execute, in our example the relay.

16. Select **Assign Device** on top of the list field.
    The **Select a Device** pop-up menu appears.
17. Go to the **All** tab and select the relay.
18. Click **OK** to confirm and close the window.
    The device will be added to the list window.

19. Click **Finish** to confirm all choices and launch the assignment and configuration process. The last option provided by the wizard is to go directly to one of the objects, that is, the operational rule or the task, if one was created.
20. For our example we will directly activate the rule and change to focus to it, therefore check the **Go To Operational Rule** box and click **Yes**, to directly activate the rule.

Configuring remote access

Remote access to devices is configured in two different ways:

- First you might need to have the remote user's permission to access his or her device (system authentication).
- Secondly you might need identify yourself to remotely control the device or you might even be completely denied access to specific devices (access permissions)

This section includes following topics:

Configuring System Authentication

By default, any administrator with a valid BMC Client Management login can remotely access all devices in the network that he has access permissions to. You may, however, limit these accesses by requiring specific local access credentials to the remote devices. This can be configured via the **Security** tab of the **System Variables** node.

By activating any combination of the **Request System Credentials for Linux Remote Access**, **Request System Credentials for Mac OS Remote Access** or **Request System Credentials for Windows Remote Access** system variables you can require that administrators trying to remotely access devices of the respective operating system need to provide access credentials.

In this case a pop-up window appears when you select the **Direct Access** node or try to establish a remote control session. At the same time a window appears of the target device requesting access acknowledgment from the local user. You need to click the **OK** button to close this window and then refresh the view. If the user acknowledged your request the connection is established and you have access to the remote device. If the user did not acknowledge, the pop-up window appears again on the screen.

When you try to access the Remote Manager functionalities to a client you will be asked to provide the login and password to the remote computer to verify you have access permissions. You can provide the login as one of the following possibilities:

- as the "simple" login name of a local user of the remote computer, such as Administrator as `\\domain\logon`
- for a domain login of the administrator, such as `\\LAB\TEST`. The domain part can be set to dot (.) to indicate the local computer.

If you are not sure that your local administrator login has the same passwords for all targets, use the domain logon. For domain logons to work correctly, the necessary domain trust relationships must already were set up between the different domain controllers.

Configuring access permissions via dynamic objects

BMC Client Management remote control access permissions are assigned to the devices via the **Security Profile** of the administrator accessing the device. You can specify the access permissions either for static or for dynamic objects. As static objects the access is defined individually per device, for dynamic objects it is assigned to the result of the object, that is, to all members of a specific group or query.

For example, to provide an administrator with read access to the master but refuse remote control and direct access to it proceed as follows:

1. Go to **Global Settings** > **Administrators** and select the administrator.
2. Select the **Security Profile** node and the **Static Objects** tab.
3. Verify that in the list of static objects you have the **Device Groups** top node with at least read access defined.
    a. If this is not the case click the **Add Object** icon.
    b. Leave the **Top Nodes** value selected in the **Object Type** drop-down box.
    c. Select the **Device Groups** option and click the **Add** button to the right.
    d. In the **Properties** window make the necessary changes to the **Write Access** and **Assign Access** options, but leave the **Read Access** set to **Allow** and click **OK**. The entry is now added to the **Selected Objects** list box.
4. Now select the **Device Group/Device** value in the **Object Type** drop-down box.
5. Click the **All** icon in the left window bar.
6. Select the master from the list of all devices and device groups that is now displayed.
7. Click the Add button.
8. In the **Properties** window select the **Deny** radio buttons in the **Direct Access Acknowledgement** and **Remote Control Acknowledgement** sections.
9. Click **OK** to confirm the denial and click **OK** again to confirm the new static objects. The administrator now has full access to the master but he cannot remotely access or control it.

To prohibit remote control access to all devices but the clients proceed as follows:

1. Go to **Global Settings** > **Administrators** and select the administrator.
2. Select the **Security Profile** node and the **Static Objects** tab.
3. Verify that in the list of static objects you have the **Device Groups** top node with at least read access defined.
    a. If this is not the case click the **Add Object** icon.
    b. Leave the **Top Nodes** value selected in the **Object Type** drop-down box.
    c. Select the **Device Groups** option and click the **Add** button to the right.

   d. In the **Properties** window make the necessary changes to the **Write Access** and **Assign Access** options, but leave the **Read Access** set to **Allow** and click **OK**. The entry is now added to the **Selected Objects** list box.
   e. Click **OK** again to confirm all static objects.
4. Select the **Dynamic Objects** tab.
5. Click the **Add Query** icon.
6. Click the **All** icon in the left window bar.
7. Select the **All Devices** query from the list.
8. Click **OK**.
9. In the **Properties** window select the **Deny** radio buttons in the **Direct Access Acknowledgement** and **Remote Control Acknowledgement** sections.
10. Now select the **Client Devices** query in the **Out of the Box > BMC Client Management Architecture** folder and click **OK**.
11. In the **Properties** window select the **Not Required** radio button in the **Direct Access Acknowledgement** and **Remote Control Acknowledgement** sections.
12. Click **OK** to confirm the settings and click **OK** again to confirm the new dynamic objects. The administrator can now see all devices but only remotely control or directly access the clients, that is, all devices apart from the master and the relays.

Configuring diagnostic tool

Contrary to the majority of the other CM modules, the configuration of the **Diagnostic Tool** module is not done via the **Agent Configuration** of the device but directly under the main compliance node via its own **Configuration** node.

Under this node you can configure the following:

Parameter	Description
Diagnostic Timeout (min)	Maximum duration in minutes before considering the diagnostic as blocked.
Maximum Diagnostic Log File Count	Maximum number of diagnostic log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.

Configuring Operational Rules

In most cases the default settings allow you to start creating **Operational Rules** without having to do any configuration.

However, if required by your infrastructure, you can configure the **Operational Rule** settings to adapt it to your needs.

Related topics

- Configuring the master for operational rules
- Configuring the devices
- Modifying the default schedule for an operational rule

Configuring the master for operational rules

The Master is the device in your network responsible for storing and distributing **Operational Rules** . To modify the settings of the rules, proceed as follows:

1. Go to **Global Settings > System Variables** and click the **Operational Rules** tab.
2. Double-click any line of the table in the right window pane.
   The **Properties** dialog displays.
3. Make the necessary changes to the parameters and click **OK** .

Configuring the devices

By default all your devices have the same settings for **Operational Rules** . Since not all devices have the same requirements and specifications, it might be useful to modify certain settings.

1. Go to **Device Topology > Your Device > Agent Configuration > Module Configuration > Operational Rules** .
2. Double-click any line of the table in the right window frame.
   The **Properties** dialog displays.
3. Make the necessary changes to the parameters and click **OK** .

> To modify these settings for a group of devices create an operational rule with the modified settings and assign and execute it on all target devices.

Modifying the default schedule for an operational rule

If you don't define it otherwise, the default schedule is used for distributing **Operational Rules** . With the default schedule an **Operational Rule** is assigned and executed immediately and only once. You can modify it so that all **Operational Rules** with the default schedule are distributed according to your requirements.

1. Click the **Options > User Preferences** menu item.
   The **Preferences** dialog displays.
2. Click **Object Assignments** in the left pane.
   - To change the default schedule, click **Modify** , then define your schedule in the **Validity** and **Frequency** tabs and click **OK** .

- To change the default assignment date, in the **Assignment Date** group box select the **Deferred to** radio button and define your desired date and time in the two drop-down lists.

3. Click **OK** to confirm you changes.

You modified the default schedule. The next time an **Operational Rule** is assigned and executed with the default schedule, your new schedule is applied.

Setting up inventory

This section provides you with the necessary information for the basic and advanced configuration of the different types of inventory. It explains in detail the configuration parameters of the different types of inventory, hardware, software, custom and unconnected device inventory.

It also details how the different types of inventory can specify, limit, extend, and so on, their content via filters and object types.

The following topics are provided:

- Managing inventory filters
- Managing custom inventory object types

Managing inventory filters

During the collection process, hardware and software inventory lists are passed a number of times through a "translation" process, which converts executable file names and sizes into information about the hardware/software package, such as the name of the manufacturer, the version number and the type of application. These translation rules are stored in XML formatted text files on the individual clients. The files are specific in their schema for either hardware (`hwinvcfg.xml`) or software (`swinvcfg.xml`). The **Inventory Filters** node provides the administrator with a tool to manage these files directly for individual or groups of devices without actually having to edit the xml file itself.

All inventory filters created via the console are stored on the master in its file system in the <MASTER_INSTALL_DIR>/data/InventoryFilter/hw and <MASTER_INSTALL_DIR>/data /InventoryFilter/sw directories. When they are assigned to a device the file will be copied to the target and replace the currently existing XML file.

This section includes:

- Saving inventory filters
- Reverting to saved filter
- Related topics

Saving inventory filters

Any changes made to a hardware inventory filter must be saved before selecting another node, otherwise they are lost. Saving in this case means to upload the changes to the master server and the database. The operation in this node saves all modifications made to the WMI Filters and the Cleaning Filters. To save the changes, proceed as follows:

1. Select the **Hardware Inventory Filter** in the left window pane.
2. Click **Edit > Save** .

The modifications will be saved and uploaded to the master.

Reverting to saved filter

You can also revert to the last saved version of the currently selected inventory filter to abandon all modifications made up to this point. To do so, proceed as follows:

1. Select the **Hardware Inventory Filter** to be reloaded in the left window pane.
2. Click **Edit > Revert to Saved** .

The filter is reloaded in its last saved version and all modifications are lost.

Related topics

- Managing hardware inventory filters
- Managing software inventory filters
- Cleaning Rule - Inventory Filter

Managing hardware inventory filters

When collecting hardware inventory information not all available data is generally needed, thus filters are applied to sort the required data from the information which is currently not being regarded as useful. Filters can be defined for different kinds of clients and for devices with different operating systems, for example.

This section includes:

- Creating hardware inventory filters
- Managed WMI Classes
- Hardware Inventory Filter

Creating hardware inventory filters

It is possible to create new inventory filters for the hardware inventory. These filters will then replace the configuration filters in the form of an .xml file on the devices to which the newly created filters will be assigned. This file is based on the default .xml hardware template. To create a new hardware inventory filter, proceed as follows:

1. With the **Hardware Inventory** node selected in the left window pane select **Edit > Create Filter** .
   The **Properties** pop-up menu appears.
2. Enter the name for the new hardware inventory filter into the provided field.
3. Click **OK** to confirm the new object and close the window.

Managed WMI Classes

Windows Management Instrumentation (WMI) is a component of the Windows operating system that provides management information and control in an enterprise environment. WMI can be used to query and set information about desktop systems, applications, networks, and other enterprise components. Developers can use WMI to create event monitoring applications that alert users when important incidents occur.

WMI provides a standardised means for managing your computer system, be it a local computer or all the computers in an enterprise. It is collecting data about the state of a managed object on the computer system and altering the state of the managed object by changing the data stored about the object. A managed object can be a hardware entity, such as a memory array, a port, or a disk drive. It can also be a software entity, such as a service, a user account, or a page file. WMI can manage the many components of a computer system. In managing a hard disk, WMI can be used to monitor the amount of free space that remains on the disk. You can also use WMI to remotely alter the state of the drive by deleting files, changing file security, or partitioning or formatting the drive.

This tab displays the list of all WMI classes which are available. Be aware, however, that it is not an exhaustive list, it contains the most commonly used classes, to which you can add specific classes if necessary.

Creating WMI class

In WMI, a class is an object that describes some aspect of an enterprise. You can use an object to hold information or control an aspect of your enterprise. For example, you can create a WMI object that describes a CD-ROM drive. An object works with a WMI provider to fill the properties of an object. Creating a class means defining the properties that describe that class. You can also define the functions you can call to manipulate the object that the class represents. Each class has key properties. You cannot create an instance of a class with more than 256 keys. To create a new class, proceed as follows:

1. Select the **Hardware Inventory** node in the left window pane.
2. Select **Edit > Create WMI Class** .
   The **Create WMI Class** dialog box appears.
3. Enter the desired data into the respective boxes.
4. Click **OK** to create the new class and to close the window.

The newly created class will directly be displayed in the table in the right window pane.

Creating WMI classes

In WMI, a class is an object that describes some aspect of an enterprise. You can use an object to hold information or control an aspect of your enterprise. For example, you can create a WMI object that describes a CD-ROM drive. An object works with a WMI provider to fill the properties of an object. Creating a class means defining the properties that describe that class. You can also define the functions you can call to manipulate the object that the class represents. Each class has key properties. You cannot create an instance of a class with more than 256 keys. To create a new class, proceed as follows:

1. Select the **Hardware Inventory** node in the left window pane.
2. Select **Edit > Create WMI Class** .
   The **Create WMI Class** dialog box appears.
3. Enter the desired data into the respective boxes.
4. Click **OK** to create the new class and to close the window.

The newly created class will directly be displayed in the table in the right window pane.

Hardware Inventory Filter

Hardware inventory filters are completely customizable to be adapted to the specific needs of the different devices within your infrastructure. Hardware inventory objects can have one or several instances and attributes providing further information. These objects are completely customizable about name, number of instances, number of attributes and their types and contents.

Related topics

- WMI Filters
- WMI Classes

WMI Filters

This node displays the list of WMI classes which are in the `hwinvcfg.xml` file. This file is part of the hardware inventory collection, it is made to suit the users needs. Inventory collection is done by "passing" the list of available WMI classes through this configuration file. The file is an XML formatted text file supplied with the agent and can be modified or added to as required.

Adding WMI class

To add new WMI class to the hardware configuration file it must exist in the common list of WMI classes listed in the **Managed WMI Classes** tab of the main **Hardware Inventory** node. To add a WMI class to the filter, proceed as follows:

1. Select the filter to which a new class is to be added in the left window pane.
2. Click **Edit> Add WMI Class** .
   The **Select a WMI Class** pop-up menu appears.
3. Select the desired class from the list of the **Name** field.
4. Then define if the new class is to be accepted or rejected in the **Action** field.
5. Click **OK** to confirm and close the window.

For more information, see WMI Classes.

WMI Classes

In WMI, a class is an object that describes some aspect of an enterprise. You can use an object to hold information or control an aspect of your enterprise. For example, you can create a WMI object that describes a CD-ROM drive. An object works with a WMI provider to fill the properties of an object.

WMI attributes

A WMI class displays all its attributes, or properties which were added to the currently selected WMI class. These attribute lists tend to not be exhaustive, they include the most common attributes of the class. If a property important to your environment is missing in this list it can be added.

Creating a WMI attribute

1. Select the class to which a new attribute is to be added in the left window pane.
2. Click **Edit > Create Attribute**  .
   The **Properties** pop-up menu appears.
3. Enter the data for the new attribute in the respective boxes.
4. Click **OK** to confirm and close the window.

Managing software inventory filters

BMC Client Management - Inventory comes with a predefined filter for the software inventory that contains a quite large list of the most common software programs. However, it become necessary to modify this filter and adapt it to the software used in your infrastructure, which might not include a number of these programs but some other branch or company specific software. In the same way as for the hardware inventory, filters can be defined and customized for your needs about software inventory collection.The **Software Inventory** node displays the list of all software inventory filters that were created.

This section includes:

- Creating software inventory filters
- Software Inventory Filter

Creating software inventory filters

It is possible to create new inventory filters for the software inventory. These filters will then replace the configuration filters in the form of an xml file on the devices to which the newly created filters will be assigned. To create a new software inventory filter proceed as follows:

1. With the **Software Inventory** node selected in the left window pane select **Edit > Create Filter**  .
   The **Properties** pop-up menu appears.
2. Enter the name for the new software inventory filter into the provided field.
3. Click **OK** to confirm the new object and close the window.

Software Inventory Filter

Similar to hardware, software inventory filters are completely customizable to be adapted to the specific needs of the different devices within your infrastructure. Software inventory objects can have one or several instances and attributes providing further information. These objects are completely customizable about name, number of instances, number of attributes and their types and contents.

The following topics are provided:

- Software filter definitions
- Adding software filter definition
- Related topics

Software filter definitions

This node displays a number of predefined filters of software programs for the `swinvcfg.xml` file. This file is part of the software inventory collection and is made to suit the users needs. Inventory collection is done by "passing" the list of executable files through this configuration file. The file is an XML formatted text file supplied with the agent and can be modified or added to as required.

A software filter definition is an object that describes a specific software used in an enterprise. You can use an object to hold information or control an aspect of your enterprise, such as licensing issues. Software filtering is done in two steps:

1. In the MATCHFILE Tag tab conditions are specified which need to be fulfilled for an executable being translated into a software package.
2. If all conditions are fulfilled, and the action defined in the General tab is **Accept** , the CREATE Tag tab contains information on how to create a new installed software entry from information in the executable file.

Adding software filter definition

To add new software definition to a software inventory filter, proceed as follows:

1. Select the object to which a new attribute is to be added in the left window pane.
2. Click **Edit> Create Filter Definition**  .
   The **Select a Software Filter Definition** pop-up menu appears.
3. Enter the data for the new definition in the respective text boxes.
4. Click **OK** to confirm and close the window.

Related topics

- Software Filter - MATCHFILE Tag
- Software Filter - CREATE Tag

Software Filter - MATCHFILE Tag

The **MATCHFILE Tag** tab contains the match conditions for the translation entry of the XML file. This tag also specifies conditions an executable file must satisfy in order for the requested action being done. The matching operator is an AND operator which means that all of the specified criteria must be satisfied for a match.

Software Filter - CREATE Tag

If the match criteria defined in the **MATCHFILE Tag** tab were all satisfied and the action was to Accept the file, the **CREATE Tag** tab determines the characteristics of the software entry to be created. The attributes contained within this tag are used to set and define individual fields of a newly created software entry. This is in contrast to the attributes within the **MATCHFILE Tag** which are used as comparison criteria.

Cleaning Rule - Inventory Filter

This topic explains the for inventory filter cleaning rules for software and hardware inventory.

Software inventory filter cleaning rules

After the translation of executable files into installed software entries has taken place, the list of software entries is processed by passing it through another translation cycle which just acts on the software list. The aim of this second pass is to clean up and possibly cause the merging of the created software entries. No new software entries can be created as a result of this second translation process. The translation of software entries is slightly different to that of executable files in that whereas the translation of files is a single pass process, the software translation process repeats itself until no changes occur during a pass. This allows fairly complicated processing to take place by using fewer more focused translation entries.

Hardware inventory filter cleaning rules

After the inventory collection has taken place, passing it through a translation cycle processes the list of attributes. The aim of this is to clean up the values of those attributes and format their output. The attributes values translation process repeats itself until no changes occur during a pass. This allows fairly complicated processing to take place by using fewer more focused translation entries.

Next step

- Creating a cleaning filter

Creating a cleaning filter

To create a new cleaning filter, proceed as follows:

1. Click **Edit> Create Cleaning Filter**  .
   The **Properties** pop-up menu appears.
2. Enter the data for the new filter in the respective boxes.
3. Click **OK** to confirm and close the window.

Related topics

- Modifying the attributes of a tag
- Hardware filter -General tab
- Hardware filter - MATCH Tag
- Hardware filter - MODIFY Tag

Modifying the attributes of a tag

To modify a tag attribute, proceed as follows:

1. Select the filter definition for which the tag is to be modified in the left window pane.
2. Click either of the two table rows in the right window pane.
3. Click **Edit > Properties** .
   The **Properties** pop-up menu appears.
4. Modify the data according to your needs in the respective boxes.
5. To verify a regular expression you can click **Test** . This will open the **Regular Expression Helper** dialog box. The **Native Regular Expression** box will display the data of the **Data** box of the **Properties** window.
6. Enter the expression to verify in the text box **Test** and click **Test** .
   If correct, the following **Matching Groups** box will display the list of results.
7. Click **OK** to close the window and return to the **Properties** pop-up menu.
8. When you modified all necessary boxes click **OK** to confirm and close the window.

Hardware filter -General tab

The **General** tab of a WMI Class/Filter displays the following information about the class/filter:

Attribute	Description
Device Name	The name of the device on which the hardware was found. If a hardware element exists on more than one device there will be one entry per device in this table.
Name	Displays the name of the class/filter.
Action	This field displays the action that is to be taken when generating the inventory, possible values are ACCEPT and REJECT.

Hardware filter - MATCH Tag

This tab deals with the MATCH conditions for the hardware translation entry. The MATCH tag contains a number of attributes which in turn specify the conditions a hardware attribute must satisfy in order to match the translate hardware entry which will then take the requested action. The matching operator is an AND operator which means that all of the specified criteria must be satisfied for a match.

Hardware filter - MODIFY Tag

If the match criteria were all satisfied and the action was to accept the attribute value, the MODIFY Tag of a cleaning filter determines the characteristics of the hardware attribute to be changed. The child attributes contained within this tab are used to set and define individual attributes of the hardware entry being changed. This is in contrast to the attributes within the MATCH Tag tab which are used as comparison criteria.

Managing custom inventory object types

The BMC Client Management agent can also compile custom inventory objects of a remote client for inspection by the administrator. This is based on a periodically generated Custom Inventory list. In addition to the list objects and object instances can be added to the custom inventory locally through the console. If an object is added twice, once manually through the console and via the list, the entry defined by the console will take precedence.

The **Custom Inventory** list is an .xml file which is editable by the administrator and can then be transferred to all clients in the network. The generation of the custom inventory list is based on a number of parameters which are set in its configuration file, CustomInventory.ini. For more information about this subject refer to chapter Custom Inventory of the technical reference manual.

The **Custom Inventory** node of the console displays a list of all custom defined objects on the remote device. The list is generated by the agent and uploaded into the database at regular intervals. As with the other inventory information, all entries are stored in the database to be available even if the actual device is off-line. This information is by default updated once every 4 hours.

Custom inventory for a device shows a number of objects which should be applicable to all supported operating systems, that is, Windows, UNIX and Linux. Each of these objects will be displayed split up into object specific properties.

Each object property lists the different items it found and clicking one of these displays the type of the object plus some details on this item.

Like hardware and software objects, custom inventory objects can have one or several instances and attributes providing further information. These objects are completely customizable about name, number of instances, number of attributes as well as their types and contents.

You can execute following operations on custom inventory objects:

- Creating an object
- Adding an attribute
- Adding a new instance

Creating an object

It is possible to create new object types for the custom inventory. By default the Windows Security Settings and Windows MSS are already available. When creating a new object type, this new type will be added to the database and thus made available for all clients in the network. To create a new custom inventory object, proceed as follows:

1. With the **Custom Inventory Object Types** node selected in the left window pane, select **Edit > Create Object** .
   The **Create New Object** window appears.

2. Enter the name for the new object into the provided field.
3. Click **OK** to confirm the new object and close the window.

Adding an attribute

To add new attributes to a custom inventory object type, proceed as follows:

1. Select the object to which a new attribute is to be added in the left window pane.
2. Click **Edit> Add Attribute** .
   The **Add Attribute** pop-up menu appears.
3. Enter the data for the new attribute in the respective text boxes.
4. Click **OK** to confirm and close the window.

Adding a new instance

To add a new instance to a custom inventory object type, proceed as follows:

1. Select the object type to which an instance is to be added in the left window pane.
2. Click **Edit > Add Instance** .
   The **Properties** pop-up menu appears. It displays text boxes for the name of the instance and those for each of the attributes for this object type.
3. Enter the desired data for the new instance into the respective text boxes.
4. Click **OK** to confirm and close the window.

Configuring Financial Asset Management

The first step when using **Financial Asset Management** is to configure the necessary values for the devices in your network.

Configuration consists of the following steps:

- Configuring the currency to use for calculations.
- Configuring the global basic financial data of the device types in your network.
- *(Optional)* Configuring the evaluation schedule.
- *(Optional)* Adding customized lifecycle status values.
- Configuring specific data for individual devices and device groups.

Related topics

- Configuring the calculation currency
- Configuring the global data for device types
- Defining the financial data evaluation schedule
- Adding lifecycle status values
- Configuring device specific data
- Default Values

- Financial asset management parameters
- Lifecycle Status

Configuring the calculation currency

The first step for your configuration should be to define the currency. All subsequent values that you enter in the financial assessment views are based on this value.

Before you begin

Make sure you have the **Parameters** tab of the **Global Settings > Financial Asset Management** node selected.

1. Select the **Parameters** tab of the **Global Settings > Financial Asset Management** node.
2. Double-click the **Currency** entry.
3. Enter the denomination for the currency to use for your calculations into the text box of the appearing **Properties** window, for example, *$, Eur* or *GBP* .
4. Click **OK** to confirm and close the window.

The currency for your calculations is now defined and you can continue defining the global data for the device types of your infrastructure.

Configuring the global data for device types

The **Default Values** table of the **Global Settings > Financial Asset Management** node provides a large list of device types that tend to be available in networks with some default values that are preentered. If these do not apply to your company defaults you need to modify these for accurate financial assessment.

Before you begin

Make sure you have the **Default Values** tab of the **Global Settings > Financial Asset Management** node selected.

1. Select a device type that is available in your network in the table to the right, for example, **Server** or **Workstation** which would correspond to your master, relays and clients.
2. Right-click and select the **Properties** menu item from the appearing pop-up menu.
3. Define the following values in the appearing **Properties** window:
   - Enter the currently remaining value of the asset into the **Residual Value** box. The residual value is an estimate of the value of the asset at the time it is sold or disposed of; it may be zero. Residual value is also known as scrap value or salvage value.
   - Enter the number of months that this asset is supposed to work in your network into the **Estimated Useful Life of Asset (months)** box.
   - Select the method used to calculate the costs from the **Depreciation Type** list.
4. Click **OK** to confirm and close the window.
5. Repeat the preceding steps for all device types available in your network.

The general data is now defined for the device types that exist in your infrastructure.

Defining the financial data evaluation schedule

The schedule specified in this view manages the evaluation frequency of all financial data. By default it is always active and evaluates your data every hour. If this does not fit your requirements you can modify the schedule as follows:

Before you begin

Make sure you have the **Lifecycle Status** tab of the **Global Settings > Financial Asset Management** node selected.

1. Select the entry in the right window pane.
2. Click **Properties** .
   The **Scheduler** window appears.
3. Make the required modifications in the available options.
4. Click **OK** to confirm.

The new schedule takes effect immediately.

Adding lifecycle status values

You can add more lifecycle status values if the predefined ones are not explicit enough or do not fit your requirements. Any status values that you add can be applied to all your assets.

Before you begin

Make sure you have the **Evaluation Schedule** tab of the **Global Settings > Financial Asset Management** node selected.

1. Click **Add Status** .
   The **Add a Status** window appears on the screen.
2. Enter the name for the new status in the **Status** field.
3. Click **OK** to confirm.
   The status is added to the list at the bottom with the next sequence number available.
4. If the status needs to be moved to another place in the sequence select it.
5. Click **Move Up** until it is at the desired position.

> Be aware that your new status can never be the first in the order, this place is always held by **On Order** .

The new lifecycle status is now available for all assets and can be assigned to any new and existing one.

Note:

Be aware, that any custom created lifecycle status values are never included in the automatic data evaluation, therefore it must be deactivated on each device for which you select a custom status manually.

Configuring device specific data

In addition to the general device type data, some device specific data must be defined individually for each device in your network. Some of the information to provide is probably common to groups of devices, such as the **Vendor** , the **Purchase Date** , the **PO Number** . These values can be defined for the whole group instead of individually.

Default Values

This tab references all device types and their default values that are needed for any type of calculation by the financial asset management module.

Parameter	Description
Device Type	The device type of the asset.
Residual Value	Enter into this field the currently remaining value of the asset. The residual value is an estimate of the value of the asset at the time it is sold or disposed of; it may be zero. Residual value is also known as scrap value or salvage value.
Estimated Useful Life of Asset (months)	Enter the number of months that this asset is supposed to work in your network.
Depreciation Type	The method used to calculate the costs: • **Straight Line** : the most often used method, in which the company estimates the residual value of the asset at the end of the period during which it is used to generate revenues (useful life) and expenses a portion of *original cost* in equal increments over that period. • **Declining Balance** : the book value is multiplied by a fixed rate.

Financial asset management parameters

The parameters in this tab define the general behavior of the financial asset management.

This step sends an email with the list of newly autodiscovered devices since the last verification. The email contains the complete list of devices with other information pertinent to the individual devices, such as the operating system, discovered date and agent version, that have been added since the last verification.nThis step is only applicable on the master.

Parameter	Description
Currency	Enter into this field the abbreviation for the currency that is used for all financial asset management calculations. You may enter it as the three-letter-abbreviation, for example, *USD* for US Dollar ($), as its currency symbol *$* or a combination, for example, *US$* with a maximum of 3 characters. All parameters referring a cost item is followed by this value in parenthesis, for example, **Warranty Cost ($)** .

Lifecycle Status

Here you need to define the different stages of the lifecycle that an asset runs through in his life within your network.

A number of default stages are already predefined:

Parameter	Description
On Order	The purchase order for the asset was emitted but the asset has not yet arrived at the target location.
Received	The purchased asset has arrived at its target location.
In Stock	The purchased asset has arrived at its target location and is currently still stored there, that is, not yet installed at its final location in the network.
Deployed	The asset is now installed at its destination and used by the designated personnel.
Deprecated	The asset has finished its useful life in the company and been removed from the network.

Configuring Patch Management

In most cases the default settings of the **Patch Manager** allow you to start patching without having to configure it. The Master is defined as **Patch Manager** and the Patch Knowledge Base is updated every day at 11:00 PM to always have the latest patches ready for scanning.

However, if required by your infrastructure, you can also configure patching to adapt it to your needs.

Related topics

- Defining a Patch Manager
- Configuring the Patch Manager
- Configuring device settings for patch management
- Connecting to a Proxy Server
- Updating the Knowledge Base

Defining a Patch Manager

A Patch Manager is a device in your network which manages the patching system. With a Patch Manager you can:

- scan devices in your network for patches
- download patches
- deploy patches on affected devices
- check for new bulletins/ patches
- assess existing bulletins

Any device with a supported Windows operating system can be defined as Patch Manager. To be able to deploy patches efficiently across your network, the Patch Manager should have a strong configuration and at least 2GB disk space to store patches.

To be able to manage patches, a device must be a **Patch Manager**. Only Windows devices can be **Patch Manager** .

- If your Master has a Windows operating system, it is by default defined as the **Patch Manager** .
- If your Master has a Linux operating system, you must define another device as **Patch Manager** first before you can start inventorying for missing patches and patching.

> **Note**
>
> If you must use a Proxy Server to access the Internet, see the Connecting to a Proxy Server topic before selecting your **Patch Manager** .

1. Go to **Patch Management > Patch Manager** .
2. Click **Add a new Patch Manager** .
   The **Add a new Patch Manager** dialog box appears.
3. Click **All** .
   All available devices are listed.
4. Select the device you want to define as the new **Patch Manager** and click **OK** .
   The dialog closes and the device is listed as **Patch Manager** in the right window pane.

Configuring the Patch Manager

You can perform the following configurations:

- Update the Patch Knowledge Base
- Inform yourself about the status of the Patch Knowledge Base
- Configure proxy

To configure the Patch Manager proceed as follows:

1. Go to **Patch Management > Patch Manager > Your Patch Manager > Configuration** .
2. Double-click any line of the table in the right window frame.
   The **Properties** dialog displays.

3. Make the necessary changes to the parameters and click **OK** .

Configuring device settings for patch management

By default, all your devices except the Patch Manager have the same settings for Patch Management . Since not all devices have the same requirements and specifications, it might be useful to modify certain settings.

1. Go to **Device Topology > Your Device > Agent Configuration > Module Configuration > Patch Management** .
2. Double-click any line of the table in the right window frame.
   The **Properties** dialog appears.
3. Make the necessary changes to the parameters and click **OK** .

> Use an operational rule to configure more than one device with the same new settings.

Connecting to a Proxy Server

For security reasons you possibly set up a proxy server to protect the devices in your network from attacks or to keep them anonymous. In this case, you must define the login to the proxy server so that your Patch Manager can establish a connection to the Internet to download patches or update the Patch Knowledge Base .

> **Note:**
>
> Note, that configuring the proxy server as described in the following is not applicable to Windows XP or Windows Server 2003 Patch Managers.

> **Note:**
>
> Be aware, that if you are using the device as a patch manager and a scanner, the proxy will also be the same. If a proxy was already defined and you modify options here, these will then also apply to the other functionalities.

To connect to the proxy server proceed as follows:

1. Go to **Patch Management > Patch Manager > Your Patch Manager > Configuration** and click the **Proxy Options** tab.
2. Double-click any line of the table in the right window frame.
   The **Properties** dialog box appears.

3. Enter the following information into the respective text boxes:

Text box	What you must do
Host Name	Enter the host name of your proxy server.
Port	Enter the port of the proxy server to which you want to connect, for example, 8080.
User	Enter the proxy user name.
Password	Enter the proxy password.

4. Click **OK** to save your proxy settings.

You set up a connection to your proxy server. The next time the Patch Manager tries to establish a connection to the Internet, it will do so via the proxy server.

This section also includes:

Proxy server special cases

In environments, where a proxy server is used to control Internet access, some further configuration might be required depending on the operating system to use the Patch Management feature in CM .

- If your proxy server requires authentication, and there is no way to configure the proxy /firewall to allow the patch manager to either bypass the proxy, or allow connections from the patch manager to pass through the proxy without authentication, you must use a Windows XP or Windows Server 2003 system as the patch manager. If you do not have any available Windows XP or Server 2003 systems available, you must use option 4.
- If the proxy server can be configured to allow connections from the patch manager without requiring authentication, the patch manager can be a system running any version of Windows supported by the CM agent .
- If the proxy server cannot be configured to pass connections from the patch manager, but the proxy or firewall can be configured to allow connections from the patch manager to bypass the proxy, the patch manager can be a system running any version of Windows supported by the CM agent .
- This option is only recommended in cases, where none of the preceding options are possible, because you must manually download the patch definition files (which contain information needed to determine if a patch is missing), and manually download the patch files from the application vendor. For more information about this method, see the option 2 section in article 000010276.

Updating the Knowledge Base

When you scan a device for missing patches, the results are based on the data of the Patch Knowledge Base . The Patch Knowledge Base consists of all information about patches like severity, download links, descriptions, and so on By default the Patch Manager checks if updates are available for the Patch Knowledge Base every day at 11:00 PM. If there is an update, it is immediately downloaded.

With a delay of 24 hours, the updated Patch Knowledge Base is sent to all devices administrated by the Patch Manager . Thereby new files are only downloaded once and centrally distributed throughout the network.

If required, you can configure the default settings to adapt them to your needs. For example, it might be necessary to modify the schedule of checking for updates or the delay between update and distribution to devices.

Additionally you can also manually update the Patch Knowledge Base . If you have an Internet connection, you can do so with one click. If your Patch Manager does not have an Internet connection, you must download the files first on another device, put them on the Patch Manager and update the Patch Knowledge Base with these files.

Related topics

- Configuring the Knowledge Base
- Manually Updating the Knowledge Base - Internet Update
- Manually Updating the Knowledge Base - Local Update

Configuring the Knowledge Base

1. Depending on whether you want to configure the Patch Knowledge Base for the Patch Manager or a particular device, proceed with one of the following two options:
   - To configure the Patch Manager , go to **Patch Management> Patch Manager> Your Patch Manager> Configuration** .
   - To configure a particular device, go to **Device Topology> Your Device> Agent Configuration> Module Configuration> Patch Management**
2. Double-click any line of the table in the right window frame.
   The **Properties** dialog displays.
3. Make the necessary changes to the parameters and click **OK**.

Patch knowledge base parameters

Knowledge base parameters for patch manager

The following table provides more information about knowledge base parameters for the patch manager:

Parameter	Default Value	Description
Enable Internet Check for Knowledge Base Update	**Yes**	Check this box to activate the verification for new versions of the Knowledge Base via the Internet. This value is only applicable to the Patch Manager, for all other devices this value should be deactivated.
Internet Check Schedule for Knowledge Base Update	Every Day, at 23:00	Click the **Edit** icon to the right of the field to define or modify the schedule for the Knowledge Base update via Internet. Select the desired values from the options in the appearing window.
Automatic Knowledge Base Update after Check	**Yes**	Check this box to automatically update the configuration files with the newly found version of the files. If activated this option only downloads the file if the file is of a newer version than the version currently available on the Patch Manager, or if the **Force Parse** parameter is activated. It then directly updates the local file.
Force Parsing	**No**	Defines if the Knowledge Base is to be parsed again, even if it was already parsed before.
Update Type	23	Defines if the local device is to update its version of the Knowledge Base locally or via the Internet.

Knowledge base parameters for a device

The following table provides more information about knowledge base parameters for a device:

Parameter	Default Value	Description
Enable Internet Check for Knowledge Base Update	**No**	Check this box to activate the verification for new versions of the Knowledge Base via the Internet. This value is only applicable to the Patch Manager, for all other devices this value should be deactivated.
Internet Check Schedule for Knowledge Base Update	Dimmed	Click the **Edit** icon to the right of the field to define or modify the schedule for the Knowledge Base update via Internet. Select the desired values from the options in the appearing window.
Automatic Knowledge Base Update after Check	Dimmed	Check this box to automatically update the configuration files with the newly found version of the files. If activated this option only downloads the file if the file is of a newer version than the version currently available on the Patch Manager, or if the **Force Parse** parameter is activated. It then directly updates the local file.

Manually Updating the Knowledge Base - Internet Update

By default, the Patch Knowledge Base is updated every day at 11:00 PM to ensure that devices are scanned for the latest patches. If you are connected to the Internet and immediately want to update the Patch Knowledge Base , proceed as follows:

1. Go to **Patch Management > Patch Manager > Your Patch Manager > Configuration** .

> If **Database Status** displays the status `Up to Date` , the Patch Knowledge Base already is up-to-date.

2. To check for updates, in the right window pane click **Check for Update** .
    a. If the **Database Status** line displays the final status `Up to Date` , the Patch Knowledge Base already is up-to-date.
    b. If the **Database Status** line displays the status `Out of Date` , the Patch Knowledge Base must be updated. Continue with the next step.
3. To update the Patch Knowledge Base , click **Update** .
4. To update the Patch Knowledge Base even if the **Database Status** status `Up to Date` displays, click **Force Update** . In this case the currently used Patch Knowledge Base will be replaced with the newly downloaded version, even if the version number is the same.

> This option might be useful, if for example the last update was interrupted by a power cut or any other network interruption and you are not sure if the update installed correctly.

You updated the Patch Knowledge Base of the Patch Manager . For your next scan these configurations will be used.

Patch knowledge base update status values

When checking for available updates or updating the patch knowledge base, the following status values can be displayed for the **Database Status**:

Parameter	Description
`License Error`	Either the license is not imported or the license could not be verified.
`Checking`	The agent is currently trying to download or parse the XML file containing the information for the knowledge base update.
`Check Failed`	The XML file containing the information for the knowledge base update could not be downloaded or parsed.
`Out of Date`	This status indicates that a newer version of the knowledge base exists and is available for download.
`Downloading`	The patch knowledge base update file is currently being downloaded by the Patch Manager.
`Download Failed`	The download of the patch knowledge base update file failed.
`Published`	The patch knowledge base update file was downloaded by the Patch Manager and was published on the master. It is now ready for distributing and updating to all agents.
`Updating`	The update file is being sent to the agents and the patch knowledge base is being updated on all Windows devices, the Patch Manager included.
`Update Failed`	The update of the knowledge base to the new version failed.
`Deployed`	The patch knowledge base on the master is updated.
`Up to Date`	This status indicates that the knowledge base is of the latest version. It is accompanied by a green flag next to it.

Manually Updating the Knowledge Base - Local Update

Automatically updating the Patch Knowledge Base requires a permanent Internet connection. If your Patch Manager is not connected to the Internet, you can still keep the Patch Knowledge Base up-to-date. This process consists of downloading the files on another device, putting them on the Patch Manager and updating the Patch Knowledge Base with these files. To do so, proceed as follows:

1. Access another device with an agent installed on it and has access to the internet.
2. Launch the command line tool.
3. Go to the bin folder of the agent. Typically, the agent is located at, `cd .../agent/bin.`
4. Create a Temp folder in the bin folder of the agent.
   mkdir `Temp`
5. From the bin folder, launch the command line and enter the following command. .
   `mtxpatch.exe -u --outdir=./patch --tmpdir=./patch --manifest=https://content.ivanti.com/data/oem/BMC-Numara/data/925/manifest/partner.manifest.xml`
6. In the Temp folder, a new file is created, `update.bin.`
7. On the master server, copy the update.bin file to the `data/Vision64Database/pmupdates/pending` folder.
8. Remove the temp folder in the bin folder of the agent.
9. Restart the master server. The knowledge base will be updated and then sent to all devices.

You manually updated the Patch Knowledge Base of Patch Manager with files on your local device. To update the Patch Knowledge Base again at a later time, put the four files into the updatefolder and click **Update** again.

Configuring Windows Device Management

Like most other modules, **Windows Device Management** is configured via the **Agent Configuration** of the respective device.

The following topics provide more information about configuring device management:

Configuring the Windows Device Management

The **Windows Device Management** node defines the configuration parameters of the Device Management module as it is configured for this device.

To modify the settings of the module, proceed as follows:

1. Select **Device Groups> Your Managed Device> Agent Configuration** in the left window pane.
2. Select any line in the table in the right window pane of the respective subnode.
3. Select **Edit> Properties** 
   The **Properties** window appears.

4. Make the desired modifications to the individual values.
5. Click **OK** to confirm the modifications and close the window.

Generated events

All alerts and events that are generated for the **Windows Device Management** can be viewed locally under the **Event Management** tab of **Agent Configuration** node of the respective device. The tab displays all events which were logged at agent level and currently stored in the local database. It displays the following information about the individual events:

Parameter	Description
Event Date	The date and time at which the device management action, was executed, for example, a USB storage device was connected.
Type	This field displays the type of event that occurred, that is, the screen saver was activated, the device was put in hibernation, and so on.

Configuring compliance management

The following topics help you configure compliance management features and functions:

- Configuring compliance constants
- Configuring custom compliance
- Configuring SCAP Compliance

Configuring compliance constants

Compliance constants can be used in criteria as placeholders for values. The constants defined here can be used in any compliance rule to be defined.

You can execute following operations on compliance constants:

- Creating a constant
- Creating a compliance rule using a constant

Creating a constant

Compliance constants can be used in criteria as placeholders for values. The constants defined here can be used in any compliance rule to be defined. To create the constant that represents the BMC Client Management installation directory, proceed as follows.

1. Select the **Constants** tab.
2. Click **Create Constant** .
3. Enter *PATH CM Client* as the constant name.
4. Enter *C:/Program Files/BMC Software/Client Management* as the value that the constant represents.
5. Click **OK** to confirm and add the new constant.

The constant is now created and can be used in compliance rules.

Creating a compliance rule using a constant

This compliance rule finds all clients on which the CM client is not installed in its default directory. This rule will use a constant instead of entering a value or selecting it from the lists provided by the search functionality. This rule will have one criteria group.

1. Click **Create Compliance Rule** .
2. Enter *CM Client Installation Directory* into the **Name** box and then click **OK** .
3. Double-click the new rule in the table to the right.
4. Select the **Criteria** tab.
5. Click **Add Criteria Group** .
6. Enter *Client Path* into the **Name** box.

This group will find all devices on which the client is installed in the specified directory.

1. In the **Class** list, select the **Software Inventory** value.
   The following **Table** box will update its contents to the fields available for the software inventory.
2. Select the value **Scanned Application (Deprecated)** in the **Table** box.
3. Select the criterion **Installation Directory** .
4. Click **Constant** next to the **Value** box.
5. Select the *PATH CM Client* constant and click **OK**.
6. Click **Add** .
7. Click **OK** to add the criteria group to the rule.
8. To activate the compliance rule select the green colored option *active* instead of the currently displayed red option *inactive* in the **Status** list.

You have now created a compliance rule that uses a constant. To check for device compliance assign this rule to the required devices/device groups and evaluate.

Configuring custom compliance

Contrary to the majority of the other CM modules, the configuration of the **Custom Compliance** module is not done via the **Agent Configuration** of the device but directly under the main compliance node via its own **Configuration** node.

> **Note:**
>
> Be aware that this node will not be displayed if you do not have the **Configure Compliance** capability.

Under this node you can configure the following:

- The general settings of the compliance behavior via its parameters.
- You can also define constants that are to be used with the compliance rules
- In addition you can define for which rules or groups assigned to rules alerts are to be generated.

The General Parameters of Custom Compliance

This tab provides the access to the module specific parameters and their values.

Parameter	Description
Evaluation Frequency (min)	Defines the interval in minutes at which the compliance rules is newly evaluated. If no value is specified, the rules are evaluated at agent startup, otherwise the automatic evaluation feature is deactivated.

Configuring SCAP Compliance

Contrary to the majority of the other CM modules, the configuration of the **SCAP Compliance** module is not done via the **Agent Configuration** of the device but directly under the main compliance node via its own **Configuration** node.

> **Note:**
>
> Be aware that this node will not be displayed if you do not have the **Configure Compliance** capability.

Under this node you can do the following:

- Import CVE and CCE lists in the **CVE & CCE Lists** tab.
- Specify the alerts that are to be generated for SCAP compliance under the **Alerts** tab.
- Import and manage the SCAP packages that are to be used for the SCAP jobs under the **SCAP Packages** subnode.

Related topics

- CVE and CCE lists
- Importing CVE and CCE lists
- SCAP compliance alerts
- SCAP Packages

CVE and CCE lists

The **CVE & CCE Lists** view allows you to import downloaded CVE and CCE lists and display the imported lists in tabular format. Once imported, the content of these lists populates the **Properties** windows of the rules contained in a package or the rules of a scan result, to provide the available information about the CVEs and CCEs the rule contains.

- CVE (Common Vulnerabilities and Exposures) is a dictionary of common names (that is, CVE Identifiers) for publicly known information security vulnerabilities. CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other. You can download the CVE List, copy it, redistribute it, reference it, and analyze it, provided you do not modify CVE itself. For more information about CVE and their terms of Use refer to the CVE website .
- CCE (Common configuration Enumeration) lists provide unique identifiers to security-related system configuration issues in order to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools. For more information about CCE and their terms of Use refer to the CCE website .

Both of these lists are part of the existing open standards used by NIST in its Security Content Automation Protocol (SCAP) program. Both lists help, through the use of consistent identifiers, to improve data correlation; enable interoperability; foster automation; and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance. CVE provides this capability for information security vulnerabilities, CCE assigns a unique, common identifier to a particular security-related configuration issue.

The view shows the following information about the imported lists, which are referenced by the SCAP rules and in visualizing the SCAP job results:

Parameter	Description
Name	The name of the imported file.
Type	The type of the list, that is, if it is a CVE or CCE list.
Integration Date	The date at which the list was imported into the CM database.
Publication Date	The date at which this specific list was made publicly available by its owning organism.
Entry Count	The number of entries, that is, vulnerabilities or configurations that the list includes.

Importing CVE and CCE lists

CVE and CCE lists can be added to Client Management at any time.

> **Note:**
>
> Before you can import any of these lists into Client Management you need to download them.
>
> NVD/CVE XML feeds with CVSS and CPE mappings (version 2.0) can be downloaded at the following URL: http://nvd.nist.gov/download.cfm .
>
> NVD/CCE XML feeds with 800-53 mappings can be downloaded at the following URL: http://nvd.nist.gov/cce.cfm .

Client Management provides a some of these lists with its installation; lists, containing CCEs and CVEs, which are specifically used for the USGCB tests. You can import these from the **<InstallDir>\master\data\Vision64Database\scap\data_feeds** directory. These lists are the most up-to-date at the time of this version's release. If you install and import considerably later, newer lists may be available on the respective sites.

To import these lists, proceed as follows:

1. Click **Edit > Import CVE List** or **Edit > Import CCE List** , depending on the list type to import.
   The **Import a CVE List** / **Import a CCE List** window opens on the screen.
2. Browse to the directory into which you downloaded the list and select it.

   > You can import several lists of the same type at the same time by holding the CTRL key when selecting the lists.

3. Click **Open** .

The imported list is directly added to the CM reference database and displayed under the **CVE & CCE Lists** tab.

> **Note:**
>
> Depending on the number of lists selected and their size this operation can take some time and you should refresh.

SCAP compliance alerts

This view displays all alerts that are configured for the Compliance Management. It also allows you to add new alerts.

The view shows the following information about the defined alerts:

Parameter	Description
Name	The name of the alert.
SCAP Job Name	The name of the SCAP job name for which the alert is to be generated.
Group Name	The name of the device group assigned to the SCAP job for which the alert is to be generated. This field might be empty if the alert is to include all device groups assigned to the job.

Defining SCAP Compliance alerts

To specify for which compliance rule or for which group assigned to a specific compliance rule an alert is to be generated, proceed as follows:

1. Click **Add Alert** .
   The **Add an Alert** window appears.
2. Select the rule and, if required, the specific device group for which an alert is to be generated.
3. Click **OK** to confirm.

The alert is added directly to the list. Now, if any status change occurs for this rule or, if the alert is to be generated for an assigned group, on any of the group's members an alert is generated.

SCAP Packages

Under this node you can import, manage and remove SCAP packages of versions 1.0, 1.1 and 1.2 and you can order them into folders according to your requirements. These packages are used as the base for compliance tests and verifications of your device population.

It is not possible to modify any SCAP package parameters except the **Notes** , nor can you copy and paste a package. You can, however, cut and paste a package from one SCAP package folder to another.

By default, an imported version 1.0 or 1.1 SCAP package and its data stream are created with the same name as that of the benchmark in CM . If the package file contains several xml files, one 1.2 SCAP package is created for each data stream collection and is given its predefined name.

Depending on the version the downloaded zip archives can contain one or more xml files: for version 1.0/1.1 a zip file only contains one package, for version 1.2, a zip file can contain several xml files, and an SCAP package will be created for each of these files.

SCAP packages general data

This view displays the following data about all imported SCAP packages:

Parameter	Description
Name	This field displays the name of the SCAP package.
Version	The fields of this column display the SCAP version number of the package.
Validation Date	The field displays the date at which the package was validated.
Use Case	This field displays the use case for the package. This field is only applicable to packages of version 1.0 and 1.1.

Related topics

- Importing new SCAP packages
- Validating a newly imported SCAP package

- Deleting SCAP packages
- SCAP Package

Importing new SCAP packages

SCAP packages can be added to CM at any time.

> **Note:**
>
> Before you can import packages into BMC Client Management you need to download them, for example from the [NVD (National Vulnerability Database) of the NIST (National Institute of Standards and Technology)|http://web.nvd.nist.gov/view/ncp/repository] website.

To import SCAP packages, proceed as follows:

1. Click **Edit > Import SCAP Package** .
   The **Select an SCAP Package** window opens on the screen.
2. Browse to the directory into which you downloaded the package and select it.
3. Click **Open** .

The imported file (zip or xml) is send to the master, which unzips and parses it. It then creates the new SCAP package in the CM database with its associated components (data streams, benchmarks, profiles, OVAL checks, etc.). The imported files are saved in a subdirectory with the ID of the newly created package as its name, in the **data/scap/checklists** directory.

If a version 1.2 zip file contains multiple xml files, multiple SCAP packages are created. Each of these SCAP package is given is predefined name.

You can view the package components in the respective tabs and subnodes.

Validating a newly imported SCAP package

It is possible to download SCAP packages from many different sources, it is possible that the downloaded data is not 100% compliant with the Schema and Schematron rules. It is therefore important to ensure that the content is compliant, and this validation operation verifies all these Schema (XSD) and Schematron rules.

To verify an imported SCAP package proceed as follows:

1. Select the package to verify in the table in the right window pane.
2. Click **Edit > Validate SCAP Package** .
   The CM agent now runs verifications to check that the content of the package is compliant with all required Schema and Schematron rules.

If the verification is successful the **Validation Succeeded** window appears indicating that the package was successfully verified.

Deleting SCAP packages

To delete an SCAP package, proceed as follows:

> **Note:**
>
> Be aware that only packages which are not assigned to any SCAP job can be deleted. If the package is still assigned you first need to delete the respective SCAP job before you can delete the package here.

1. Select the package to be deleted in the right window pane.
2. Click **Edit > Delete** .
   A confirmation window appears.
3. Click **OK** to confirm the delete operation.

The selected package is immediately deleted from the CM database.

SCAP Package

SCAP packages (security checklists) define a collection of data streams, and each of these data streams is expected to reference external components:

- Dictionaries: Provides references to the CPE standard
- Checklists: Provides references to the XCCDF standard
- Checks: Provides references to OVAL or OCIL standards

It is created when the downloaded security checklist is imported into CM and unzipped and parsed.

Starting from version 1.2, SCAP defines itself a specific XML file format. The idea is to provide a container for embedding all the required components into a single file. Before version 1.2, different XML files were required in order to conduct an SCAP scan. Additionally, the new standard makes it possible to build mappings between components, easing cross reference between each of them.

Security checklists of versions 1.0 and 1.1

The package is downloaded in the form of a zip file that contains an **xccdf** , one or more **OVAL** check files, optional **CPE** dictionaries and possibly some other files. The **xccdf** file contains one benchmark only and its profiles.

By default, an imported SCAP package and its data stream are created with the same name as that of the benchmark in CM .

Security checklists of version 1.2

The downloaded package is either a individual xml file or it can be a zip file that can contain several xml files. Each xml file is a data stream collection containing a list of data streams. Each of these data streams can contain several benchmarks, which in turn, can also have several profiles.

By default, each SCAP package is given the name of the associated data stream collection in CM .

General data of an SCAP package

This view displays the following data about a specific SCAP package:

Parameter	Description
Name	This column displays the name of the selected SCAP package.
Version	This field displays the version number of the package.
Validation Date	The field displays the date at which the package was validated.
Use Case	This field displays the use case for the package. This field is only applicable to packages of version 1.0 and 1.1.

Related topics

- SCAP package Data Stream
- SCAP package Benchmarks

SCAP package Data Stream

An SCAP package can have one or more data streams. If the package is version 1.2 or later it can contain a collection of data streams, otherwise only one.

The following information is available for data streams:

Parameter	Description
Name	This column displays the list of names of all data streams contained in the checklist. By default the package and data stream will be created with the name of the associated benchmark.
Version	The fields of this column display version number of this checklist.
Publication Date	The date at which this specific data stream was made publicly available by its owning organism.

Additional information about the data stream and its contents is available via its tabs and subnodes, see SCAP package benchmarks.

SCAP package Benchmarks

A data stream can have one or more benchmarks, depending on its version. If it is version 1.2 or later it can contain several benchmarks, otherwise only one. Benchmarks contain the rules, which are the actual tests that are executed and the profiles, which are a sort of a filter on these rules.

The following information is available for benchmarks:

Parameter	Description
Name	This column displays the list of names of all benchmarks contained in the checklist.
Version	The fields of this column display the version number of this benchmark.
Title	The field displays the exact title of this benchmark.
Description	The field displays a more explicative description on the benchmark and what exactly it contains.
Creator	The fields of this column display the name of the person, organization and/or service that initially created this benchmark.
Publisher	The fields of this column display the name of the person, organization and/or service that published the benchmark.
Contributor	The fields of this column display the name of the person, organization and/or service that contributed to the creation of the benchmark.
Source	The fields of this column display the link from where the benchmark can be downloaded. (This is a identifier that indicates the organizational context of the benchmark's @id attribute.)
Status	Represents the level of maturity or consensus level for this benchmark.
Status Date	The date this benchmark achieved the indicated status.
Platform	The target platform for this benchmark using CPE naming form.

Additional information about the benchmark and its contents is available via its tabs and subnodes:

- SCAP package Profiles
- SCAP package Rules
  - Viewing the SCAP rule information

SCAP package Profiles

The **Profiles** tab displays the list of all profiles that are included in the package. It is possible that a package does not include a profile. A profile makes a preselection of the rules that are included in the package that apply to a specific role or situation. When a profile is then selected for a SCAP job this means that only the rules that are listed in this profile and not all that are included in the package are to be run.

The following information is available for profiles:

Parameter	Description
Name	This column displays the list of names of all profiles contained in the checklist.
Title	The field displays the exact title of this profile.
Description	The field provides a more explicative description on the profile and what exactly it concerns.

SCAP package Rules

The **Rules** tab displays the list of all rules that are included in the SCAP package. Rules are the actual tests that are executed on the targets to check if they are compliant to a specific requirement.

The following information is available for rules:

Parameter	Description
Name	This column displays the list of names of all rules contained in the checklist.
SCAP Rule ID	The field displays the ID of each SCAP rule.
Description	The field provides a more explicative description on the rule and what exactly it does.

Viewing the SCAP rule information

To display more detailed information about a specific rule proceed as follows:

1. Select the rule for which you want more information in the right window pane.
2. Click **Edit > Properties** .
   The **Properties** window appears. It displays all the information available in its different tabs. Depending on the type of rule, that is, if it is CVE or CCE, the content of the window changes. If the rule has several CVEs or CCEs or both, there is one panel per CVE or CCE, each of which can be expanded and collapsed.

   > **Note:**
   >
   > If this window does not show any additional information you have not downloaded the respective CVE or CCE. Refer to Importing CVE and CCE lists to import them.

3. Click **Close** to close the window.

Configuring mobile device management

Before you invite users to enroll their mobile devices, you need to configure the mobile device management.

The following BMC Client Management video (5:28 min) provides step-by-step process to configure mobile device management:

https://youtu.be/Ymm12v4oiJY

Perform the following tasks to complete the end-to-end process of configuring mobile device management in BMC Client Management:

Task	Description	Reference
1	Review the prerequisites.	Before you begin

Task	Description	Reference
2	Set up the mobile device manager.	To define and configure the mobile device manager
3	Set up an Apple push certificate.	To prepare and install an Apple Push Certificate
4	Set up authorized domains.	To add an authorized email domain
5	(*Optional*) Set up the terms and conditions.	To create terms and conditions
6	Authorize users and the user groups.	To add users (or user groups) to authorized users (or authorized user groups) list
7	(*Optional*) Customize the logo for the enrollment page.	To customize a logo for the enrollment page
8	Send an enrollment invitation.	To invite users or user groups to enroll

For more information about mobile device management capabilities, see Mobile device management.

Before you begin

Ensure that the following prerequisites are met before configuring mobile device management :

- At least one computer (physical or virtual) with internet access to serve as the mobile device manager. This computer is used to manage enrollment, notifications, and other communication with the managed mobile devices.
- An Apple account to prepare an Apple Push Certificate. For more information about Apple account, see Before You Enroll .
- At least one directory server is configured for authentication. This directory server must be able to authenticate the users who are enrolling their mobile devices for mobile device management. For more information about the directory server, see Managing directory servers.
- Default email system is set up for sending and receiving emails. For more information about default email settings, see Managing email settings.
- Email addresses defined in the directory server for the users who will enroll their mobile devices. The users will receive the invitation on this email address and they will have to enroll their mobile devices using the same email address.

To define and configure the mobile device manager

After verifying the prerequisites, the first step in configuring mobile device management is to define and configure a mobile device manager.

1. In the left pane, click **Mobile Device Management**.
2. Right-click **Mobile Device Managers** , and select **Add Device** .
3. In the **Add a new Mobile Device Manager** dialog box, search or browse to select the computer, and click **OK**.
   The computer is defined as the mobile device manager.
4. In the left pane, select the newly defined mobile device manager.
5. In the right pane, right-click any row and select **Properties** .
6. In the **Properties** dialog box, specify the parameters as required.
   a. The **Enrollment URL** is a read-only, auto-populated field.
   Once enrolled, the mobile device will connect to the mobile device manager using this secure URL.
      - If you specify a **Server Name** in the step b, the URL is populated with the specified server name. For example, if you specify the server name as `mobiledevicemanager.bmc.com`, the URL is: `https://mobiledevicemanager.bmc.com:1661/mdm`.
      - If you leave the **Server Name** field empty, the URL is populated with the IP address after the following mobile device management configurations are completed:
         - The Apple Push Certificate is installed.
         - At least one email domain is added to the **Authorized Email Domains** list.
         - At least one user or user group with a valid email address is added in the **Authorized Users** or **Authorized User Groups** lists, respectively.

      > **Note**
      >
      > If you use the IP address in the URL, the server must be assigned a static IP address. If the URL changes (due to a change in the IP address or the port number), the enrolled mobile devices will not be able to connect with the mobile device manager.

   b. (*Optional*) Specify a **Server Name** for the mobile device manager.

      > **Note**
      >
      > It is strongly recommended that you specify a server name. If you have specified the server name, the enrollment URL is built with the specified server name. So, even if the IP address of the server changes, the URL does not change and the enrolled mobile devices have continuous access to the mobile device manager.

c. (*Optional*) Specify a different **Server Port**.
The default port is 1661.

> **Note**
>
> Once assigned, the port number must not be changed. If the port number is modified, the enrollment URL will change and the enrolled mobile devices will not be able to connect to the mobile device manager.

d. (*Optional*) Specify the **Server Certificate** and **Signing Certificates** names.
- If these certificates are already installed, the certificate names are automatically populated.
- If these certificates are already available but not installed, you can put the certificate in appropriate folder on the master server and specify the certificate file names in these fields. You can also select option to install the certificates.
- If you do not have certificates, you can purchase and install the new certificates. If the server certificate is not configured, a temporary certificate is issued each time the agent service starts up. The temporary certificate is issued by the currently configured BCM Certificate Authority (CA).

> **Notes**
>
> - When purchasing new certificates, ensure that the **Server Name** matches the **Certificate Subject Name** or the **Subject Alternative Name** attributes in the certificate. These certificate attributes are used when the mobile device connects with the mobile device manager.
> - If you need to update the agent CA certificate, first you must install the new CA certificate in the mobile device using the Certificate payload. Then, the mobile device will trust the new CA certificate and continue connecting with the mobile device manager.

For more information about preparing and installing the certificates, see Adding an SSL certificate.

e. (*Optional*) Specify the number of notification threads to be opened in **Notification Thread Count** .
The default value is 2. To disable notification, specify the value as 0. If two or more mobile device managers are configured with a value greater than 0, only one mobile device manager is used for notification.

7. Click **OK**.
   The mobile device manager is defined and configured.

To prepare and install an Apple Push Certificate

After at least one mobile device manager is defined and configured, you need to prepare and install an Apple Push Certificate. If you already have an Apple Push Certificate available, you can select the option to install the certificate.

1. In the left pane, select **Mobile Device Management** > **Configuration** .
2. Right-click **Apple Push Certificate**, and select **Prepare Certificate** .
   The **Apple Push Certificate Creation Wizard** dialog box is displayed.

> **Note**
>
> If you have already created and downloaded the Apple Push Certificate file, you can select the **Install Certificate** option and refer to step 8.

3. Read the information, and click **Next**.
4. On the Create CSR Certificate page, type the required information, and click **Generate CSR Certificate**.
5. Type a name for the certificate request (**.csr**) file and save it on the local drive.
   You will need to upload this certificate in the next page to generate and download the Apple Push Certificate file.
6. Click **Next**.
   The Apple Manual Procedure page is displayed. Follow the instructions on this page to create and download the Apple Push Certificate (**.pem**) file.
7. After you have downloaded the Apple Push Certificate file, select the **I have completed the steps and saved the PEM file from the Apple Portal** check box, and click **Next**.
8. On the Import Apple Push Certificate page, browse to select the Apple Push Certificate file.
   The page displays the encrypted text between the `BEGIN CERTIFICATE` and `END CERTIFICATE` marker lines.
9. Click **Finish**.
   The certificate is now installed and the right pane displays the certificate name and its expiration date.

To add an authorized email domain

To enroll for mobile device management, the users need an email address registered in the directory server. The email domain of this registered email address must be listed in the **Authorized Email Domain** list. For example, if the email domain of a user's registered email address in the directory server is bmc.com, then bmc.com must be listed in the **Authorized Email Domains** list.

T he user needs to select the appropriate email domain from the list during enrollment. For example, if bmc.com , gmail.com , and yahoo.com are listed as authorized email domains and a user with email in the bmc.com domain is enrolling, the user needs to select bmc.com from the drop-down list.

> **Note**
>
> You can add multiple email domains as authorized email domains.

1. In the left pane, select **Mobile Device Management** > **Configuration** > **Enrollment**.
2. In the right pane, right-click in the **Authorized Email Domains** tab, and select **Add Email Domain** .
3. In the Add an Authorized Email Domain window, specify the domain name that you want to authorize, and click **OK**.
   The email domain is added as an authorized email domain.

To create terms and conditions

Terms and conditions are displayed when the users enroll their mobile devices. The terms and conditions for a user or user group are selected when they are added to an authorized user or an authorized user groups list for the mobile device management. You can create multiple instances of the terms and conditions depending on your requirements. For example, you can create separate instances of the terms and conditions for the users in different countries.

1. In the left pane, select **Mobile Device Management** > **Configuration** > **Enrollment**.
2. Right-click **Terms and Conditions**, and select **Create new Terms and Conditions** .
3. In the Properties window, specify the terms and conditions details, and click **OK**.
   The newly created instance of terms and conditions is created.
4. In the left pane, select the newly created instance of the terms and conditions.
5. Go to the **Content** tab and type or paste the text for the terms and conditions.
   The text box supports plain text and HTML.
6. Click **Save**.
   The content of the terms and condition is saved.

> **Note**

You can view the users and user groups to whom this instance of the terms and conditions is assigned, in the **Authorized Users** and **Authorized User Groups** tabs respectively.

To add users (or user groups) to authorized users (or authorized user groups) list

Before you can invite the users to enroll for mobile device management, you need to authorize them. From the directory server, you can either add individual users or add user groups to the list of authorized users or user groups respectively.

Important

For the users to enroll their mobile devices for mobile device management, they must have an email address in their account information in the directory server.

1. In the left pane, select **Mobile Device Management** > **Configuration** > **Enrollment**.
2. In the right pane, right-click in the **Authorized Users** (or **Authorized User Groups**) tab, and select **Add User** (or **Add User Group**).
3. In the **Select a User** (or **Select a User Group**) dialog box, search or browse to select the users (or user groups) you want to authorize for enrollment.
4. From the **Select Terms and Conditions** list, select the terms and conditions you want to set for the selected users (or user groups).
   This instance of terms and conditions is displayed when the users enroll their mobile devices.
5. Click **OK**.
   The selected users (or members of the user group) are authorized to enroll their mobile devices.

To customize a logo for the enrollment page

From the **Customization** tab, you can customize the logo that will be displayed during mobile device enrollment.

1. In the left pane, select **Mobile Device Management** > **Configuration** > **Enrollment**.
2. In the right pane, click the **Customization** tab.

3. Click **Browse** and select the image that you want to set as logo.
   In the **Import Picture** dialog box, the red selection box displays the area of the image to be used as logo.
4. Move the red selection box to select a part of the image.
   You can also resize the red selection box by dragging the right lower corner. The right pane displays the preview of the selected part of the image as a logo. If you resize the red selection box, the aspect ratio is maintained and the cropped image is resized to appropriate dimensions.
5. After you select the image or part of the image, click **OK**.
   The **Logo Customization** page displays the preview of the enrollment page with the new logo.
6. Click **Apply** to confirm your selection.

To invite users or user groups to enroll

After completing the preceding configurations, you can start inviting users to enroll for mobile device management. To enroll, the user must have an active account in directory server with a valid email address. Also, the email domain of the registered email address must be added to the authorized email domains list.

1. In the left pane, select **Mobile Device Management** > **Configuration** > **Enrollment**.
2. In the right pane, click the **Authorized Users** (or the **Authorized User Groups**) tab.
3. Right-click the user (or the user group) you want to invite to enroll, and select **Send Enrollment Email** .
   The **Mail Settings** dialog box is displayed.
4. Select a **Mobile Device Manager** from the list.
   The mobile devices enrolled using this invitation are enrolled on this mobile device manager. Also, all future communications with the enrolled mobile device are managed by this mobile device manager.
5. Select the **Language** for the email.
   The user receives the enrollment invitation email in the selected language.
6. Click **OK**.
   An enrollment invitation email with a link to complete the mobile device enrollment is sent to the users.

Where to go from here

Enrolling mobile devices

Viewing information about managed mobile devices

Managing configuration profiles for managed mobile devices

Managing mobile applications

Performing remote operations on managed mobile devices

Locking BMC Client Management Agent service

From the BMC Client Management console, you can lock the **BMC Client Management Agent** service (referred as the *agent service*) after it starts. Locking the agent service prevents the local administrator from stopping or disabling it so BMC Client Management administrator has uninterrupted access to the device.

During the BMC Client Management master server installation, you can select the option to lock the agent service, and set a password to unlock the service.

During installation, if you do not select the option, you can lock the agent service later from the console.

Perform the following tasks to lock or unlock the agent service:

- Configuring lock for agent service
- Locking agent service on a specific device
- Configuring rollout to lock agent service
- Configuring operational rule to lock and unlock agent service
- Unlocking agent service

Configuring lock for agent service

If you did not select the option to lock the agent service during installation, you can enable this option from the console:

1. In the left pane, select **Global Settings** > **System Variables**.
2. In the **Security** tab, double-click any row.
3. In the **Properties** dialog box, select the **Lock new installed agent services** check box, and specify **Service Unlock Password**.
4. Click **OK** to save changes.

When a new agent service is installed on a Windows device, the service is locked after it starts.

Locking agent service on a specific device

1. In the left pane, do one of the following:
   - Select **Device Topology** > *deviceName* > **Agent Configuration** > **Security**
   - Select **Device Groups** > *deviceName* > **Agent Configuration** > **Security**
2. In the right pane, double-click any row.

3. In the **Properties** dialog box, select the **Lock the agent service** check box, and click **OK**.
   The agent service is locked on the target device.

> ⚠ You cannot lock the agent service on the master server.

Configuring rollout to lock agent service

1. In the left pane, select **Global Settings** > **Rollout** > **(your rollout)** > **Agent Configuration** > **Security**.
2. In the right pane, double-click any row.
3. In the **Properties** dialog box, select the **Lock the agent service** check box, and click **OK**.
   When the agent service is installed on a target device using this rollout, the service is automatically locked after it starts.

Configuring operational rule to lock and unlock agent service

You may need to lock and unlock the agent service when using operational rules. For example, for installing a patch, a step in the operational rule could unlock the agent service, and after other steps to install the patch are run, another step could lock the service again.

1. In the left pane, select **Operational Rules** > **(your operational rule)**.
2. In the **Step** tab, add the **Security Configuration** step.
3. In the **Properties** dialog box, ensure that the **Lock the agent service** check box is clear under **Parameters**.
   When this step is run, the agent service is unlocked.

> ⚠ **Note**
>
> A password is not required when you unlock the agent service by using the operational rule step. The operational rules use the system account to retrieve and use the encrypted service unlock password.

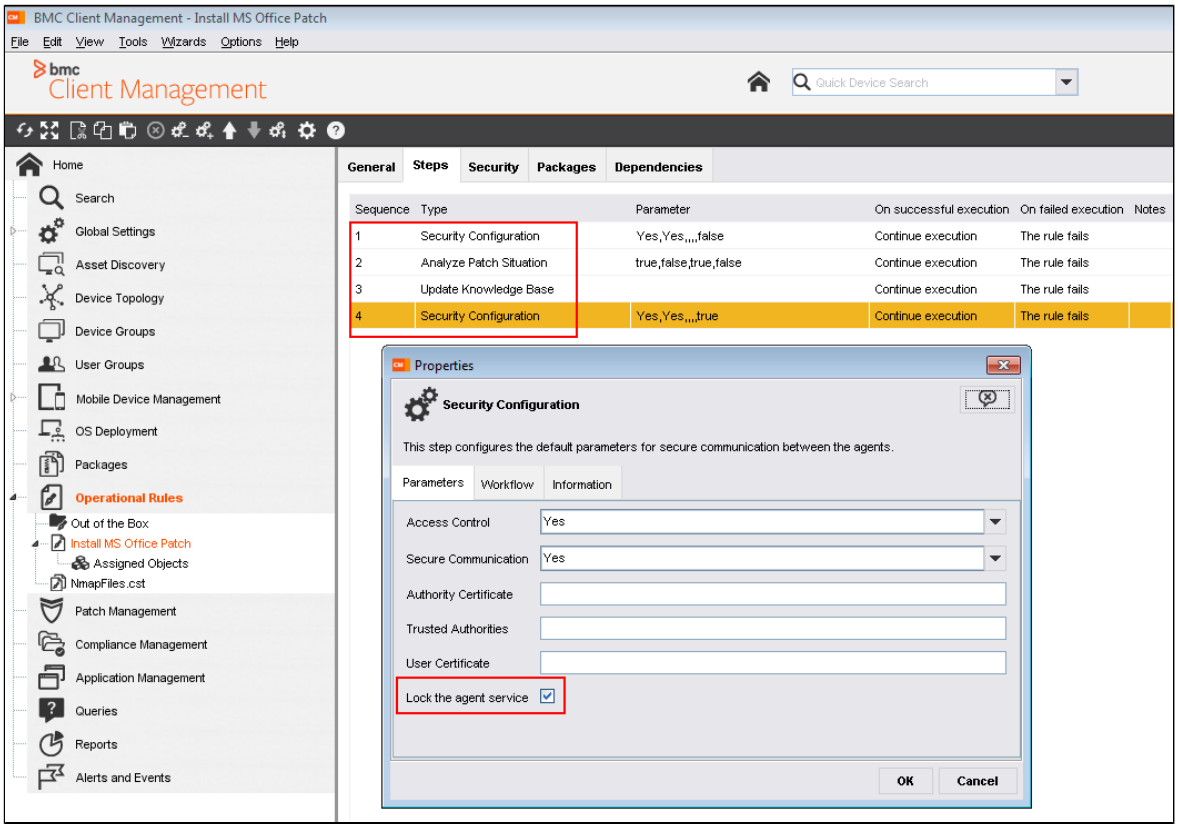
4. Add other steps as required.
5. Again add the **Security Configuration** step.

> ⚠ **Note**
>
> Add this step only after all the other steps get run that require the agent service to be stopped and after the agent service is started again.

6. In the **Properties** dialog box, ensure that the **Lock the agent service** check box is selected under **Parameters**.
7. When this step is run, the agent service is locked again.

> **Tip**
>
> You can lock the agent service on all your devices by creating an operational rule with a step to lock the agent service and assigning it to all devices.

The following screenshot displays a sample operational rule with steps to unlock and lock the agent service.



Unlocking agent service

1. In a browser, type **<*computer:port*>/service/** in the address bar and press **Enter**.
   Replace *computer* with either the IP address or computer name of the device for which you want to unlock the service.
2. Enter the local administrator or domain administrator credentials for authentication.

3. In the **Service Management for <device name>** page, enter your service management password in the **Password** field to unlock the service, and click **OK**.
   A success message is displayed indicating the agent service is unlocked. The agent service now can be stopped or disabled.

Customizing the end-user dialogs to provide a personalized experience

From BMC Client Management version 12.6 onwards, you can directly customize dialog boxes that provide product updates or acknowledgments to an end user directly through the BMC Client Management console. It enables you to deliver a personalized experience for end users. You can customize the end-user dialogs that appear for Remote Control Access, Direct Access, Operational Rules, and Patch Management.

Customizing the acknowledgment dialogs associated with Remote Control Access and Direct Access

You can customize the acknowledgment dialogs with the following attributes:

- Administrator photo
- Admin user name
- Location
- Company logo
- Remote acknowledgment timeout value

To customize dialog boxes that BMC Client Management displays for remote control access and direct access of devices:

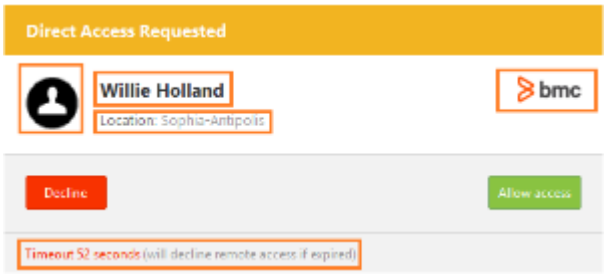
1. On the BMC Client Management console, click **Global Settings** > **Administrators** > ***admin*** > right-click **Properties**. In the **Properties** window, add the administrator photo, admin user name and location.

   ⚠ If you do not enter the **First name** and **Last name** of the administrator, the acknowledgement dialog box will display the **Login** information that was set in the **Properties** window.

> The administrator photo can be synchronized with the directory server if a picture is available on it.

2. Click **Global Settings** > **System Variables** > **Security**. Set the **Remote Access Acknowledgement Timeout (sec)** value. After the timeout value expires, you cannot take control of the device and you need to start a new remote control request for the device. If you set the timeout value to be 0, the acknowledgement dialog box never times out.
3. Click **Global Settings** > **System Variables** > **Customization**. Set the company logo that will appear on the dialog box.

   When you request remote access or direct access from the BMC Client Management console, the end user sees a customized dialog box.



Customizing the dialogs associated with Operational Rules

- You can customize the company logo on user dialogs that are associated with operational rules. When an operational rule is executed on the target device or device group, BMC Client Management displays the dialog with this customized logo.

Customizing the dialogs associated with Patch Management

- You can customize the company logo on user dialogs that are associated with patch management or application updates that need a system reboot. When a patched system needs to be rebooted, BMC Client Management displays the dialog with this customized logo.

Related topics

Managing company logo

Managing report settings

Developing

This section guides developers and application programmers through the process of customizing BMC Client Management or developing additional functionality.

The following table provides links to the relevant topics based on your goal:

Goal	Instructions
Launch console via command line	• Launching the console via command line
Launch Java Web Start console with command line options	• Launching the console via Java Web Start
Create, distribute and execute operational rules/software deployments	• Launching operational rules and software deployment through XML
Modify or unassign patch deployment	• Launching patch deployments and assigning monitoring policies through XML
Create, distribute and assign Application Management Policies	• Assigning application management policies through XML
Gather data from and exchange with the BCM database	• Integrating with the BCM database
Create customized operational rule steps	• Adding custom operational rule steps • Introduction to operational rule steps • Importing newly created steps • XML file of a step • Understanding CHL file
Execute customized actions for devices in the console	• Adding a customized menu to devices
Customize individual elements of the agent web interface	• Customizing the agent web interface • Elements of the agent interface pages • New and Extended CM HTML Tags and Parameters • Chilli in the agent interface • Tags and parameters
Customize reports	• Customizing BMC Client Management reports
Translate all elements of BMC Client Management to localized language	• Localizing BMC Client Management to an unsupported language • Localizing the console • Localizing the agent interface, reports, and emails • Translating the .locale files

Launching the console via command line

The BMC Client Management console can also be launched via the command line. In this case it can be opened directly for a specific device and at a specific functionality, such as remote control for device X.

To open the console on the **Direct Access** node of a device of your network:

1. Open a terminal window.
2. Enter the following command line to open the console on the dashboard:
   `NumaraFootprintsAssetCore.jar -u myusername -p mypassword -s 1610 -n mydevice.mycompany.com`

   If the device does not exist or you do not have sufficient rights to access it, an error message displays and the console will be opened on the dashboard.

   If `-u, -p` and `-s` are not supplied, the main login window will be displayed asking for the login and password before opening the console on the requested device /functionality.

   A device can exist under several nodes, that is under the **Device Topology** as well as in device groups under the main **Device Groups** node. When using the command line options, the console will be opened on the device node which is first returned by the search mechanism. This will always be a node under the **Device Groups** node. The console will open on the device under the **Device Topology** if the device is not a member of any group. If the search command line option is defined, the console will open on the device shown directly under the **Search** node.

   The CM console appears, and opens the hierarchy in the left panel on the **Device Groups > Your Device Group**.

Launching the console via Java Web Start

The Java Web Start (JWS) console can also be launched with command line options. It can be opened directly for a specific device and at a specific functionality, such as remote control for device X.

This topic includes:

Creating the agent interface page

BMC Client Management previews the launch of the console via JWS with different command line options, however this is not included in the software, you need to create the respective interface yourself. Following you can see an example how to do so:

1. Create a new subdirectory in the *[BMC Installation Directory]* `/master/ui directory` , for example, *jws* .
2. Create a .hchl file (for example, *demo.hchl*) and copy the code example in it.
3. Save the file in the new directory.

The new agent interface page via which the Java Web Start console can be opened is now ready to be used.

Launching the JWS agent interface

Once the agent interface page is created and stored at the proper location it can be launched via a browser.

1. Open a browser and enter the following address: `http://IPAddress:PortNumber/jws/demo.hchl`
   The agent interface page for launching the console via JWS displays in the browser.
2. Enter the required information into the boxes.
3. Select the functionality on which the console is to open by clicking the respective button, for example, **Direct Access**.

> If the device does not exist or you do not have sufficient rights to access it, an error message displays and the console will be opened on the dashboard.

> A device can exist under several nodes, that is under the **Device Topology** as well as in device groups under the main **Device Group** node. When using the command line options, the console will be opened on the device node which is first returned by the search mechanism. This will always be a node under the **Device Group** node. The console will open on the device under the **Device Topology** if the device is not a member of any group. If the search command line option is defined, the console will open on the device shown directly under the **Search** node.

The CM console appears, and opens the hierarchy in the left panel on the **Your Device> Direct Access** node either under the **Device**.

Available options

The following base options are available and can be used for opening the console via Java Web Start:

Cmd	Description
-u user	The login name of the user trying to log on. This option requires the -p option to follow providing the corresponding password. If this is not the case the login window will open requesting the password. The console will then open according to the parameters provided by the command line.
-p password	The corresponding password. This option must be used together with the -u command.
-s server: port	The master server name and port number to which the console it to connect.
-ssl sslmode	The secure mode with which the connection between the console and the master is to be established.
-n device name	The name of the device on which the console is to open. You can either list this option or the -i option to identify the device.
-i device ID	The identification of the device (the ID it is assigned in the devices table of the database) on which the console is to open. You can either list this option or the -n option to identify the device.
-search	Opens the device node under the search node.
-limited	Opens a mini console.

You can use the following options to open the console on a specific context:

Cmd	Description
-ConfigSummary/-inv	Opens the device node on the inventories subnode.
-op	Opens the device node on the assigned operational rule's subnode.
-rc	Opens the device node on the remote control subnode.
-rcd	Opens a remote control connection with the specified device.
-da	Opens the device node on the Direct Access subnode.
-FileSystems	Opens the device on the File System subnode of the Direct Access.
-Registry	Opens the device on the Registry subnode of the Direct Access.
-Services	Opens the device on the Services subnode of the Direct Access.
-Events	Opens the device on the Windows Events subnode of the Direct Access.
-Processes	Opens the device on the Process Management subnode of the Direct Access.
-Ping	

Cmd	Description
	Opens the console on the specified device and sends a ping to it. If the options -limited is used only a pop-up window will be displayed with the result of the ping operation.
-Reboot	Opens the console on the specified device and reboots it. If the options -limited is used only a pop-up window will be displayed with the result of the reboot operation.
-Shutdown	Opens the console and shuts down the device. If the options -limited is used only a pop-up window will be displayed with the result of the shutdown operation.
-Wakeup	Opens the console on the specified device and tries to wake it up. If the options -limited is used only a pop-up window will be displayed with the result of the wakeup operation.
-FileTransfer	Opens the device node with the File Transfer window already opened.

Code example of a JWS agent interface page

The following code example launches a web page in which you need to enter the required login information, such as login name, password, master and port, etc. The following line will provide a row of button via which the specific functionalities are accessed for the required device.

```
<INCLUDE htmlfile="../common/scripts/defs.hchl" onceonly>
<STYLE>
    form {
        font-family: Arial;
        font-size: 12px;
    }
</STYLE>
<SCRIPT>
    // Get keywords translations
    TranslationInfo TranslationList[]
    string szKeywords[]
    string szLine
    int i, iSize
    szKeywords <<= "_TITLE_CONSOLE_"
    szKeywords <<= "_NOTE_CONSOLE_"
    szKeywords <<= "_CONSOLE_DESC_"
    szKeywords <<= "_JRE_LINKNOTE_"
    szKeywords <<= "_JRE_LINKOTHEROS_"
    szKeywords <<= "_CONSOLE_ONECLICKINSTALL_"
    TranslationList = Translation (szKeywords)
    iSize = ArrayGetSize (TranslationList)
    szLine = "<SCRIPT language='Javascript'>" + ENDLINE
    szLine += "a = new Array (" + iSize + ");" + ENDLINE
    for (i = 0; i < iSize; i += 1)
        szLine += "a[" + i + "]=new Array (2);" + ENDLINE
        szLine += "a[" + i + "][0]=\"" + TranslationList[i+1].szKeyword + "\";" + ENDLINE
        szLine += "a[" + i + "][1]=\"" + TranslationList[i+1].szTranslation + "\";" + ENDLINE
    endfor
    szLine += "</"+"SCRIPT>" + ENDLINE
    Print (szLine)
</SCRIPT>
<SCRIPT language='Javascript'>
    function Popup (link)
    {
        window.open (link, "BmcClientManagement", "height=400, width=650, toolbar=no, menubar=no,
scrollbars=no, resizable=no, location=no, directories=no, status=no");
    }
</SCRIPT>
<FORM name='console'>
```

```
    <INPUT type='hidden' name=URL>

 <TABLE>
    <TR>
        <TD>Login:  </TD>
        <TD><INPUT type='text' name='login' size='20'>
        </TD>
     </TR>
    <TR>
        <TD>Password:  </TD>
        <TD><INPUT type='text' name='password' size='20'>
        </TD>
     </TR>
     <TR>
        <TD>Server:Port:  </TD>
        <TD><INPUT type='text' name='serverport' size='20'>
        </TD>
     </TR>
      <TR>
        <TD>SSL:  </TD>
        <TD><INPUT type='text' name='ssl' size='20' value='0'>
        </TD>
     </TR>
    <TR>
        <TD>DeviceName:  </TD>
        <TD><INPUT type='text' name='devicename' size='20'>
        </TD>
    </TR>
    <TR>
        <TD>MiniConsole:  </TD>
        <TD><INPUT type='checkbox' name='checkmini' size='20'></TD>
    </TR>
    <TR>
        <TD>Choose one context:  </TD>
    </TR>
</TABLE>
</FORM>
<SCRIPT LANGUAGE='Javascript'>
   function RefreshURL ()
   {
        if (document.forms["console"].checkmini.checked)
            document.forms["console"].URL.value="/raw/console/console.jnlp?-u=" + document.forms["console
"].login.value +"&-p=" + document.forms["console"].password.value + "&-n=" + document.forms["console"].
devicename.value + "&-s=" + document.forms["console"].serverport.value + "&-ssl=" + document.forms["conso
le"].ssl.value +"&-Limited";
        else
            document.forms["console"].URL.value="/raw/console/console.jnlp?-u=" + document.forms["console
"].login.value +"&-p=" + document.forms["console"].password.value + "&-n=" + document.forms["console"].
devicename.value + "&-s=" + document.forms["console"].serverport.value + "&-ssl=" + document.forms["conso
le"].ssl.value;
   }
</SCRIPT>
    <INPUT type='button' Value='Operational Rules' OnClick='RefreshURL ();Popup  (document.forms
["console"].URL.value +"&-op");'>
    <INPUT type='button' Value='Inventory' OnClick='RefreshURL ();Popup (document.forms["console"].URL.
value + "&-inv");'>
    <INPUT type='button' Value='Ping' OnClick='RefreshURL ();Popup (document.forms["console"].URL.value
+ "&-Ping&-Limited");'>
    <INPUT type='button' Value='Remote Control' OnClick='RefreshURL ();Popup (document.forms["console"].
URL.value + "&-rc");'>
    <INPUT type='button' Value='Registry Limited' OnClick='RefreshURL ();Popup (document.forms
["console"].URL.value + "&-Registry&-Limited");'>
    <INPUT type='button' Value='Processes' OnClick='RefreshURL ();Popup (document.forms["console"].URL.
value +  "&-Processes");'>
```

```
    <INPUT type='button' Value='Events' OnClick='RefreshURL ();Popup (document.forms["console"].URL.
value + "&-Events");'>
    <INPUT type='button' Value='Services' OnClick='RefreshURL ();Popup (document.forms["console"].URL.
value +  "&-Services");'>
    <INPUT type='button' Value='Direct Access' OnClick='RefreshURL ();Popup (document.forms["console"].
URL.value + "&-da");'>
    <INPUT type='button' Value='File Transfer' OnClick='RefreshURL ();Popup (document.forms["console"].
URL.value +"&-FileTransfer");'>
```

Launching operational rules and software deployments through XML

The entire process of creating, distributing and executing operational rules/software deployments can be accomplished within the . Alternatively you can include a XML file which contains information about:

- Assigned operational rules/packages
- Assigned devices
- Administrator with which assignment is created
- Schedule

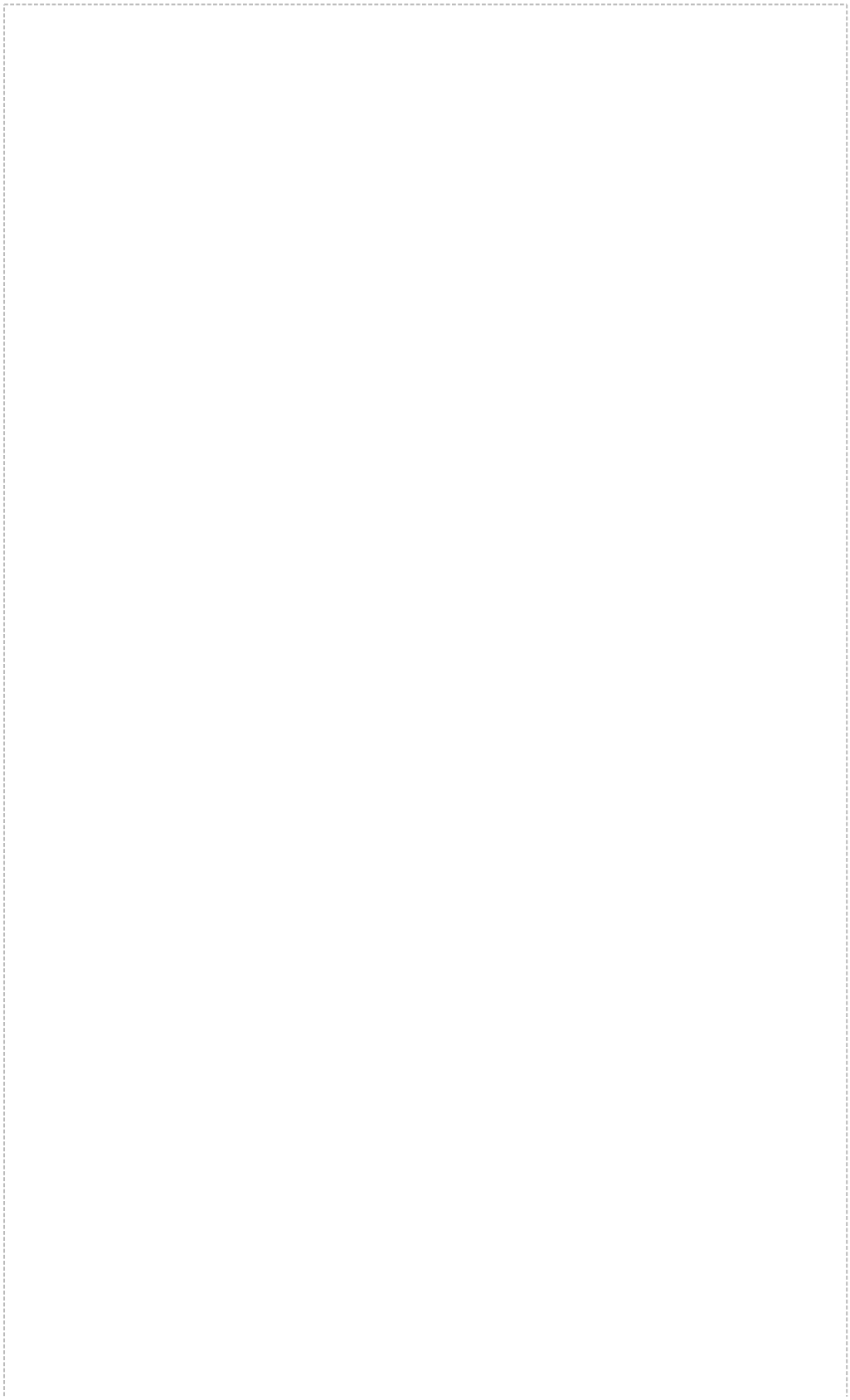
With this method you can modify operational rules/software deployments by editing the XML file without needing to have access rights to the .

1. Create an XML file with the following format:

- for operational rules:

```
<?xml version="1.0" encoding="UTF-8"?>
<RULEASSOCIATIONS>
    <!-- This section must contain the list of operational rules to assign -->
    <RULES>
        <RULE id="1001"/>             // The Rule ID/Name must be the exact value that
        <RULE name="Test Rule"/>         the rule is known in the console.
    </RULES>
    <DEVICES>
        <!-- This section must contain the list of devices to which the rules are to
                be assigned -->
        <DEVICE id="1000"/>             // The Device ID/name must be the exact value
        <DEVICE name="Device X"/>          that the device is known in the console.
    </DEVICES>
    <OPTIONS>
        <!-- When will the rule be activated (number of hours, minutes, and so on.
                Set the hours="0" to immediately activate and execute) -->
        <ADMINISTRATOR name="admin"/>
        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2011"/>
            <!--Possible value for NETWORKINSTALL: "normal", "administrative"
                and "network"-->
        <NETWORKINSTALL mode="normal" />
        </OPTIONS>
</RULEASSOCIATIONS>
```

- for software deployments:



```
<?xml version="1.0" encoding="UTF-8"?>
<PACKAGEASSOCIATIONS>
    <!-- This section must contain the list of packages to assign -->
    <PACKAGES>
        <PACKAGE id="1001"/>          // The Package ID must be the value that the package
    </PACKAGES>                             is known in the console.
    <DEVICES>
        <!-- This section must contain the list of devices to which the packages are
                assigned to-->
        <DEVICE id="1000"/>           // The Device ID must be the value that the device
is
        <DEVICE id="1002"/>               known in the console.
    </DEVICES>
    <OPTIONS>
        <!-- This section contains the optional parameters, such as the
administratorunder
                which the packages are assigned and the schedule. -->

        <ADMINISTRATOR name="admin"/>
        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2011"/>
        <!--Possible value for NETWORKINSTALL: "normal", "administrative"
                and "network"-->
        <NETWORKINSTALL mode="normal" />
    </OPTIONS>
</PACKAGEASSOCIATIONS>
```

2. Add the following step to a new or existing operational rule:
    - For operational rules: **Master Steps > Operational Rule Assignment via XML File**
    - For software deployments: **Master Steps > Package Assignment via XML File**
3. In the **Properties** dialog enter the complete path to the storage location of the XML file, as well the administrator name in the respective text boxes. This is a default administrator that will only be used if no administrator is defined in the XML file.

You created an Operational Rule which launches Operational Rules/Software Deployments through an XML file. If you want to change schedule or modify included Operational Rules /Packages/Administrator you can do so directly in the XML file without having to launch the console.

Launching patch deployments and assigning monitoring policies through XML

The entire process of creating, distributing and executing operational rules/software deployments can be accomplished within the Console . Alternatively you can include a XML file which contains information about:

- Assigned patch groups
- Assigned devices
- Administrator with which assignment is created
- Schedule

With this method you can modify patch deployments by editing the XML file without needing to have access rights to the Console .

1. Create an XML file with the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTASSOCIATIONS>
    <!-- This section must contain the list of patch groups to assign -->
    <OBJECTS>
        <!-- type can be OperationalRule, Package, PatchGroup or ApplicationList -->
        <!-- the object can be referenced with its database ID with attribute "id" -->
        <!-- or through its name with attribute "name" -->

        <OBJECT type="PatchGroup" name="Microsoft Office 2007 Patches"/>
    </OBJECTS>
    <DEVICES>
        <!-- This section contains the list of devices to which the objects are to be
                assigned -->
        <!-- Devices can be referenced with database ID (attribute "id") -->
        <!-- or name (attribute "name") -->

        <DEVICE id="1000"/>
        <DEVICE name="Device X"/>
    </DEVICES>
    <DEVICEGROUPS>
        <!-- This section contains the list of device groups to which the objects are to be
                assigned -->
        <!-- Groups can be referenced with database ID (attribute "id") -->
        <!-- or name (attribute "name") -->

        <DEVICEGROUP id="1000"/>
        <DEVICEGROUP name="My Group"/>
    </DEVICEGROUPS>
    <OPTIONS>
        <!-- Which administrator profile will be used for the assignment -->
        <ADMINISTRATOR name="admin"/>
        <!-- When will the object assignment be sent to devices (number of hours, minutes,
                etc and 0 for immediate) -->
        <!-- This only applies to OperationalRule, Package, PatchGroup object types -->

        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2011"/>
    </OPTIONS>
</OBJECTASSOCIATIONS>
```

You can mix object types in this file, that is, you can list patch groups with packages in this file, if they are all to be assigned to the same target devices and /or groups.

You can list device and/or device groups in this file, depending on the targets of the specified objects. If, for example, the objects are only to be assigned to device groups, the <DEVICES> section is not needed.

2. Add the following step to a new or existing operational rule: **Master Steps** -> **Assignment Management via XML File** .

3. In the **Properties** dialog enter the complete path to the storage location of the XML file as well the administrator name in the respective text boxes. This administrator is a default administrator that will only be used if no administrator is defined in the XML file.
4. Enter the directories into which the xml files are to be copied in case of success or error.

> If an error occurred during the assignment process you can find explanations in the *OperationalRules.log* file.

5. If you want the assignments directly activated, that is, to become operational right away, check the **Activate Created Assignment** box. If this box is left unchecked the assignments will remain paused.
6. If the newly defined assignment is to overrule any possibly already existing assignment, that is, if the object is to be reassigned with the new information, check the **Reassign if Assignment Already Exists** box. If you do not check this box and such an object assignment already exists, the original assignment will still be valid.

You created an object assignment which launches a patch deployment through an XML file. If you want to change the schedule or modify the included patch groups/application policies/administrator, you can do so directly in the XML file without having to launch the console.

Unassigning patch deployments

This step also allows you to unassign patch deployment assignments. To execute such an operation the same information is required as for the assignment process. The only difference is in the contents of the XML file: the opening and closing tag of the file use the expression <OBJECTUNASSIGN> instead of <OBJECTASSOCIATIONS>.

Example:

```
        <![CDATA[
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTUNASSIGN>
    <OBJECTS>
        <OBJECT type="PatchGroup" name="PG Test Rule"/>
    </OBJECTS>
    <DEVICEGROUPS>
        <DEVICEGROUP id="1000"/>
        <DEVICEGROUP name="My Group"/>
    </DEVICEGROUPS>
</OBJECTUNASSIGN>
```

Assigning application management policies through XML

The entire process of creating, distributing and assigning Application Management Policies can be accomplished within the Console . Alternatively you can include an XML file which contains information about:

- assigned application management policies
- assigned devices
- administrator with which assignment is created
- schedule

With this method you can modify Application Management Policies by editing the XML file without needing to have access rights to the Console .

1. Create an XML file with the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTASSOCIATIONS><!-- This section must contain the list of application rules to assign -->
    <OBJECTS>
        <!-- type can be OperationalRule, Package, PatchGroup or ApplicationList -->
        <!-- the object can be referenced with its database ID with attribute "id" -->
        <!-- or through its name with attribute "name" -->
        <OBJECT type="ApplicationList" id="1001"/>
    </OBJECTS>
    <DEVICES>
        <!-- This section contains the list of devices to which the objects are to be assigned --
>
        <!-- Devices can be referenced with database ID (attribute "id") -->
        <!-- or name (attribute "name") -->

        <DEVICE id="1000"/>
        <DEVICE name="Device X"/>
    </DEVICES>
    <DEVICEGROUPS>
        <!-- This section contains the list of device groups to which the objects are to be
assigned -->
        <!-- Groups can be referenced with database ID (attribute "id") -->
        <!-- or name (attribute "name") -->

        <DEVICEGROUP id="1000"/>
        <DEVICEGROUP name="My Group"/>
     </DEVICEGROUPS>
    <OPTIONS>
        <!-- Which administrator profile will be used for the assignment -->

        <ADMINISTRATOR name="admin"/>

        <!-- When will the object assignment be sent to devices (number of hours, minutes, and
so on, and 0 for immediate) -->
        <!-- This only applies to OperationalRule, Package, PatchGroup object types -->

        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2011"/>

        <!-- Add if type is OperationalRule and only advertizemnt is needed -->

        <ADVERTIZE/>
    </OPTIONS>
</OBJECTASSOCIATIONS>
```

You can mix object types in this file (for example,include application lists, devices and/or groups.

2. Add the following step to a new or existing operational rule: **Master Steps > Assignment Management via XML File** .
3. In the **Properties** dialog enter the complete path to the storage location of the XML file as well the administrator name in the respective text boxes. This administrator is a default administrator that will only be used if no administrator is defined in the XML file.
4. Enter the directories into which the xml files are to be copied in case of success or error.

> If an error occurred during the assignment process you can find a explanation on what happened in the *OperationalRules.log* file

> You can list device and/or device groups in this file, depending on the targets of the specified objects. If, for example, the objects are only to be assigned to device groups, the <DEVICES> section is not needed.

5. If you want the assignments directly activated, that is, to become operative right away, check the **Activate Created Assignment** box. If this box is left unchecked the assignments will remain paused.
6. If the newly defined assignment is to overrule any possibly already existing assignment, that is, if the object is to be reassigned with the new information, check the **Reassign if Assignment Already Exists** box. If you do not check this box and such an object assignment already exists, the original assignment will still be valid.

You created an object assignment which launches the management of application lists through an XML file. If you want to change the schedule or modify the included patch groups/application policies/administrator you can do so directly in the XML file without having to launch the console.

Unassigning application list

This step also allows you to unassign application list assignments. To execute such an operation the same information is required as for the assignment process. The only difference lies in the contents of the XML file: the opening and closing tag of the file use the expression <OBJECTUNASSIGN> instead of <OBJECTASSOCIATIONS>. **Example:**

```
       <![CDATA[
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTUNASSIGN>
    <OBJECTS>
        <OBJECT type="ApplicationList" name="Prohibiting Pinball"/>
    </OBJECTS>
    <DEVICEGROUPS>
        <DEVICEGROUP id="1000"/>
        <DEVICEGROUP name="My Group"/>
    </DEVICEGROUPS>
</OBJECTUNASSIGN>
```

Integrating with the BCM database

Third party applications can gather data from and exchange with the BCM database via REST (Representational State Transfer) API. For detailed integration with the BMC Client Management database via the web API and its REST operations, see *BMC Client Management - Web API Operations for Integrating with BMC Client Management* manual which explains its usage and all its available operations in detail.

The Entity Relationship diagrams include a description of each table and lists of columns grouped in subject areas. To download the BMC Client Management 12.5 Data Model ZIP file, click here .

> **Note**
>
> The entire package is required to view the data model content.

To view the data model

1. After downloading the file, save it to a new folder.
2. Extract the files.
3. Launch the **BMC Client Management 12.5.htm** file.
   The **BMC Client Management 12.5.htm** file fetches the different pages in the main page from the underlying folders in the **BMC_Client_Management_12.5_DataModel** folder.

Adding custom operational rule steps

BMC Client Management provides a large number of predefined steps for operational rules. However, you can create customized operational rule steps. The following topics are provided:

- Introduction to operational rule steps
- Importing newly created steps
- XML file of a step

- Understanding CHL file

Introduction to operational rule steps

BMC Client Management software includes a large number of predefined operational rule steps which are located in the `data/Vision64Database/opsteps` directory. In this directory CM expects to find pairs of files: an `.xml` file describing an individual operational step and a `.chl` file which is the script to execute for the step.

Upon finding such a pair, the .xml file is parsed to see if a new step can be imported into the database. If the .xml file is wrong, both files remain where they are and nothing happens. If it is correct, the script it points to is compiled using the local **Operational Rules** module. If the compile passes, the step is added to the database and the two files are placed in a specified directory structure under `opsteps` . This allows a history to be kept of all versions of this specific step. If the compile fails, the files are moved to a directory called `opsteps.invalid` . The reason for the failure is described in the `chilli.log` file. For more information, refer to the debug chapter of the **Chilli Reference** manual.

A step always needs two files:

- a `<StepName>.xml` file describing an individual operational step and
- a `<StepName>.chl` file which is the script to execute for the step

Custom operational rule steps can be added to CM by simply creating the necessary scripts and adding them to the respective directory. The operational rules steps can easily be localized for different languages if necessary. The following paragraphs explain the contents of both the .xml and .chl file, and how to create your own steps. In the following topic you can see some examples of custom operational rule steps for specific needs and situations.

Importing newly created steps

Steps can be added to CM at any time. Once their scripts are created and copied in the proper location on the master, they can be directly imported in the console. To import steps:

1. Put the files (.xml and .chl) for the new steps in the directory data/Vision64Database /opsteps.
2. Select the **Tools** -> **Import New Steps**  menu item.
3. Specify in the **Schedule Import of New Steps** window if the import is to be launched immediately or if it is to be fixed for a specific date and time by entering the values in the respective boxes.
4. Click **OK** to confirm the schedule and close the window.

Any new steps that are located in the source directory will be imported into the BCM database at the specified time.

XML file of a step

The .xml file is the "link" between the actual action which will be executed by the Chilli script and the operational rule step action's definition in the console. It contains a general description the step, calls the Chilli script, and provides the parameters to the console that need to be defined and then passed on to the script for execution. These are the parameters displayed in the **Properties** window of the **Select a Step** dialog in which you enter the values.

The following examples are included:

- Example 1
- Example 2
- Example 3
- Example of a complete XML File

The following general rules apply for the xml tags:

- None of the xml tags is allowed parameters.
- All tags must have an opening and an end tag.

For the XML file, you can use the following elements. Their relation is indicated in the table by indentation, for example, PARAM is a child of PARAMS and a parent of LABEL.

> **Note:**
>
> Be aware that the xml file must always start with the processing instruction: `<?xml version="1.0"?>`

Name	Description	Required
STEPTYPE	The root element. It has no parameters. The only allowed tags within this element are CLASS, NAME, SCRIPT, NOTE and PARAMS.	Yes
CLASS	The name of the step class to which this step belongs. A step class is a container for a number of steps concerning a specific topic, such as Agent Configuration, Directory and File Handling or User Message Box. You can enter either a hardcoded text such as Tools or a keyword, such as *DB_STEPCLASS_TOOLS*.	Yes
NAME	The name of the step. You can enter either a hardcoded text such as Add Line or a keyword, such as *DB_STEPNAME_ADDLINE*.	Yes
SCRIPT	The name of the Chilli script which corresponds to the .xml file, in this example `addline.chl` .	Yes
NOTE	Additional information such as a short description of the step. You can enter either a hardcoded text such as Add a line to a file or a keyword, such as *DB_STEPNOTE_ADDLINE*.	No
PARAMS	Container for the parameters. If the step doesn't have any parameters, leave this element empty.	Yes

Name	Description	Required
PARAM	Container for a single parameter.	No
NAME	The name of the Chilli variable as listed in the CHL script.	If child of PARAM
LABEL	The label of the previously defined Chilli variable. This label displays in the **Properties** dialog when adding the step. You can enter either a hardcoded text or a keyword.	If child of PARAM
TYPE	The type of the parameter. Possible values are: • String: parameter will be represented as a text field where you can enter a sequence of characters • Integer: parameter will be represented as a text field where you can only enter integers • Text: parameter will be represented as a multi-line text field • Boolean: parameter will be represented as a check box • Enum: parameter will be represented as a drop-down list. In this case ENUMGROUP, ENUMTYPE and ENUMVALUE must also be specified. • ObjectType: parameter will be represented as a text field in which objects of a specific type can be added. In this case the OBJECTTYPE, OBJECTTYPEMEMBER, OBJECTTYPEGROUP and OBJECTTYPENBOFITEMS must also be specified.	If child of PARAM
DEFAULT	The default value if one is proposed for the parameter. If no default is proposed, leave this element empty.	If child of PARAM
ENUMGROUP	The name of the enumeration under which it is stored in the database (for example, ***FirewallProfiles***).	If TYPE has the value ENUM
ENUMTYPE	The type of the items of the drop-down list. Possible values are: • String: items are a sequence of characters • Integer: items are integers • Boolean: two items Yes and No	If TYPE has the value ENUM
ENUMVALUE	The values of the items of the drop-down list. All values need to be separated by a comma, for example, ***ZIP, PKG*** . You can enter either a hardcoded text or a keyword.	If TYPE has the value ENUM
OBJECTTYPE	The type of the object which can be selected (that is, ***_DB_OBJECTTYPE_DEVICE_*** if devices and device groups can be selected).	If TYPE has the value ObjectType
OBJECTTYPE-MEMBER	Defines if the **Select Objects** dialog displays the individual objects of the specified object type (for example, devices or operational rules). Possible values are: • 1: objects are displayed • 0: objects are not displayed If both OBJECTTYPEMEMBER and OBJECTTYPEGROUP are set to 0this option will automatically be considered as set to 1.	If TYPE has the value ObjectType
OBJECTTYPE-GROUP		

Name	Description	Required
	Defines if the **Select Objects** dialog also displays the groups or folders of the selected object type (for example, device groups or operational rule folders). Possible values are: • 1: objects are displayed • 0: objects are not displayed	If TYPE has the value ObjectType
OBJECTTYPE-NBOFITEMS	Defines the number of objects that can be added to the list. If set to 0, an unlimited number of objects can be added.	If TYPE has the value ObjectType
OPTIONAL	Defines that the parameter is optional. In this case a check box is added before the actual parameter field which must be checked to activate the actual parameter	No
DEFAULT-PRESENCE	Defines if the OPTIONAL box before the parameter field is checked by default, that is, if the parameter is activated by default.	If OPTIONAL is present

The following paragraphs provide you with a number of examples for the previously explained tags. The examples are shown in two versions, once with keywords to be localized and once with hardcoded text if no localization is required. For information about how to localize your steps see the Localizing BCM to an Unsupported Language topic.

Example 1

The following is an excerpt of a script collecting values from an .ini file and placing these in the Custom Inventory, this parameter defines the path to the configuration file from which the value is to be recovered, using keywords:

```
<PARAM>
    <NAME>IniFilePath</NAME>
    <LABEL>_DB_STEPPARAM_INIFILEPATH_</LABEL>
    <TYPE>String</TYPE>
    <DEFAULT></DEFAULT>
</PARAM>
```

whereby `IniFilePath` is internal Chilli variable name for the `DB_STEPPARAM_INIFILEPATH` step label, the variable is of type string and does not have any preentered default value.

Following you can see the same example using hard coded text instead of keywords:

```
<PARAM>
    <NAME>IniFilePath</NAME>
    <LABEL>File Path</LABEL>
    <TYPE>String</TYPE>
    <DEFAULT></DEFAULT>
</PARAM>
```

Example 2

The following parameter tag defines a drop-down list box from which a choice must be made:

```
<PARAM>
    <NAME>Protocol</NAME>
    <LABEL>_DB_STEPPARAM_PROTOCOL_</LABEL>
    <TYPE>Enum</TYPE>
    <ENUMGROUP>FirewallProtocol</ENUMGROUP>
    <ENUMTYPE>String</ENUMTYPE>
    <ENUMVALUE>TCP, UDP</ENUMVALUE>
    <DEFAULT>TCP</DEFAULT>
</PARAM>
```

whereby `Protocol` is internal Chilli variable name for the `DB_STEPPARAM_PROTOCOL` step label, the ENUMGROUP defines that the parameter is to be found in the database in the *FirewallProtocol* column, the enumeration is of type `String` , its values are `TCP` and `UDP` and the prepopulated default value is the `TCP` protocol. Following you can see the same example using hard coded text instead of keywords:

```
<PARAM>
    <NAME>Protocol</NAME>
    <LABEL>Protocol</LABEL>
    <TYPE>Enum</TYPE>
    <ENUMGROUP>FirewallProtocol</ENUMGROUP>
    <ENUMTYPE>String</ENUMTYPE>
    <ENUMVALUE>TCP, UDP</ENUMVALUE>
    <DEFAULT>TCP</DEFAULT>
</PARAM>
```

Example 3

The following set of tags defines a list box in which a number of devices and device groups can be selected:

```
<PARAM>
    <NAME>Objects</NAME>
    <LABEL>_DB_STEPPARAM_OBJECTOFTYPEDEVICEORDEVICEGROUP_</LABEL>
    <TYPE>ObjectType</TYPE>
    <OBJECTTYPE>_DB_OBJECTTYPE_DEVICE_</OBJECTTYPE>
    <OBJECTTYPEMEMBER>1</OBJECTTYPEMEMBER>
    <OBJECTTYPEGROUP>1</OBJECTTYPEGROUP>
    <OBJECTTYPENBOFITEMS>0</OBJECTTYPENBOFITEMS>
    <DEFAULT/>
</PARAM>
```

whereby `Objects` is internal Chilli variable name for the `DB_OBJECTTYPE_DEVICE` step label, the list has no default object entered, individual objects, that is, *devices* , as well as group objects, that is, *device groups* , can be selected and the list is unlimited.

Following you can see the same example using hard coded text instead of keywords:

```
<PARAM>
    <NAME>Objects</NAME>
    <LABEL>Devices and/or Device Groups</LABEL>
    <TYPE>ObjectType</TYPE>
    <OBJECTTYPE>_DB_OBJECTTYPE_DEVICE_</OBJECTTYPE>
    <OBJECTTYPEMEMBER>1</OBJECTTYPEMEMBER>
    <OBJECTTYPEGROUP>1</OBJECTTYPEGROUP>
    <OBJECTTYPENBOFITEMS>0</OBJECTTYPENBOFITEMS>
    <DEFAULT/>
</PARAM>
```

Example of a complete XML File

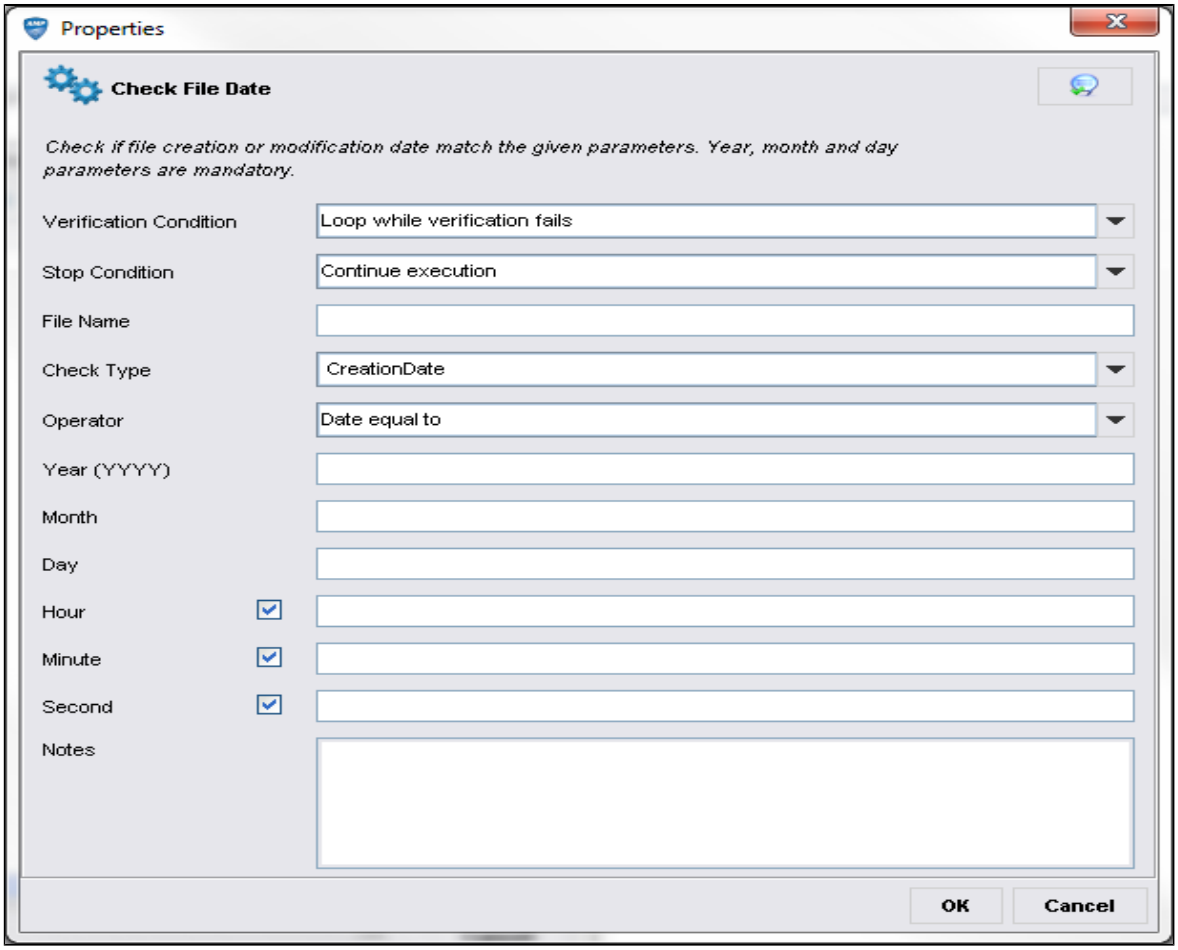
The following example shows the code of an XML file as well as what the step looks like in the Console .

This is the code of the checkfiledate.xmlfile of the predefined step **Check File Date** :

```
<?xml version="1.0"?>
<STEPTYPE>
    <CLASS>_DB_STEPCLASS_MONITORING_</CLASS>
    <NAME>_DB_STEPNAME_CHECKFILEDATE_</NAME>
    <SCRIPT>checkfiledate.chl</SCRIPT>
    <NOTE>_DB_STEPNOTE_CHECKFILEDATE_</NOTE>
    <PARAMS>
        <PARAM>
            <NAME>FileName</NAME>
            <LABEL>_DB_STEPPARAM_FILENAME_</LABEL>
            <TYPE>String</TYPE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>CheckType</NAME>
            <LABEL>_DB_STEPPARAM_CHECKTYPE_</LABEL>
            <TYPE>Enum</TYPE>
            <ENUMGROUP>CheckType</ENUMGROUP>
            <ENUMTYPE>String</ENUMTYPE>
            <ENUMVALUE>ModificationDate, CreationDate</ENUMVALUE>
            <DEFAULT>CreationDate</DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>CheckDateRange</NAME>
            <LABEL>_DB_STEPPARAM_CHECKDATERANGE_</LABEL>
            <TYPE>Enum</TYPE>
            <ENUMGROUP>CheckDateRange</ENUMGROUP>
            <ENUMTYPE>String</ENUMTYPE>
            <ENUMVALUE>_DB_STEPPARAM_DATELESSTHAN_,_DB_STEPPARAM_DATEGREATERTHAN_,
            _DB_STEPPARAM_DATEEQUALORGREATERTHAN_,_DB_STEPPARAM_DATEEQUALORLESSTHAN_,_
            DB_STEPPARAM_DATEEQUAL_,_DB_STEPPARAM_DATENOTEQUAL_</ENUMVALUE>
            <DEFAULT>_DB_STEPPARAM_DATEEQUAL_</DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Year</NAME>
            <LABEL>_DB_STEPPARAM_YEAR_</LABEL>
            <TYPE>Integer</TYPE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Month</NAME>
            <LABEL>_DB_STEPPARAM_MONTH_</LABEL>
            <TYPE>Integer</TYPE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Day</NAME>
            <LABEL>_DB_STEPPARAM_DAY_</LABEL>
            <TYPE>Integer</TYPE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Hour</NAME>
            <LABEL>_DB_STEPPARAM_HOUR_</LABEL>
            <TYPE>Integer</TYPE>
            <OPTIONAL>true</OPTIONAL>
            <DEFAULTPRESENCE>false</DEFAULTPRESENCE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Minute</NAME>
            <LABEL>_DB_STEPPARAM_MINUTE_</LABEL>
            <TYPE>Integer</TYPE>
```

```
            <OPTIONAL>true</OPTIONAL>
            <DEFAULTPRESENCE>false</DEFAULTPRESENCE>
            <DEFAULT></DEFAULT>
        </PARAM>
        <PARAM>
            <NAME>Second</NAME>
            <LABEL>_DB_STEPPARAM_SECOND_</LABEL>
            <TYPE>Integer</TYPE>
            <OPTIONAL>true</OPTIONAL>
            <DEFAULTPRESENCE>false</DEFAULTPRESENCE>
            <DEFAULT></DEFAULT>
        </PARAM>
    </PARAMS>
</STEPTYPE>
```

This is what the step looks like in the Console :



Notice that all keywords in the code were replaced by their english translations. **Verification Condition** , **Stop Condition** and **Notes** . Parameters with different values for the TYPE elements are displayed in the following way:

- String: a free text box
- Boolean: a check box
- Integer: a text box in which only numbers can be entered

- Enum: a drop-down list with several options defined via the ENUMVALUE tag.
- Optional: a check box before the actual data box, the DEFAULTPRESENCE parameter defines if it is checked by default.

Understanding CHL file

This topic includes:

What is a CHL file?

A CHL file is script that executes the desired action(s). It is written in Chilli, the BMC Software proprietary programming language.

What is the structure of a CHL file?

A CHL file has the following structure:

Description

Contains information about the script, version, creation date, programmer, and so on.

```
#########################################################################
# CustomPackagerModuleSetup
# Modify the Custom packager module parameters
#
#########################################################################
```

Global variables

Similar to other programming languages Chilli uses global variables. You can call any number and type of external variables, however be aware that the following two are mandatory for all step scripts:

- StepParamsContainer: contains the values of all parameters defined by the step

- RuleParamsContainer: contains general information about the **Operational Rule** the step is added to. It can be used by the steps to communicate with each other if an **Operational Rule** contains more than one step.

```
#### The Rule container can be used by steps to communicate with each other.

extern ContainerHandle StepParamsContainer, RuleParamsContainer
```

Local variables

The value of the NAME elements of parameters defined in the XML file need to be defined as local variables in the CHL file.

Following you find the example of the predefined step **Custom Package Module Setup** which demonstrates how the parameters in the XML and CHL files are linked:

```
<PARAMS>
     <PARAM>
         <NAME>PackageExtension</NAME>
         <LABEL>_DB_STEPPARAM_PACKAGEEXTENSION_</LABEL>
         <TYPE>String</TYPE>
         <DEFAULT>.zip</DEFAULT>
     </PARAM>
     <PARAM>
         <NAME>MaxRetry</NAME>
         <LABEL>_DB_STEPPARAM_MAXRETRY_</LABEL>
         <TYPE>Integer</TYPE>
         <DEFAULT>5</DEFAULT>
     </PARAM>
     <PARAM>
         <NAME>RetryInterval</NAME>
         <LABEL>_DB_STEPPARAM_RETRYINTERVAL_</LABEL>
         <TYPE>Integer</TYPE>
         <DEFAULT>300</DEFAULT>
     </PARAM>
 </PARAMS>
```

custompackagermodulesetup.xml

```
#### Our parameters to be found in StepParamsContainer:
const PACKAGERCUSTOM_PARAM_PACKAGEEXTENSION   "PackageExtension"
const PACKAGERCUSTOM_PARAM_MAXRETRY           "MaxRetry"
const PACKAGERCUSTOM_PARAM_RETRYINTERVAL      "RetryInterval"
const ERROR_CODE                              "ErrorCode"

const PARAM_NAME                              "Name"
const PARAM_PERSISTENT                        "Persistent"
const PARAM_STATE                             "State"
const PARAM_STATE_INITIALISE                  1
const ACTIONDB_ERROR_DUPLICATE                11
```

custompackagermodulesetup.chl

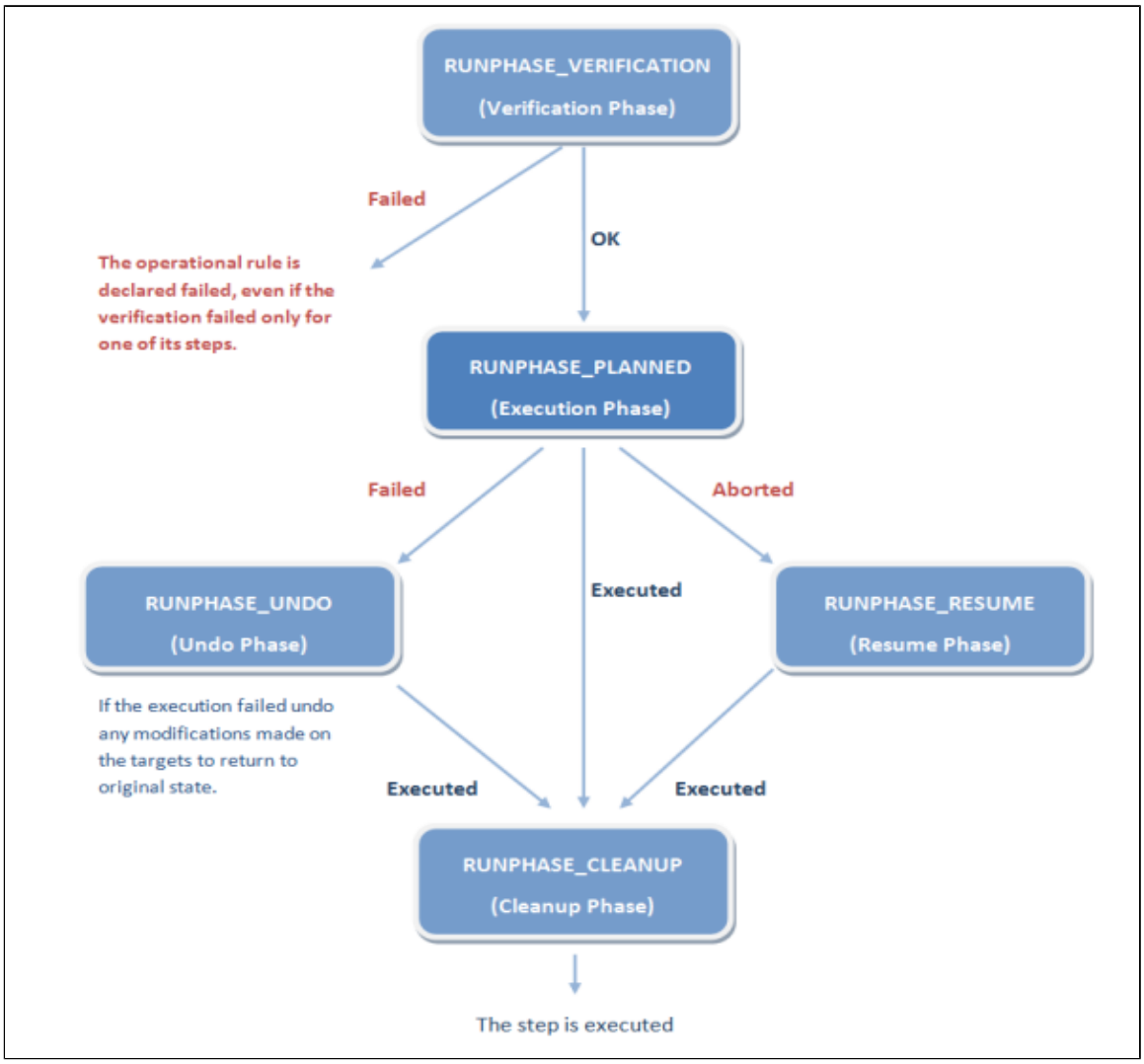
Notice how the three NAME elements PackageExtension, MaxRetryand RetryIntervalare defined in the CHL file. Additionally you find the five local variables ERROR_CODE, PARAM_NAME, PARAM_PERSISTENT, PARAM_STATE, PARAM_STATE_INITIALISEand ACTIONDB_ERROR_DUPLICATEwhich are used later on in the Main procedure.

Custom defined procedures

code that is defined once in the script and can be executed as often as needed by other parts of the script or program

Main procedure

The main procedure follows the same basic rules as in other programming languages. However, due to the functioning of the operational rules module the Main procedure must be divided into runphases. There are 5 different runphases, of which the RUNPHASE_PLANNEDis mandatory. The operational rules module will not execute step scripts which do not at least contain this runphase. Also all individual operations are required to return either 0 for successful execution or non-zero for failed.The process of executing an operational rule containing three steps for example is as follows:



RUNPHASE_VERIFICATION

The verification phase verifies if all prerequisites for the execution of the steps are given, that is, it verifies for the correct operating system, if the environment variable or the registry key exists, etc. The process verifies the steps in the order in which they are defined. If the verification of all steps returns OK, the script passes on to RUNPHASE_PLANNED. If the verification fails, the **Operational Rule** is cancelled.

RUNPHASE_PLANNED

This phase is the actual execution phase of the script. It executes one step after the other in the defined order. This phase can have one of the following results:

- If all steps are successfully executed, the script passes to RUNPHASE_CLEANUP
- If execution failed, the script passes to RUNPHASE_UNDO
- If execution is stopped due to a "non-execution" problem such as the CM agent crashing or the computer shutting down, the script passes to RUNPHASE_RESUMEat the next CM agent startup.

RUNPHASE_UNDO

This phase is used to undo all changes executed via the steps if the execution of the **Operational Rule** fails. After the undo the device will be in exactly the same state and situation as before the execution of the **Operational Rule** .

RUNPHASE_RESUME

If execution is stopped due to a "non-execution" problem such as the CM agent crashing or the computer shutting down, at the next CM agent this phase will check the **Operational Rule** and verify which of its steps it finished executing. It will then proceed to re-execute the step at which the execution was interrupted, and run all remaining steps.

RUNPHASE_CLEANUP

This last phase cleans up the device , for example, deleting the MSI file used for a software installation.

How does Chilli work?

Chilli is a procedural programming language, combining the features of BASIC and C as well as some C++ concepts into a flexible computer language. This powerful script language is a self-contained stand-alone language with its own compiler. For in-depth information about Chilli consult the ***Chilli Reference*** .

Adding a customized menu to devices

When right-clicking an object in the left or right window pane, a context menu opens. The available items in the menu depend on the object and the position in the console . You can expand options for devices by adding a **Customized Menu**.

This topic includes:

A **Customized Menu** is an additional menu for devices in the Console with which you can quickly execute customized actions. You can create one **Customized Menu,** which comprises three different item types:

- **Executable**: Launchs an executable file
- **HTTP**: Opens a web page in the browser
- **Command Line**: Executes a command in the command line

In the console, you can find a **Customized Menu** in different places. To execute an existing **Customized Menu** item, in the left window pane right-click a device and select the **Customized Menus** option.

The icon next to a **Customized Menu** item indicates its type:

-  = **Executable**

- = **HTTP**
- = **Command Line**

Creating a customized menu

1. Go to **Global Settings> System Variables** and ensure that the **Device Menu** tab is selected.
2. Click **Create Device Menu** .
   The **Properties** dialog box appears.
3. From the **Menu Type** drop-down list, select the item type and fill in the two text boxes.
   The following three examples illustrate possible applications:

Example	Name	Value	Menu Type
Example 1	Open ***your web page***	http://www. ***yourwebpage*** .com	**HTTP**
Example 2	Open Editor	C:/Windows/notepad.exe	**Executable**
Example 3	Open Registry Editor	regedit.exe	**Command Line**

4. Click **OK** .
   The dialog closes and the new **Customized Menu** item is listed in the right window pane.
   You can add more items by repeating the steps.

Launching a customized menu

After creating a new **Customized Menu**, you can launch its items.

1. In the left window pane, right-click a device .
2. In the context menu, select **Customized Menus** and click the item you created.
   The defined operation is executed.

You launched a **Customized Menu** item. You can access your **Customized Menu** from any device in the left window pane.

Customizing the agent web interface

The following topics describe the individual elements of the Agent Web interface. . This section begins with information about the HCHL pages in general and specific information about HCHL for the agent pages in particular:

- Elements of the agent interface pages
- New and Extended CM HTML Tags and Parameters
- Chilli in the agent interface
- Tags and parameters

The pages for the agent interface are designed exclusively in standard HTML 4.0, the BMC Software extended tags and parameters, and Chilli, a proprietary BMC Software programming language. See the BMC Software Chilli Reference Guide for detailed information. The following

instructions assume you are already familiar with standard HTML 4.0. This section explains in detail tags and parameters specifically designed by BMC Software for the optimally run the agent interface.

Elements of the agent interface pages

The basis for the web page (HCHL) files of the CM agent Interface is standard HTML 4.0. However, for optimal execution of the CM agent Interface, the functionalities for several standard tags were extended (for example, new parameters, tags were created). Another important element in the handling of the HCHL files are headers. Some adjustments were made to the headers for the easy manipulation of the interface. The following paragraphs and topics describe in detail the use and concepts for the following basic elements of the CM agent Interface pages:

- **BMC Software Tags**
  The basis of all CM agent Interface pages is standard HTML 4.0. However, because the Agent Interface has some very specific needs, existing HTML tags were given extended functionalities, such as the capability to handle Chilli expressions., New tags and parameters were created where necessary
- **Chilli in the CM agent Interface**
  Chilli is used in the Agent Interface to execute repetitive and automated tasks through scripts. These scripts can be called through the new the command line. In addition to the script being called, further parameters can be specified within the tag's arguments. These Chilli functions are explained in more detail in later topics. References to the *Chilli Reference* guide will be made where further explain an item.

New and Extended CM HTML Tags and Parameters

The basis for the HTML files of the BMC Client Management is standard HTML 4.0. However, for the agent Web interface to run optimally, several standard tags were extended in their functionalities (for example, by adding parameters and new tags). This reference assumes that you are already familiar with standard HTML 4.0.

HTML Tags

BMC Software extended standard tags:	New BMC Software tags:
A (Anchor)	Deftag
Form	IF/ELSE
Script	Include
	Loop
	Setvar

The difference between these two groups of tags is that the new BMC Software tags are completely newly created tags, as well as the parameters they use. The Extended Tags are standard HTML 4.0 tags with additional parameters to extend their functionality, which will be explained in detail later in this reference.

In principle, the new and extended tags follow the general rules of standard HTML tags, which have three parts:

- a start tag
- the content
- an end tag

Standard tag syntax

```
<TAG parameter1=value1, parameter2=value2, ....>Content</TAG>
```

A tag is special text ("markup") that is delimited by angle brackets ("<" and ">"). An end tag includes a forward slash ("/") after the left angle bracket ("<"). For example, the anchor tag "A" has a start tag, "<A>", and an end tag, "</A>". The start and end tags surround the content of the anchor tag: `<A>http://www.metrixsystems.com</A>`

Some tags do not have an end tag, and this will be explicitly mentioned in the respective section. Tag names are always case-insensitive, so <setvar>, <Setvar>, and <SETVAR> are all the same.

Chilli and HTML tags

One of the principal functionalities of all BMC Software extended or created tags is the possibility to directly handle Chilli expressions. (Chilli is a programming language created by BMC Software specifically for the purpose of network and systems management. For more information about Chilli, refer to the Chilli Reference guide.)

BMC Client Management tag syntax

```
<TAG parm1=(Chilli Expression) parm2=....>Text</TAG>
```

Chilli expressions can be used as values of HTML tag parameters. They are enclosed in parentheses to distinguish them from "normal" parameter values. When the parser finds an opening parenthesis at the beginning of the parameter value, it will evaluate everything in the parentheses as a Chilli expression.

Parameters

To further extend the functionality of standard HTML 4.0 tags, as well as those of the tags newly created by BMC Software, the following parameters were added to the previously mentioned tags:

Parameter Name	Used by Tags
condition	IF/ELSE, INLCUDE, LOOP
htmlfile	A, FORM, INCLUDE
language	SCRIPT
Name	DEFTAG, SETVAR
onceonly	INLCUDE
parseoutput	DEFTAG, SCRIPT
proc	DEFTAG
value	SETVAR
vars	A, SCRIPT

A tag's parameters define various properties for the tag. For example, the IMG element takes an SRC parameter to provide the location of the image and an ALT parameter to give alternate text for users who disabled image autoloading:

```
<IMG SRC="bmcsoftwarelogo.png" ALT="BMC Software Logo">
```

A parameter is included in the start tag only - never the end tag - and takes the form parameter name="parameter-value". The 'name=value' pairs are separated from each other by a space (and no comma). The parameter value is enclosed by single or double quotes if it consists of more than one word. For example, when listing variables: vars='iid, myvar, secondvar'. If the value is a one-word-expression, it does not need to be put in quotes. The parser does not distinguish between single and double quotes, so either of them can be used. If quotes are used when not needed, the parser will ignore them. Parameter names are case-insensitive, but parameter values are case-sensitive.

Chilli in the agent interface

Chilli is a procedural programming language, combining the features of BASIC and C, as well as some C++ concepts into a flexible computer language. This powerful script language is a stand-alone language with its own compiler.

Chilli is used in the CM agent Web Interface to execute repetitive and automated tasks through scripts integrated into its HCHL pages. These scripts can be called through the new BMC Software extended tags or via the command line. Additional parameters can be specified with the script to be called within the tag's arguments. How these Chilli functions are called is explained in more detail in the topics on the respective tags later in this reference.

Below are some examples of a tag including Chilli.

Example 1

```
<SETVAR name=CountModels value=(ArrayGetSize (NaviLoopModelList.ExpModelDescList))>
```

In this example a Chilli function, ArrayGetSize with its argument, is used as the value for the value parameter of the BMC Software specific SETVAR tag.

Example 2

```
<SCRIPT language=chilli>
    if (defined ('_wpcolor'))
        if(_wpcolor != "")
            UserSettingSetValue (REMOTE_USER, "Prop/WpColor", _wpcolor)
        endif
    endif
</SCRIPT>
```

In this example a Chilli script is executed through the SCRIPT tag, where the language parameter is defined as the Chilli scripting language.

Chilli Functions in the CM agent Interface

The Chilli language was extended for the CM agent Interface with some additional function modules. However, almost all existing modules either are or can be used with it.

Functions of the following general Chilli modules are used by the CM agent Interface:

- File
- SNMP
- String
- Miscellaneous
- HTML File
- CSV File
- Gif Image Manipulation
- Variable Manipulation
- DBM Database

As this reference concentrates on the CM agent Interface specific elements, it will not explain any Chilli functions. For more information about these refer to the BMC Software Chilli Reference guide. This guide includes detailed information about the Chilli language in general, as well as the overall possibilities and functionalities of all Chilli functions.

Tags and parameters

The following topics describe in detail all standard HTML 4.0 tags which were extended by BMC Software to allow for additional functionality, as well as all HTML tags specifically created by BMC Software for the purpose of a smooth and uncomplicated execution of the CM agent interface. It is a complete reference to all changed and new tags and parameters of the CM agent interface. There are also a number of examples showing the typical use and manner of application of these tags and parameters.

The following tags and parameters are available:

- A (Anchor Tag)
- DEFTAG
- FORM

- IF
- INCLUDE
- LOOP
- SCRIPT
- SETVAR

These topics only explains the special BMC Client Management agent interface tags and extended tags. They are all based on standard HTML version 4.0. If you are not familiar with HTML yet, it is recommended you refer to a standard HTML guide first.

A (Anchor Tag)

The A tag denotes an *anchor* - a hypertext link or the destination of a link. This section will only deal with the additional functionalities of the anchor tag created by BMC Software. For more information about the anchor tag's standard functions refer to a general HTML 4.0 reference. Contrary to the general anchor tag of the standard HTML versions, the BMC Software extended anchor tag does not use the *href* parameter to define links in the source file. It uses a tag called `htmlfile` with additional parameters and variables to pass the necessary information about to the Chilli programming language. Chilli will then translate this information into the standard *href* parameter.

Start Tag	required
End Tag	required
Syntax	`<A htmlfile='file name' [vars='variable names']></A>`

Mandatory Parameters

htmlfile	The htmlfile parameter defines the file to be displayed next on the screen.

Optional Additional Parameters

vars	The anchor tag can also mention variables (vars) to be passed through to the scripts included in the HTML file.

htmlfile

The BMC Software extended anchor tag expects the htmlfile parameter to define the file to be displayed on the screen. The file path can either be relative to the current directory or absolute.

Example

You can use any Chilli supported operations, specified within parentheses, so that the htmlfile parameter is calculated. For instance, if_hchldirequals to"/myhchl", then the following anchor tag in an HCHL page:

```
<A htmlfile=(_hchldir + "/editquery/editquery_utils.hchl")>
```

will be translated by the parser into the following:

```
<A href="/myhchl/editquery/editquery_utils.hchl">
```

vars

The anchor tag can also specify a list of variables (vars) to be passed through to the next script.

DEFTAG

The DEFTAG tag provides a means for agent interface developers to define their own tags that call user-defined Chilli procedures. (The majority of commands in the agent interface are executed through Chilli scripts.)

Start Tag	required
End Tag	forbidden
Syntax	`<DEFTAG name='tag name' 'proc='procedure name' [parseoutput]>`

Mandatory Parameters

name	The name of the tag to be defined.
proc	The name of the Chilli procedure which will handle the tag when it is encountered in an HCHL file (=calling a Chilli procedure).

Optional Additional Parameters

parseoutput	Defines if the output of the execution of the chilli script is to be parsed again. If the parseoutput parameter is not mentioned in the tag, the Chilli generated output will not be re-parsed before being passed to the browser.

name

The BMC Software DEFTAG expects the name parameter to define the name of the new tag. The naming conventions for new tag names are the same as the naming rules in the Chilli language, that is:

- The name may have a maximum length of 32 characters.
- The name may be any combination of alphanumeric characters (that is, letters, digits, and underscores.
- The name may be in lowercase or uppercase or a mixture of both.
- The name may start with an underscore (_) or a letter, but not with a digit.
- The name must not contain any spaces.
- The name must not be a reserved statement, a function name, or a keyword.
- The name must not be an already declared variable or constant.

Example

The following example shows an excerpt that creates a tag called SUBMIT that draws the submit buttons (Apply, Reset, Cancel, etc.) on the screen.

```
<SCRIPT>
        proc DrawSubmitTag (HtmlTagList HtmlFile, int index)
                string szFormName, szTarget, szButtons
                int iButtons
                GetTagParamValueStr (HtmlFile, index, "formname", "", szFormName)
                GetTagParamValueStr (HtmlFile, index, "target", "", szTarget)
                GetTagParamValueInt (HtmlFile, index, "buttons", SUBMIT_ALL, iButtons)
                DrawSubmit (szFormName, szTarget, iButtons)
        endproc
        </SCRIPT>

        <DEFTAG name=SUBMIT proc=DrawSubmitTag>
```

proc

The BMC Software DEFTAG expects the `proc` parameter to declare the name of the procedure which defines the new HCHL tag. The naming rules for the procedure are the same as those for the new tag name. The defined procedure has a fixed signature and must include the following arguments:

Syntax

```
proc NewProcedure (HtmlTagList HtmlFile, Int Index)
```

HchlFile	contains the list of all tags called by the procedure. For more information about this structure, see the Chilli Reference Manual in Section II under the heading HTML Functions.
Index	the number of tags called by the procedure.

Example

The following script excerpt of an HCHL file defines two new tags PRINT and MAILTO in its procedures and declares them then through the DEFTAG.

```
<SCRIPT>
   ....
   proc HandlePrint (HtmlTagList HtmlFile, int index)
        print (StrEvalAsString (HtmlFile.Tags[index].TagParams[1].TagParamValue))
   endproc

   proc HandleMailto (HtmlTagList HtmlFile, int index)
        string mailto
        mailto = StrEvalAsString (HtmlFile.Tags[index].TagParams[1].TagParamValue)
        print ("&lt;A href='mailto:" + mailto + "'>" + mailto + "&lt;/A")
   endproc
   ....
 </SCRIPT>

   <DEFTAG name=PRINT proc=HandlePrint>
   <DEFTAG name=MAILTO proc=HandleMailto>
```

parseoutput

If the parseoutput parameter is supplied with the DEFTAG tag, when the script is run, the output is parsed again. If the `parseoutput` parameter is not mentioned, then the output, in whichever format it was returned by the script, will display on the screen.

Example

The following script is an excerpt of an HCHL file that defines a procedure to display panels on the screen.

```
<SCRIPT>
        proc DrawPanelTag (HtmlTagList HtmlFile, int index)
                string title, width, height, name
                int buttons, NoTitle
                bool fNoTitle
                GetTagParamValueStr (HtmlFile, index, "title", "", title)
                GetTagParamValueInt (HtmlFile, index, "buttons", 0, buttons)
                GetTagParamValueStr (HtmlFile, index, "name", "", name)
                GetTagParamValueStr (HtmlFile, index, "height", "400", height)
                GetTagParamValueStr (HtmlFile, index, "width", "250", width)
                GetTagParamValueInt (HtmlFile, index, "notitle", 0, NoTitle)
                ....
                if (NoTitle == 1)
                fNoTitle = TRUE
                else
                fNoTitle = FALSE
                endif
                DrawPanel (title, buttons, name, height, width, ...., fNoTitle)
        endproc
        </SCRIPT>
        <DEFTAG name=PANEL proc=DrawPanelTag parseoutput>
```

FORM

The FORM tag defines an interactive form and is used in the agent web interface in its standard format with additional BMC Software specific functionality. For more information about the FORM tag in general. refer to a standard HTML 4.0 reference.

Forms are generally created for data input. When the user submits the form through an input or button element the form values are submitted to the URL given in the form's required action attribute.

The FORM tag was extended by BMC Software through the htmlfile parameter to allow the agent interface to execute specific actions. It is not necessary to specifically include the action and method parameters, because they are directly included into the parser: action always is 'mwcparse' and method is 'post'.

Start Tag	required
End Tag	required
Syntax	`<FORM htmlfile='filename.html'></FORM>`

Mandatory Parameters

htmlfile	The htmlfile parameter defines the file to be loaded next. This file contains the necessary Chilli scripts to process the entered data.

Optional Additional Parameters

There are no optional parameters for this function.

To enter and process data via the FORM tag in the agent interface two files are necessary:

1. An HTML file containing the FORM with its boxes to be filled in and the *htmlfile* parameter.
2. A file containing Chilli scripts to process the data entered into the FORM of the HTML file called through the *htmlfile* parameter in the first form sheet HTML file.

htmlfile

The BMC Software extended FORM tag expects the htmlfile parameter to define the file which will compile and execute the data entered into the form sheet. The file path can either be relative to the current directory or absolute.

Example

myfile.html:

```
....
        <FORM htmlfile=DataProcess.html>
                Enter Data:
                <INPUT name=Data type=text>
                ......
                <INPUT name=submit type=submit>
        </FORM>
```

When the form is submitted, it calls the file DataProcess.html, which processes all entered data through Chilli scripts.

DataProcess.hchl

```
<SCRIPT>
        extern string Data
</SCRIPT>
<SCRIPT>
        if (defined (`Data'))
                print ("Your data is " + Data.s)
        else print ("No data specified")
        endif
</SCRIPT>
```

Line 1-3:

Before any of the entered data can be processed in this file, all data variables need to be declared through the external keyword in a structured script. If the variables are not specifically declared at the beginning of the file, the following script
will not compile because it cannot find the variables.

In this example, the "Data" variable has the suffix ".s" to indicate that the variable is a string variable. The variables may optionally be specified in the form of var.suffix, if the value of the variable might be ambiguous. The parser will automatically add the respective suffix if it is not mentioned.

Possible suffixes are:

```
i = integer
c = character
f = float
d = double
b = boolean
s = string
```

Line 4-9

After the variables are declared, a script is needed to compile all entered data. In the preceding example, this script could consist of only lines 4, 6 and 9. However, if the "Data" field is left empty, this might cause the script to not compile or compile with an error. Therefore, it is recommended to always add an if/endif (lines 5-8) statement to avoid any compiling problems.

IF

The agent interface's HCHL pages can now also contain conditional sections through the integration of the IF tag. The IF tag consists in effect of four different tags – IF, ELSEIF, ELSE and ENDIF – used exactly the same way as the Chilli IF language statement. The IF tags can be nested to any level. For more information about the IF tag, see the Chilli Reference Manual.

Start Tag	required
End Tag	required
Syntax	`<IF condition=(Chilli expression)><ELSEIF condition=(Chilli expression)> <ELSE> <ENDIF>`

Mandatory Parameters

condition	a value which is evaluated as an expression and determines if the statement following the condition is executed or not.

Optional Additional Parameters

There are no optional parameters for this tag.

condition

The condition parameter is a value which is always evaluated as an expression:

Example

```
<IF condition=(BROWSER_TYPE="Mozilla/3.6.13 [en] (X11; U; Linux 2.2.5-15 i568), Mozilla Firefox")>
        <p>Your browser is Mozilla Firefox version 3.6.13.
<ELSEIF condition=(BROWSER_TYPE="Mozilla/5.0 (compatible; MSIE 5; Windows 2000), Microsoft Internet
Explorer")>
<p>Your browser is Microsoft Internet Explorer version 8
<ELSE>
        <p>Your browser is not certified for use with the BCM Agent Interface v 10.1.
<ENDIF>
```

INCLUDE

The INCLUDE tag is a very useful tag to keep the HTML files unclustered and to guarantee the same appearance of all pages.

General information about the basic structure of all HTML files, such as background color and background image in the BODY tag, as well as the structure of titles and footers can be defined in special small files.They can then be included into all pages via the INCLUDE tag instead of being repeated in every single file. Many of the actions to be executed through Chilli scripts are very similar in quite a number of pages. Therefore, they also can be put into separate files, which will then be included in many other files through the INCLUDE tag.

This considerably reduces the work required to set up the pages as well as the file sizes. It furthermore facilitates the task of making changes to the basic appearance of the HTML files should the need occur. The INCLUDE tag will be replaced in its entirety by the contents of the included file.

Start Tag	required
End Tag	forbidden
Syntax	`<INCLUDE htmlfile='file name' [condition='condition value'] [onceonly]>`

Mandatory Parameters

htmlfile	The htmlfile parameter defines the name and path of the file with which to replace the INCLUDE tag. The file path is relative to the path of the current file into which the new file is to be included.

Optional Additional Parameters

condition	A value which is evaluated as an expression and determines if the file include is to be executed or not.
onceonly	The onceonly parameter is used to avoid the multiple loading of the same data, which causes an error and stops the execution of a script.

htmlfile

The file parameter defines the name and path of the file with which to replace the INCLUDE tag. The file path is relative to the path of the current file into which the new file is to be included. If, for example, the current file is located in a directory `webconsole/commonviews/user` , and the file containing all body information, located under directory `webconsole/lib` is to be included, the file information would read like this: `file='../../lib/Body.html'` .

Example

The included file in the following example is a file called `Body.html` which gets the background image file. If this is set to NONE it gets the wall paper color.

Source File

```
<INCLUDE htmlfile=../../ScriptLib/Body.html onceonly>
```

Output File

```
<BODY TEXT='#000000' LINK='#0000ff' VLINK='#800080' BACKGROUND='/Console/Icons/backgrounds/blue.png'>
```

onceonly

The onceonly parameter is used to avoid the multiple loading of the same data, which can cause an error and stop the execution of a script. This is used to make sure a file is only loaded once, because files can be called several times through the INCLUDE tag of included files, for example.

Example

The index file calls the following files containing the components required to create the base page:

```
<INCLUDE htmlfile="../common/scripts/defs.hchl" onceonly>
<INCLUDE htmlfile="../common/scripts/header.hchl" onceonly>
<INCLUDE htmlfile="../common/scripts/footer.hchl" onceonly>
```

Due to the `onceonly` parameter, the scripts contained in these files are only executed once, as required for the creation of the pages.

condition

The condition parameter is a value which is always evaluated as an expression, whether it is included in parentheses () or not. If the value is true, the included file is executed. If the value is false, nothing happens and the included file will be
ignored. The default value is "true" (if the condition parameter is not specifically mentioned).

LOOP

The LOOP tag defines a section in an HCHL file which repeats an operation. This tag is very useful for listings of values where it is not known how many instances of the attribute exist. The loop tag is only used to initiate the loop action for a table; it cannot be seen in the output file's source code.

Start Tag	required
End Tag	required
Syntax	`<LOOP [condition='condition value']></LOOP>`

Mandatory Parameters

There are no mandatory parameters for this tag.

Optional Additional Parameters

condition	A value which is evaluated as an expression and determines if the loop is executed or not.

condition

The condition parameter is a value which is always evaluated as an expression, whether it is enclosed in parentheses () or not. If the value is true (or a non-zero value), the loop is executed. If the value is false (or zero), nothing happens and the loop will be ignored (that is, the parser jumps to the </LOOP> tag and continues with the next element). The default value is `true' (if the condition parameter is not specifically mentioned).

SCRIPT

Scripts offer authors a means to extend HTML documents in highly active and interactive ways. For example:

- Scripts can be evaluated as a document loads to modify the contents of the document dynamically.

- Scripts can accompany a form to process input as it is entered. Designers can dynamically fill out parts of a form based on the values of other fields. They can also ensure that input data conforms to predetermined ranges of values, that fields are mutually consistent, etc.
- Scripts can be triggered by events that affect the document, such as loading, unloading, element focus, mouse movement, etc.
- Scripts can be linked to form controls (for example, buttons) to produce graphical user interface elements.

In the agent web interface, the SCRIPT tag is mainly used to call Chilli scripts which do most of the internal work within the agent interface. However, the SCRIPT tag can also call other scripts, such as Unix shell scripts or others.

Scripts can be either included into the HTML file if they are only applicable in a specific situation, or they can be stored in separate files. Since most scripts are applicable in more that one situation, those are stored in separate HTML files under the ScriptLib directory. These scripts are called via the BMC Software INCLUDE tag. Depending on the context of the script, its execution can then result in other scripts being executed, in a direct HTML output or an output which is then parsed again before being passed on to the browser.

When encountering a SCRIPT tag in an HTML file, the parser checks the ScriptInterpreters section of the webconsole.ini file for an entry matching the supplied language name. If it does not find a non-blank value, it passes the tag and its contents to the browser without changes. If it finds an entry in the .ini file with a non-blank value, it assumes that the value is the path of the interpreter to be used for handling the script. In this case it copies the text between the <SCRIPT>and < /SCRIPT> tags into a temporary file and executes it using the supplied path. The path can be relative (for example, `sh.exe /bin/sh`

The default value of the language parameter is "Chilli". If the language specified is "Chilli" or the lang parameter is absent, the script tag will treat the value as a Chilli script. If the parameter value is not Chilli or empty, the parser will check the .ini file for the value specified in the lang parameter.

Start Tag	required
End Tag	required
Syntax	`<SCRIPT [language='script language'] [vars='variable name(s)'] [parseoutput]></SCRIPT>`

Mandatory Parameters

There are no mandatory parameters for this tag.

Optional Additional Parameters

language	The language parameter defines the program with which the script is to be executed.
vars	The variable parameter vars defines which variables are being used in the script.
parseoutput	

	If the parseoutput parameter is supplied with the SCRIPT tag, the output after the script was run is parsed again by the parser.

language

The `language` parameter defines the program with which the script is to be executed. The default value is `chilli.` If the language parameter is missing, the parser automatically interprets the language parameter as being Chilli.

Example 1

The following script is written in JavaScript and after execution shows the language choices for the the agent interface.

```
<!-- Start location -->

<IMG src="/common/images/bulletsubsection.png" width="13" height="11">
<SPAN class="LOCATION">
    <SCRIPT language='Javascript'>document.write (FindTranslation ("_MENU_KIOSK_"));&lt;/SCRIPT>
</SPAN>

<IMG src="../../../common/images/bulletsubsection.png" width="13" height="11">
<SPAN class="LOCATION">
    <SCRIPT language='Javascript'>document.write (FindTranslation ("_MENU_LIST_"));&lt;/SCRIPT>
</SPAN>

<!-- End location -->
```

Example 2

An HTML file contains the following SCRIPT tag:

```
<SCRIPT language= bourneshell>
```

When the parser encounters this tag it will check the ScriptInterpreters section of the webconsole.ini file for an entry called bourneshell. This section contains the following entry:

```
[ScriptInterpreters]
BourneShell=/bin/sh
```

This entry tells the parser that the executable with which to execute the script is a Unix shell script called "sh", which is located in the local bin directory. Note, that the language name and the entry in the .ini file are *not* case sensitive, so 'bourneshell' and 'BourneShell' are equivalent.

The parser now places the text between the <SCRIPT> and </SCRIPT> tags into a newly created temporary file and executes this file with the unix shell "sh".

vars

The variable parameter vars defines which variables are used in the script. The variables need to be defined before the SCRIPT tag through the SETVAR parameter. If the script language is Chilli, no vars parameter is needed, because the Chilli scripts are run inside the HTML pages, where all variables are already mentioned. All other scripts run outside the HTML pages and need the variables specified in order to run.

parseoutput

If the `parseoutput` parameter is supplied with the SCRIPT tag, the output after the script was run is parsed again by the parser. If the `parseoutput` parameter is not mentioned, the output will be directly displayed on screen.

Example

The following code is from the HCHL file creating the layout of MyApps page in the browser:

Source File

```
<SCRIPT parseoutput>
    Print ("<INCLUDE htmlfile='"+ HTTP_DOCUMENT_ROOT + "common/scripts/tabs.hchl'>" + ENDLINE)
</SCRIPT>
```

SETVAR

The SETVAR tag defines variables for use in the HCHL file. The variables created through SETVAR have global scope. Variables are named storage locations capable of containing a certain type of data, such as a numerical value or string of text used in the program that can be modified during program execution. These variables can be used directly by a tag or a script that follows the variable definition. They can also be used by files that are called through the INCLUDE tag. Contrary to the other BMC Software tags, the SETVAR tag does not produce any direct output.

Start Tag	required
End Tag	forbidden
Syntax	`<SETVAR name='variable name' value='value of variable>`

Mandatory Parameters

name	The name parameter defines the name of the variable.
value	The value parameter is an expression.

Optional Additional Parameters

There are no optional parameters for this tag.

name

The name parameter defines the name of a variable to be used later in a script within the HTML page. The naming conventions for new variable names are the same as the naming rules in the Chilli language, that is:

- The name can have a maximum length of 32 characters.
- The name can be any combination of alphanumeric characters (that is, letters and digits, and underscores.
- The name can be in lowercase or uppercase or a mixture of both.
- The name can start with an underscore (_) or a letter, but not with a digit.
- The name must not contain any spaces.
- The name must not be a reserved statement, a function name, or a keyword.
- The name must not be an already declared variable or constant.

Example

```
<SETVAR name="_hchldir" value="/myhchl">
<SETVAR name="_id" value="345">
...
<A htmlfile=(_hchldir+"/mypage.hchl?_id="+_id)>
```

value

The value parameter is an expression representing the value of the defined variable. The value can be a simple integer or string or it can be a rather complicated function expression surrounded by parentheses.

Customizing BMC Client Management reports

The CM console comes with two different types of reports: style-based and template-based reports. Both types can be customized, however, while template-based reports are generated via a quite complicated XML file it is very easy to customize style-based reports according to your requirements.

Style-based reports are based on a layout type that defines the number of subreports the report contains and how these subreports are ordered on the displayed or printed page. The appearance of all subreports is based on a css style sheet.

You can customize the following elements of this report type:

- Customizing report logo
- Customizing report style sheet

Customizing report logo

BCM provides you the possibility to store more than one logo, so you can use different ones for different reports if necessary.

1. Go to the **[BMC Installation Directory]/data/Vision64Database/reports/common/images/logos/** directory.
   This directory contains all logos that can be used in reports. The default logo, BMC.png, comes with BCM.
2. Either modify the existing logo or copy the new logo to this location.
   The logo file must be in .png format and have a size of 272 x91 pixels. If it is larger it will be cut down to the right size.
   The new or modified logo is now available via the Console and will appear in the drop-down list of the Logo box in the Properties window when creating a new or modifying and existing report.

Customizing report style sheet

BCM comes with two css style sheets:

- Numara.css: This style sheet is the default css, it has a fixed width of 1024 pixels.
- Compatible.css: This style sheet has the same values as the Numara.css sheet apart from the width which is not fixed. It is used for the existing reports after upgrading from a pre 10.1 version.

To customize style sheet,

1. Go to the **[BMC Installation Directory]/data/Vision64Database/reports/common/css** directory. This directory contains all css files that may be used for the reports.
2. Either modify the existing css file or copy the new css file to this location.
   The new or modified stylesheet is now applied to the reports.

Localizing BMC Client Management to an unsupported language

BMC Client Management is available in the following languages:

- American English
- French
- German
- Japanese
- Brazilian Portuguese
- Spanish

Localization comprises translations of all elements of the Console GUI, balloon tips, and Instant Expert. In addition to the six available languages, you can localize CM in an unsupported language. This process consists of the following steps:

- Localizing the console
- Localizing the agent interface, reports, and emails
- Translating the .locale files

Localizing the console

You can localize the following elements of the console :

- Elements of the GUI like the names of buttons, nodes, tabs, and so on.
- Balloon tips
- Instant Expert

The translations for these elements are saved in different files.

Localizing console includes:

- Adding languages to the database
- Creating localization files

Adding languages to the database

All available languages for localization are in a specific database table called ***Enumeration***. When you want to add a new language to the console, you must add a new entry to the table.

1. Copy the following command and replace the four sample values in the second line with your information:

```
INSERT    INTO Enumerations (EnumID, EnumGroup, EnumName, EnumValue)
       VALUES (<userinput>11905, 'AvailableLanguages', '_DB_LANGUAGE_NEWLANGUAGE_',
'NewLanguage'</userinput>);
```

The four expressions represent:

Expression	Value	Information
EnumID	11905	Unique identifier for any option in the database. You can use any value between 11950 to 11999. If you add more than one language option make sure to use different EnumIDs.
EnumGroup	AvailableLanguages	Type of the enumeration. In this case the value must always be AvailableLanguages.
EnumName	_DB_LANGUAGE_NEWLANGUAGE	Keyword for the new language, for example, _DB_LANGUAGE_CHINESE.
EnumValue	NewLanguage	Name of the language (for example, Chinese). Do not use special characters such as ç orñ.

2. In the ***Enumeration*** table of your database, execute the modified command.
   The new language is added to your database. In the next step, you add a .locale files for your new language which contain the translations.

Creating localization files

Localization files are text files with the extension ***.locale*** . To add a new language you need to create three new ***.locale*** files.

1. On the device on which the Console is installed go to <BMC Installation Directory>/ui /console/jws.
2. Open the **NumaraFootprintsAssetCore.jar** file with a file archiver such as WinZip or WinRAR.
3. Extract its locales folder to the jws folder.
4. In the **NumaraFootprintsAssetCore.jar** file delete the locales folder and close it.
5. Open the locales folder and add the following line to each <Language> .locale file:
   _DB_LANGUAGE_NEWLANGUAGE_=LanguageValue
   To add Chinese as a new language, add:**_DB_LANGUAGE_CHINESE_=Chinese** to **English.locale** or **_DB_LANGUAGE_CHINESE_=Chinois** to **Francais.locale**.

> Language Valueis the value that will be displayed among the language options in the **Preferences** dialog, from which you select the language of the Console .

6. Duplicate a ***<Language>.locale*** file and rename it so that it matches EnumValue of your new language that you added to the database.
   To create a Chinese ***.locale*** file rename it to **Chinese.locale**.
7. Repeat the last step for ***<Language>Params.locale*** and ***<Language>_GuidedHelp.locale***.

> If you don't create three new ***.locale*** files, the english ***.locale*** file will be used in place of the missing file.

8. Translate all translation values in the files (the expression to the right of the equal sign (=).
9. To verify your translations, launch a Console and select your newly added language from the **Language** drop-down list in the **Preferences** dialog.
   The Console displays in your new language.

You created the three required ***.locale*** files and localized the Console to a new language.

Localizing the agent interface, reports, and emails

In addition to the Console, you can also localize the following elements of BMC Client Management that are accessible outside of the console :

- Agent interface in a browser
- Reports created in the console and displayed in a browser or with other software programs
- Emails sent by the console

Localizing agent Interface, reports, and emails include:

- Adding language to agent interface files
- Adding language to SQLite database

Adding language to agent interface files

To add a new language to the Agent Interface you need to define the new language in a file, as well as an image of a flag that represents it. To add a language:

1. Go to ***[BMC Installation Directory]*** **/ui/common/images** and check if there is a matching **LANG_YourLanguageAbbreviation.png** file for your language.
   - If there is no such file, create a new .png file of the flag representing your language with dimensions of 16 x 11 pixels.
2. Open the ***[BMC Installation Directory]*** **/ui/common/scripts/menu_items.js** file in a text editor.

3. Replace the three variables in the following line with your information and add it after line 29:

```
[
<img style=/"position:absolute;top:5px;left:7px;/" src=/"/common/images
/LANG_<varname>YourLanguageAbbr</varname>.png/" width=16 height=11>
<div style=/"position:absolute;top:4px;width:46px;left:27px;/" align=left><varname>YourLanguage<
/varname></div>',szURL + '_language=<varname>YourLanguage</varname>']
```

To add Chinese as a new language, replace ***YourLanguageAbbr*** with CN and ***YourLanguage*** with Chinese.

4. Save the file and close it.

You included the new language with its matching flag. In the Agent Interface the new language can be selected, but the translations are still missing. In the next step you add the translations to the database.

Adding language to SQLite database

To add a language to a SQL database you need:

- your new as well as the existing ***<Language>.locale*** files as described in the Translating the .locale files.
- BMC Client Management Installation file

Contrary to the console, the localization data of the gent interface , reports and emails are contained in a small SQLite database to which all new languages must be added.

To add a new language to the SQLite database

1. Copy the files **Locale2SQLite.bat**, **Locale2Sqlite.jar**, and **sqlite.exe** to any folder on your computer.
2. Open **Locale2SQLite.bat** in a text editor and modify the command as follows:

```
java -jar Locale2Sqlite.jar "[BMC Installation Directory]/ui/console/jws/locales"
```

3. Save **Locale2SQLite.bat** and double-click it.
   The command line displays and the SQL file is generated.
4. Wait until the command line closes.
   In the folder, a **translation.sqlitefile** is created.
5. Copy the **translation.sqlite** file to ***[BMC Installation Directory]*** **/ui/common/dict** and ***[BMC Installation Directory]*** **/data/core** which will overwrite the existing files.
6. To verify your translations, open the agent interface and select your newly added language from the drop-down list on the top left. The agent interface displays in your new language.

Translating the .locale files

What is a .locale file?

A ***.locale*** file is a text file with the extension ***.locale*** . It contains all keywords used by CM and its respective translations. There is a separate ***.locale*** file for each language.

How is a .locale file structured?

A ***.locale*** file has the following structure:

```
KEYWORD1=Keyword1Value KEYWORD2=Keyword2Value KEYWORD3=Keyword3Value ...
```

Each pair of keywords and values is on a separate line. The keyword and its value are connected by an equal sign (=). A ***.locale*** file must be in UTF-8 format.

What should I translate in a .locale file?

In a ***.locale*** file only translate the value of a keyword, which is the expression on the right side of a a equal sign (=).

Never modify any part of the keyword, which is on the left side of the equal sign. If you do, the link between keyword and translation breaks and CM keywords appear instead of translations.

What is the syntax of a keyword?

A keyword has the following characteristics:

- The general syntax of a keyword is the following: _ ***SECTION*** _ ***ACTION*** _ ***OBJECT*** _
  - For the most important ***SECTION*** s see the table.
  - ***ACTION*** is generally composed of a verb only or a verb plus its child
  - ***OBJECT*** is the element on which the action is executed, for example, *ASSIGNGROUP_QUERY* (Assign a group to a query)
- Each keyword starts and ends with an underscore, with the exception of values directly coming from the CM agent database, which cannot be forced into this scheme. These keyword values appear as they are (. that is, as simple text, such as ***DebugLogMax)***
- The "name" part of an element name is generally dropped for the keyword (for example, *COLNAME_DEVICE* for the table column "Device Name".
- The following abbreviations are used:
-
  - Administrator = ADMIN
  - Operational rule(s) = OPRULE(S) or OR(S)
  - Parameter(s) = PARAM(S)
  - Attribute(s) = ATTR(S)
  - Database Server(s) = DBSERVER(S)
  - Hardware Inventory = HWINVENTORY
  - Software Inventory = SWINVENTORY
  - Transfer Window Folder = TWFOLDER

The most important ***SECTION*** s are:

Name	Description
ACTION	Name of an action, menu item, window, button, and so on.
AGTMOD	Any type of values or messages being generated from the CM agent
CLASS	Name of an action, menu item, window, button, and so on.

Name	Description
COLNAME	Name of a table column
CONSOLE	Any type of values or messages being generated from the CM agent
CONST	Constants in drop-down lists in dialogs
DB	Values from the database
ERROR / ERRORCODE	Text returned by errors
HEADER	Title right window pane if different from the node name
HOME	All elements that can appear on the home page
LABEL	Any type of item appearing in the main window of the Agent Interface , such as field names, and so on.
MENU	Name of menus, those of the Console as well as those of the Agent Interface
MESSAGE	Any content appearing in simple message boxes on the screen
MISC	Any item appearing in the right window panes which are not boxes or table elements, or do not fit in any of the other sections.
MSI	MSI package specific items in the right window panes
NODENAME	Name of the tree node in the left window pane
NOTE	Explanations of the contents of a browser page
POPUP	All items contained in a pop-up window
PREF	All elements of the **Preferences** dialog
SCHEDULE	All schedule specific items
SEARCH	All elements of the search tab
SNPXXX	Snapshot specific items in the right window panes
STATUSBAR	Info appearing in the status bar of the main window
SUBTITLE	This is the prefix for all subtitles of the Agent Interface
SWINV	Elements with this prefix pertain to software inventory
TABNAME	Name of the tabs in the right window pane
TITLE	Titles of the Agent Interface
TOOLTIP	All tooltip expressions – for each action there is a tooltip equivalent
WINTITLE	Title of a dialog

Is there anything else I need to pay attention to?

Make sure that:

- you do not modify any keywords
- you do not modify the structure of the file with a pair of keywords and values per line
- every space ( ) in the value is preceded by a backslash (/), for example, Create/ Package/ Folder...

- you save the file in UTF-8 format
- you do not modify the file name

Can I add new keywords to the .locale file?

You can add new keywords to the ***.locale*** file, but they have no functionality in BMC Client Management.

Do I have to translate all keyword values?

If you want all elements of CM to appear in your new language, you have to translate all keyword values of the ***.locale*** file. You can also just translate keyword values that are important to you and leave the rest in the original language of the ***.locale*** file.

Reviewing and testing REST Web APIs

Representational State Transfer (REST) is only an architectural style and not a protocol. For example, there is no "official" standard for REST web services. However, it can use standards like HTTP, URI, XMS, and so on, like any standard.

The REST web API is a web service activated via a module in BMC Client Management using HTTP and a collection of resources, with four defined aspects:

- the base URI for the web service, such as `http(s)://localhost:1611/wsdoc`.
- the Internet media type of the data supported by the web service. This is often XML but can be any other valid Internet media type provided that it is a valid hypertext standard.
- the set of operations supported by the web service using the HTTP methods GET, PUT, POST, and DELETE.
- The API must be hypertext driven.

For more information about activating the web services module, see Configuring the web service.

The following HTTP methods are supported in BMC Client Management:

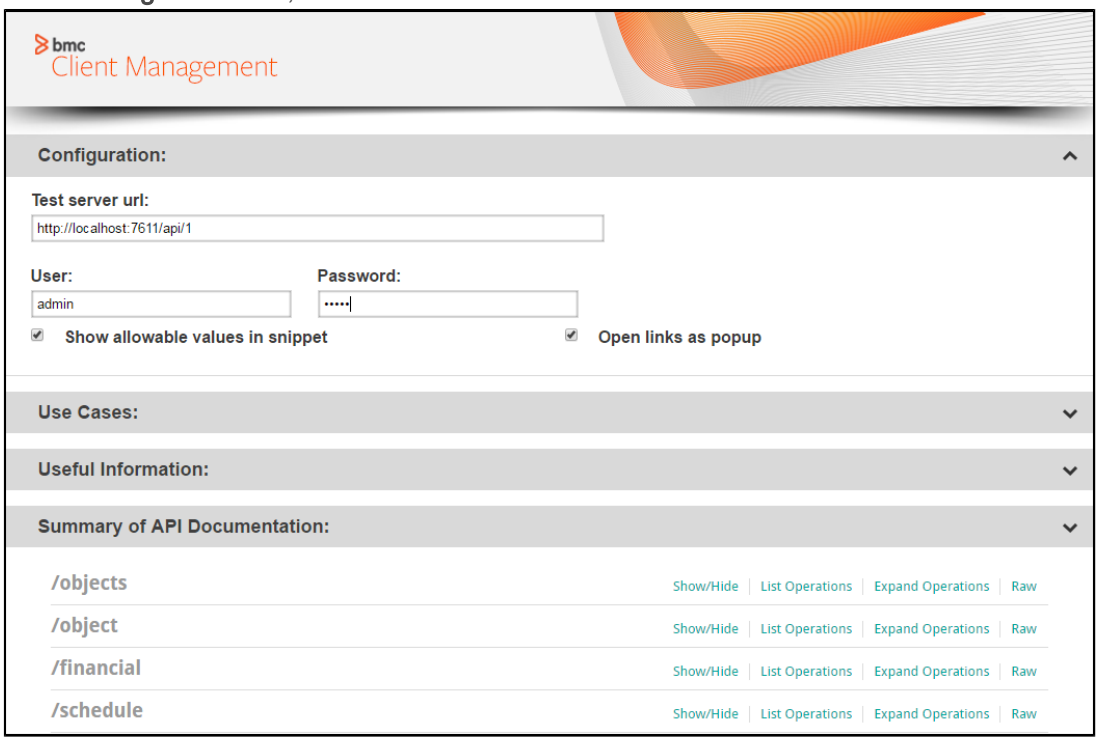
- GET: List the URIs and perhaps other details of the collection's members if executed on a collection URI, or retrieve a representation of the addressed member of the collection, expressed in an appropriate Internet media type if executed on an individual element.
- POST: Create a new entry in the collection. The new entry's URI is assigned automatically and is usually returned by the operation. This method is mainly used on a collection URI not for execution on an individual element. If run on an individual element it treats the addressed member as a collection in its own right and creates a new entry in it.
- PUT: Replace the entire collection with another collection if executed on a collection URI. If executed on an individual element it replaces the addressed member of the collection, or if it doesn't exist, creates it.
- DELETE: Delete the entire collection or the addressed member of the collection.

BMC Client Management provides a tool to review and test the REST web API operations available for interaction with BMC Client Management database. It is divided in the following different sections:

- **Configuration:** Configure the access to the BMC Client Management database.
- **Useful Information:** Find more useful information about the Swagger online help tool as well as for the API operations.
- **Use Cases:** Find use case examples for specific situations.
- **Summary of API Documentation:** Provides access to all available operations via their groups.

To test the web service

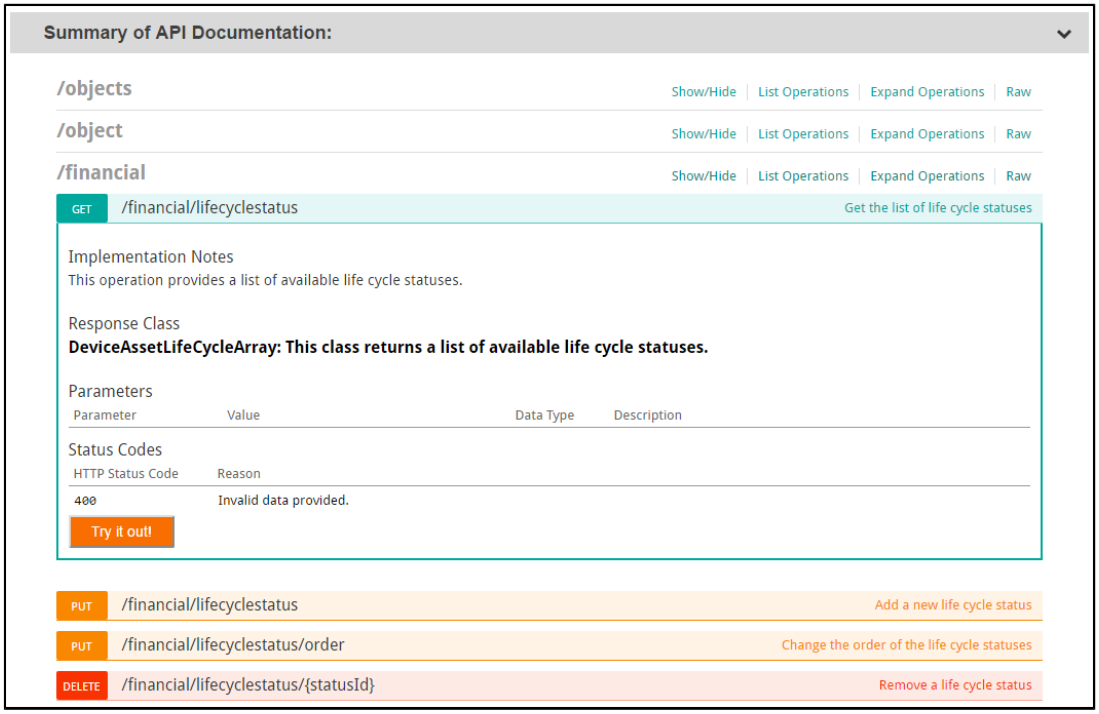
1. In a browser window, enter the tool URI in the https://*server:port*/wsdoc format. For example, http://scotty:1611 or http://localhost:1611.
2. In the **Configuration** box, enter the test server URI and credentials.



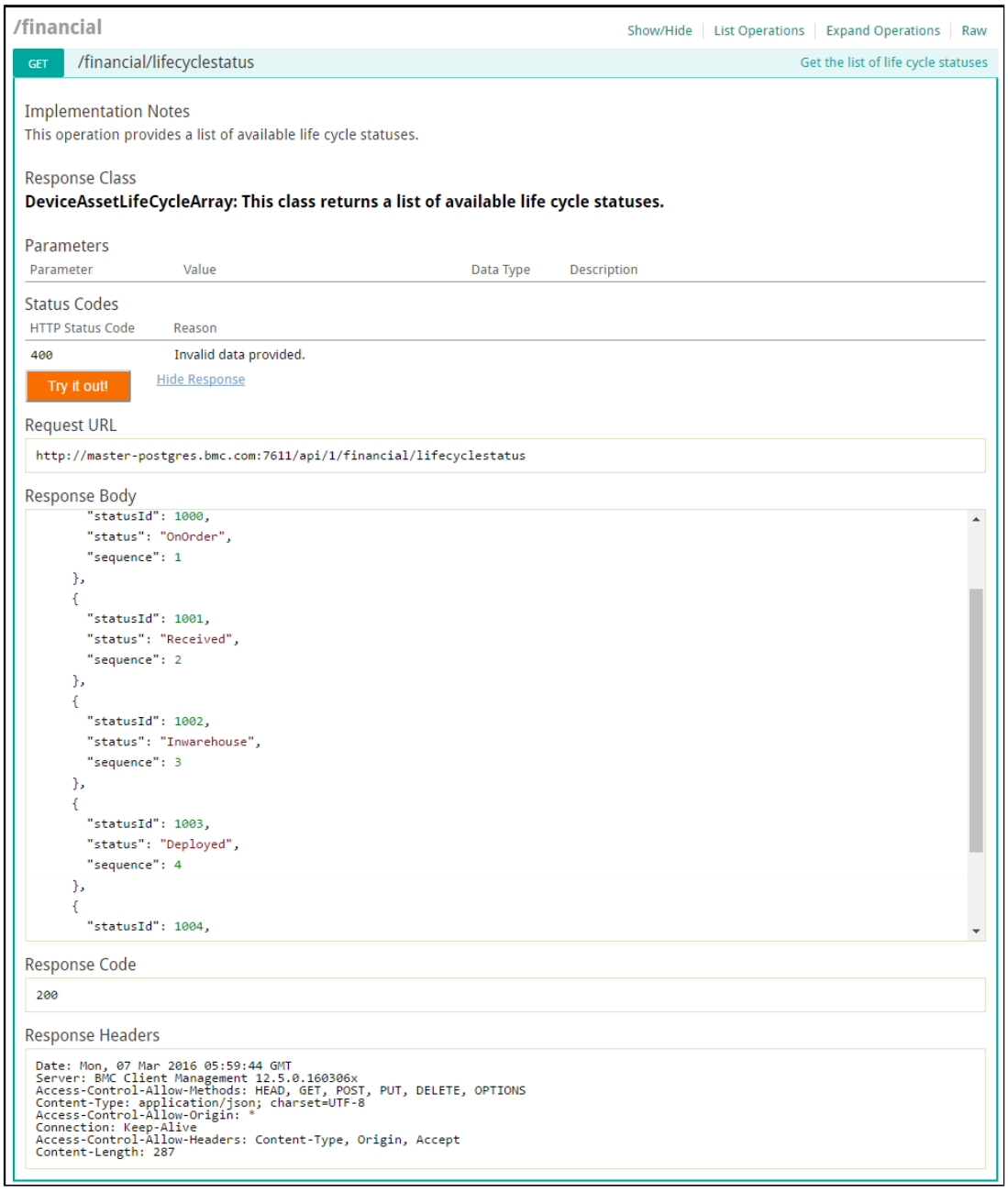
The access to the BMC Client Management database is now granted.

> **Note**
>
> If your credentials contain domain name, enter the credentials in the following format: **[domain]\\[username]** (with two '\'). For example,**production\\administrator**.

3. Select the **Show allowable values in snippet** check box if it is not yet checked. A number of parameters require specific database values that you cannot be aware of. By selecting this check box, the list of possible values that can be entered into these parameters is provided with the snippet.
4. Select the **Open links as pop-up** check box to open the the online help on return classes and snippets in a new pop-up windows. If clear, it opens in a new tab of the browser.
5. To access the operations click the respective group link below the **Summary of API Documentation** bar and the available operations will be listed.



6. To test an operation, enter the required data in the available boxes and then click **Try it out!** The operation zone is expanded enlarged and the new boxes show the result of the executed operation.



For more information about supported REST web services operations, download and see the BMC Client Management - Web Services Operations Manual for Integration with BMC Client Management.

Troubleshooting

This section provides information about troubleshooting this release.

The following table provides links to relevant topics based on your goal:

Goal	Instructions
Troubleshoot issues when installing a BMC Client Management master on CentOS 7	• Troubleshooting installation on Linux
Remotely control a MAC device	• Troubleshooting remote control
Enable logs to view, analyze and collect them	• Working with logs

Difficulties when installing a BMC Client Management master on CentOS 7

When installing a master with the default parameters on Linux CentOS 7 x64 with a PostgreSQL database on the same device at the end of the installation, the following error message may appear:

```
Changing configuration files...
awk: cmd. line:1: $1!="SSL" && $1 != "CertAuth" && $1 != "CertTrusted" && $1!="PAC" && $1!="
ConnectionQueueMaxSize" $1!="Mode" && /^.*$/ {print}
awk: cmd. line:1: ^ syntax error
```

This error occurs on CentOS 7 x64 because the awk version is 4.0.2. On a CentOS 6.4 x64, the master installs without problems, because the awk version is 3.1.7.

Workaround:

1. Open the file **bmc-client-management-master-12_0_0.sh** .
2. Remove `$1!="Mode"` from the file.
3. Start the master installation again.

Troubleshooting remote control

Troubleshooting remote control

Cannot remotely control a MAC device

If you cannot establish a remote control connection with a Mac OS X device, try rebooting the device.

> **Note:**
>
> When installing a CM agent for the first time on a MAC OS X device, the device must be rebooted to ensure that the remote control driver is working properly.

Working with logs

This section explains how to enable logs, view and analyze them, and collect them to provide BMC Customer Support.

Debugging CM and its components is done via the log files generated by the CM agent and some of the functionalities. The parameters for the logging functionality can be defined via the console for the main agent logs, the **mtxagent.log** and the audit file log, **mtxagent_audit.log** . Both these logs are also shown in the console, each in its own tab. Some of the CM functionalities, such as BMC Client Management - Patch Management , also create log files which can or cannot be shown in console views, however, they are all accessible in their respective directories on the master device under **[Installation Directory]/master/log** , or on the client devices under **[Installation Directory]/client /log.**

Related topics

- Defining log parameters
- Accessing log files available via console
- Accessing log files not available via console

Defining log parameters

The **Logging** node allows you to define the basic parameters for log generation and displays the main agent log, `mtxagent.log` and the audit log file, `mtxagent_audit.log` , in their tabs.

This topic includes:

Modify the configuration settings

1. Select any line in the table in the right window pane of the respective topic.
2. Click **Edit> Properties** .
   The **Properties** window appears.
3. Make the appropriate modifications to the individual values.
4. Click **OK** to confirm the modifications and close the window.

Logging parameters

The parameters in this view define the basic settings for log files of the software, that is, the values specify the contents of granularity of the log files as well as their output location for example. This also includes the log file sizes and numbers, which types of entries are to be logged, the time format, if alerts are to be sent in case of logged errors, etc.

Parameter	Description
Output File	Defines the path to the log file relative to the installation directory: • **none** : There is no debugger output regardless of the other settings. • **stdout -sa -cw** : The debugging output is sent to the standard output. • **file** : The debugging output is written to a file whose name is to be specified in this field with a path relative to the agent installation directory, for example, *../../logs/namp.log* for a file located on the same level as the installation directory, not below.
Enable List	A comma separated sequence of message filter names which are to be output to the log file. The special character * means all possible values, an empty string disables the list.
Disable List	A comma separated sequence of message filter names which are to be filtered from going to the log file. The special character * means all possible values. By default the disable list is applied AFTER the enable list and so has a higher precedence.
List to Load First	

Parameter	Description
	Defines if the debugging is executed according to the principle of everything being disabled with some exceptions or everything being enabled with some exceptions. This system is defined through two lists, the **Disable List** and **Enable List** , which are explained following.
Displayed Types	A comma separated list of debug message types which are to be output to the log file. The special character * means all possible values.
Maximum Agent Log Size (Byte)	The maximum size of the log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified at all, there is no limit check on the size of the file.
Maximum Agent Log File Count	Maximum number of log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Agent Log Clean Start	Defines if the specified log file is to be backed up at each start of the agent. If enabled the log file specified in **Output File** is backed up at agent start time.
Maximum Audit Log File Size (Bytes)	Controls the maximum size of the audit log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified the limit is the value of the **Maximum Agent Log Size** entry.
Maximum Audit Log File Count	Maximum number of audit log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Audit Log Clean Start	Defines if the specified audit log file is to be backed up at each start of the agent.
Column Separator	The separator character between the columns in the output. If no value is supplied, the output is padded out for readability. If a value is supplied, no text padding is done.
Time Format	A formatting string used to format the timestamp part of the logged output. This field may however contain any string of characters the administrator deems appropriate and the variables may be ordered in any desired way. The variables this entry may contain are the following: %y for the year part of the timestamp with 4 digits, for example, 2004, %m for the month as its number, for example, 01 for January and 12 for December, %d for the day of the month, %H for the hour indication, %M for the minutes of the hour and %S for the seconds of the minute.
Send alert when an error occured	Check this box if an alert is to be sent to the master when an error is added to the agent log file.

Accessing log files available via console

Most of the BMC Client Management log files can be directly accessed at different locations in the console.

Some log files can be accessed directly via the modules of the respective device. All these are located under the **Agent Configuration > Module Configuration** node of the respective device.

Note:

> Be aware that log files larger 5 MB cannot be shown in these views. If, however, you apply a filter to reduce the displayed size they will be shown.

The following log files are available to access via console:

- Asset discovery log
- Audit log file log
- Main BMC Client Management agent log
- Operational rules log
- Patch manager log
- Reboot log file
- Rollout logs

Asset discovery log

The asset discovery scanner also keeps its own log files of its activities, therefore any logs concerning an asset discovery can only be found on the respective scanner. They are located in directory `Installation Directory/client (or master)/log/AssetDiscovery/scan` . Here you can find a number of different log files, each concerns the execution of a specific script on a specific device, the main log file of a scan is `user.log` , it contains all the general information about the scan execution.

It is possible to directly access the log file of a specific scan in the **Device List** tab of the **Asset Discovery > Scanners > Your Scanner > Module Configuration** node, or the **Device List** tab of the **Device Topology > Your Device > Agent Configuration > Module Configuration > Asset Discovery** node.

The log displays the date and time at which any patch action or operation occurred, the name of the patch module, a letter(s) that indicates of which type the explanation following is, such as ERR for error or `I for` installation, and so on, as well as the description itself. The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** boxes.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2006 the date box must be filled in as follows:*2006/11/14 12:30.** .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. For example, to display all lines containing "toto" in the description, enter the following in the **Description** text box: .***toto.*** .
Type	

Parameter	Description
	From this drop down box you can select the type of entry you want to display, possible values are `T` for Trace, `I` for Information, `ERR` for any type of error, `D` for Details, `W` for Warning and `A` for Audit.
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding text box click the **Sort** button to the right. The right window pane will be refreshed with only the requested lines.

Audit log file log

Logging of auditing operations is not included in the general logging in the `mtxagent.log` file, it is written in its own specific log file, the `mtxagent_audit.log` , which is located next to the general log file in the `/log` directory of every client. The tab **Audit Log File** of the **Agent Configuration > Logging** node of a device displays the contents of this log file in its right window pane for inspection.

The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as `ERR` for error or `T` for trace, and so on, the ID of the thread and the description itself.

On the master it logs everything that is executed in the console therefore it can become very large, on the client it is used to log remote control sessions and direct access.

The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** box.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2006 the date box must be filled in as follows: `2006/11/14 12:30.*` .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. If the preceding box **Use Regular Expressions** is activated you can also use regular expressions in this text box. The description starts from the administrator name, it therefore corresponds to `administrator name+IP address+description` . Example: to display all lines containing "toto" in the description, enter the following in the **Description** box: `.toto.` .
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding text box click **Sort** to the right. The right window pane will be refreshed with only the requested lines.

Main BMC Client Management agent log

The tab **Agent Log File** of the **Agent Configuration > Logging** node of a device displays the contents of the general CM log file `mtxagent.log` in its right window pane for inspection. This file is located in the `Installation Directory/master/log` directory.

The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as ERR for error or T for trace, and so on, the ID of the thread and the description itself.

The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** field.
Date	In this field you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12: 30 on the 14 November 2006 the date field must be filled in as follows: `2006/11/14 12:30.*` .
Description	In this field you can enter any string value which is to be contained in the description of log entry you are looking form. If the preceding box **Use Regular Expressions** is activated you can also use regular expressions in this field. The description starts from the administrator name, it therefore corresponds to `administrator name+IP address+description` . Example: to display all lines containing "toto" in the description, enter the following in the **Description** field: `.toto.` .
Type	From this drop down box you can select the type of entry you want to display, possible values are `T` for Trace, `I` for Information, `ERR` for any type of error, `D` for Details, `W` for Warning and `A` for Audit.
Module	From this list you can select the module for which the entries are to be displayed.
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding field click **Sort** to the right. The right window pane will be refreshed with only the requested lines.

Operational rules log

Logging of operational rules is not included in the general logging in the `mtxagent.log` file, it is written in its own specific log file, the `OperationalRules.log` , which is located next to the general log file in the `Installation Directory/master/log` directory.

The **Agent Log File** tab of the **Device Topology > Your Device > Agent Configuration > Module Configuration > Operational Rules** node shows if there are any operational rules associated with the remote device and if yes displays amongst other information the log file for the selected device concerning the execution of all assigned rules. The tab **Agent Log File** displays the contents of this log file in its right window pane for inspection.

If you are looking for the log of a specific operational rule on a specific device you can find it directly under the **Assigned Objects** node of either the device or the rule. When opening the log via the **View Log File** menu item in the **Operational Rule Log File** window, only the part pertaining to the currently selected device-operational rule relation is shown.

The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as ERR for error or T for trace, and so on, the ID of the thread as well as the description itself. The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** boxes.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2006 the date box must be filled in as follows:*2006/11/14 12:30.** .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. For example, to display all lines containing "toto" in the description, enter the following in the **Description** box: *.toto.* .
Type	From this drop down box you can select the type of entry you want to display, possible values are `T` for Trace, `I` for Information, `ERR` for any type of error, `D` for Details, `W` for Warning and `A` for Audit.
Name	In this text box you can enter the name of the operational rule for which to display all entries, for example, all entries concerning a rule called *Software Distribution Rule* .
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding text box click the **Sort** button to the right. The right window pane will be refreshed with only the requested lines.

Patch manager log

Logging of patch groups is not included in the general logging in the `mtxagent.log` file, it is written in its own specific log file, the `<PatchGroupID>.log` , one per patch group, which is located in the `Installation Directory/master/log/Patches` directory.

It is possible to directly access the log file of a specific client assigned to the currently selected patch group under the **Patch Management > Your Patch Group > Assigned Objects > Devices** node.

The log displays the date and time at which any patch action or operation occurred, the name of the patch module, a letter(s) that indicates of which type the explanation following is, such as ERR for error or `I for` installation, and so on, the ID of the thread, as well as the description itself. The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** boxes.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2006 the date box must be filled in as follows:*2006/11/14 12:30.** .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. For example, to display all lines containing "toto" in the description, enter the following in the **Description** box: *.toto.* .
Type	From this drop down box you can select the type of entry you want to display, possible values are `T` for Trace, `I` for Information, `ERR` for any type of error, `D` for Details, `W` for Warning and `A` for Audit.
Name	In this box you can enter the name of the patch for which to display all entries, for example, all entries concerning a patch called *csi2010-kb1258964-fulfile-x86-glb.exe* .
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding text box click the **Sort** button to the right. The right window pane will be refreshed with only the requested lines.

This directory also contains another log file, `hfcli.log` , which contains the log of the patch inventory generation.

Reboot log file

This file logs all operations concerning the reboot of a device, that is, when a reboot was launched by whom or which module, what pop-up window is shown on the screen, which options were available, which options were chosen by the local user, and so on.

Log entries of device reboot operations are included in the general agent log file, the **mtxagent.log** file, however for easier referencing they are also written to a specific log file, the **reboot.log** , which is located next to the agent log file in the **/log** directory of every client. This specific log file is required in addition, because the a **mtxagent.log** file is started anew on the device every time the agent is restarted, which is, of course, the case when a reboot occurs. This this information is no longer available in the console, there you can only see the contents of the newest **mtxagent.log** file. The reboot is not reinitiated after a reboot, thus it keeps all reboot messages and makes them available in its tab in the console.

Whenever a reboot window is assigned to a device, a message displays in the reboot log file. If the reboot window is immediately activated the message is: *The reboot window "RebootWindowName" is currently permitting reboots, the agent is attempting to display the pop-up to the user and request a reboot.* If not, the message is: *The reboot window "RebootWindowName" is currently prohibiting reboots, the reboot window opens again on Monday at 9pm, no reboot will occur until then.* If the assigned reboot window prohibits rebooting at the time when a reboot request arrives, a

log message indicates that and also provides the next allowed time-slot for a reboot. If reboot windows allow rebooting but the maximum number of reboots is already reached, a log message is also written. These messages are displayed only once in the log because the reboot check is done every minute.

The agent maintains a counter for the number of reboots that already be effected during the day, this counter is reinitialized every day. When a reboot is performed the agent adds a new entry to the log displaying the number of reboots remaining after the current one is executed. (*Reboot: Reboot is performed. 2 of the allowed 5 reboots are remaining for today.*)

If the reboot is cancelled because an application is in full screen mode a new entry is also added to the log file.

The tab **Reboot Log File** of the **Agent Configuration > Logging** node of a device displays the contents of this log file in its right window pane for inspection.

This log file log displays the date and time at which the reboot occurred, a letter(s) that indicates of which type the explanation following is, such as ERR for error or `I` for information, and so on, the ID of the thread and the description itself.

The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** box.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2014 the date box must be filled in as follows: `2014/11/14 12:30.*` .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. If the preceding box **Use Regular Expressions** is activated you can also use regular expressions in this text box. The description starts from the administrator name, it therefore corresponds to `administrator name+IP address+description` . Example: to display all lines containing "toto" in the description, enter the following in the **Description** box: `.toto.` .

To apply the filters defined in the preceding text box click **Sort** to the right. The right window pane will be refreshed with only the lines matching the specified criteria.

Rollout logs

Logging of rollouts is not included in the general logging in the `mtxagent.log` file, it is written in its own specific log file, the `mtxsetup.log` , one per rollout configuration per target device. All these log files are located under the `Installation Directory/client/log/Rollout /Session/<RolloutID>/<TargetDeviceID>` directory of the Rollout Server. The `<TargetDeviceID>` is a specifically generated ID for the rollout-target assignment and has nothing to do with the GUID or the internal database ID of the assigned device.

It is possible to directly access the log file of a specific rollout via the **View Log File** menu option of the **Targets** of the **Rollouts > Servers > Your Rollout Server > Your Rollout** node.

The log displays the date and time at which the rollout action or operation occurred, a letter(s) that indicates of which type the explanation following is, such as ERR for error or `I for` installation, etc. as well as the description itself. The displayed contents of the log file can be filtered and thus reduced in size to find specific entries or types of entries as follows:

Parameter	Description
Use Regular Expressions	Check this box if a regular expressions can be used in the following **Description** boxes.
Date	In this text box you can enter a date and time value for which the respective log lines are to be displayed. The format is `YYYY/MM/DD hh:mm:ss` , and you can use wildcard characters. For example, to display everything logged at 12:30 on the 14 November 2006 the date box must be filled in as follows:*2006/11/14 12:30.** .
Description	In this text box you can enter any string value which is to be contained in the description of log entry you are looking form. For example, to display all lines containing "toto" in the description, enter the following in the **Description** box: *.toto.* .
Type	From this drop down box you can select the type of entry you want to display, possible values are `T` for Trace, `I` for Information, `ERR` for any type of error, `D` for Details, `W` for Warning and `A` for Audit.
Thread ID	In this field you can enter the unique identifier of a specific thread that you would like to follow.

To apply the filters defined in the preceding text box click the **Sort** button to the right. The right window pane will be refreshed with only the requested lines.

Accessing log files not available via console

Contrary to the log files listed before, the following log files cannot be displayed in the console via a node or tab:

- Console logs
- Database logs
- Diagnostic logs
- HTTP protocol handler logs

These log files can be viewed only via the **Direct Access** node:

1. Select the device under a device group or the **Device Topology** node in the left window pane.
2. Select its **Direct Access** node.
   If the **Request System Credentials** system variable is activated and you have not identified yourself yet to this device in the current session yet, an **Identification** window appears.
3. Enter your credentials and click **OK** .
4. Select the **File System** node and browse the directory structure down to the respective directory under `Installation Directory/master}} or {{client/log` .

5. Select the log file to display in the right window pane.
6. Select the **Edit> Edit File**  .
   An **Edit Text File** window opens on the screen with the contents of the file.
7. Select the **OK** button at the bottom to close the window.

Console logs

Two optional log files `console.log` and `console.xmlrpc` . These can only be found on the master in the default log directory `Installation Directory/master/log /HttpProtocolHandler` . They are not generated by default. You can configure the agent to generate these logs via the `console.ini` configuration file which is located in the master's `Installation Directory/master/config` directory. In this case you need to set the parameters `EnableAccessLog` and `EnableXmlRpcLog` to `true` . If you make changes to these settings the master must be rebooted for them to take effect.

- The `EnableAccessLog` parameter activates the generation of the `console.log` which logs all http access calls to the CM console.
- The `EnableXmlRpcLog` parameter activates the generation of the `console.xmlrpc` log file which contains the xml content of these calls. Be careful when activating this log, it can become very large very quickly.

Database logs

The database log file with the default name `Vision64Database.log` can only be found on the master in the default log directory `Installation Directory/master/log` . This file logs all queries that are sent to the database by the master which take longer than a specific time. By default this log file is not generated.

You can configure the settings of this log file and activate it via the `Vision64Database.ini` configuration file under the `Debug` section which is located in the master's `Installation Directory/master/config` directory. If you make changes to these settings the master must be rebooted for them to take effect.

Diagnostic logs

The diagnostics tool also generates its own log files, one per scan and device. These files are also located centrally on the master in the `Installation Directory/master/log/Diagnostics /<device_deviceID>` directory. Their naming scheme is `<device name>_<execution time>` . This file logs all queries that are sent to the database by the master which take longer than a specific time. By default this log file is not generated.

You can configure the settings of this log file and activate it via the `Vision64Database.ini` configuration file under the `Debug` section which is located in the master's `Installation Directory/master/config` directory. If you make changes to these settings the master must be rebooted for them to take effect.

HTTP protocol handler logs

The HTTP Protocol Handler provides two optional log files `HttpProtocolHandler.log` and `HttpProtocolHandler.xmlrpc` . These can only be found on the master in the default log directory `Installation Directory/master/log/HttpProtocolHandler` . They are not generated by default. You can configure the agent to generate these logs via the `HttpProtocolHandler.ini` configuration file which is located in the master's `Installation Directory/master/config` directory. In this case you need to set the parameters `EnableAccessLog` and `EnableXmlRpcLog` to `true` . If you make changes to these settings the master must be rebooted for them to take effect.

- The `EnableAccessLog` parameter activates the generation of the `HttpProtocolHandler.log` which logs all http access calls.
- The `EnableXmlRpcLog` parameter activates the generation of the `HttpProtocolHandler.xmlrpc` log file which contains the xml content of these calls. Be careful when activating this log, it can become very large very quickly.

Best Practices for masters and relays deployed on Linux

The most common cause for deteriorated performance (with frequent crash) of masters and relays on Linux is because the default values set for descriptors are very low. The following configuration checks help you improve the performance (and avoid crashes) of masters and relays on a Linux platform:

1. Connect to the device locally and launch the terminal
   OR
   Connect to the device using SSH.
2. Run the following commands as `root` (or as `sudoer`) to check the existing values:

To check	Run command	Value check
Maximum number of open files per user login	`ulimit -Hn`	If the returned value is less than 10240, run the commands in the step 3a.
System-wide maximum number of open files	`sysctl fs.file-max`	If the value returned is less than 100000, Run the commands in the step 3b
TCP max sync backlog	`sysctl net.ipv4. tcp_max_syn_backlog`	If the value returned is less than 5000, Run the commands in the step 3c.
Read-ahead parameter	`blockdev -getra /dev/sda`	If the value returned is less than 4096, run the commands in the step 3d.

3. Depending on the returned values in step 2, run the following commands:

> **Warning**

Exercise caution when running the following commands. If the commands are not run correctly, the performance of the device may deteriorate and further impact the stability of the device.

a. To set the maximum number of open file descriptors per user login (value returned by the `ulimit-HnRun` command):

```
# vi /etc/security/limits.conf

root soft nofile 4096
root hard nofile 10240
```

Save the file (:q) and run the following command to validate the changes:

```
# ulimit -Hn
# ulimit -Sn
```

b. To set the system-wide maximum number of open files:

```
# vi /etc/sysctl.conf
fs.file-max = 100000
```

Save the file (:q) and run the following command to validate the changes:

```
# sysctl -p
```

Run the following command to double-check:

```
# sysctl fs.file-max
```

c. To set the TCP maximum sync backlog:

```
# vi /etc/sysctl.conf
net.ipv4.tcp_max_syn_backlog=5000
```

Save the file (:q) and run the following command to validate the changes:

```
# sysctl -p
```

Run the following command to double-check:

```
# sysctl net.ipv4.tcp_max_syn_backlog
```

d. To set the `Read-Ahead` value to 4096 for each /dev/sd drive on your server, edit the **/etc/rc.local** file and add the following block at the end of the file (this is an example of a server with three drive entries - a, b, and c):

```
blockdev --setra 4096 /dev/sda
blockdev --setra 4096 /dev/sdb
blockdev --setra 4096 /dev/sdc
```

e. Applying `noatime` attribute can also significantly improve the file I/O performance. To apply `noatime` attribute by editing the **/etc/fstab** file and replacing the 'defaults' with 'defaults,noatime', run the following command:

```
# /etc/fstab
/dev/mapper/centos-root /                       xfs     defaults,noatime 0 0
UUID=a8f64424-1a43-4735-a20e-54a8f43304fe /boot xfs     defaults,noatime 0 0
/dev/mapper/centos-home /home                   xfs     defaults,noatime 0 0
/dev/mapper/centos-swap swap                    swap    defaults,noatime 0 0
```

4. Reboot the device.

Reference

The following table provides links to the relevant topics based on your goals:

Goal	Instructions
Review information about network autodiscovery, SSL, BCM ports, and timer. Manage bandwidth and work with a super master.	• Technical reference • Autodiscovering your network • Autodiscovery in BMC Client Management • Bandwidth management • BMC Client Management and SSL • CM Ports • Timer • Working with a Super Master
Understand installation of different types of database engines, specific installation options and configurations.	• Database installation and configuration reference • Installing Microsoft SQL Server 2014 • Configuring Microsoft SQL Server 2014 • Installing PostgreSQL • Configuring PostgreSQL • Installation and configuration of Oracle 12c Release 1 (12.1.0.2) on Linux 6
Review information about predefined operational rules and steps.	• Step reference • Agent Configuration steps • Custom Inventory steps • Directory and File Handling steps

Goal	Instructions
	• Event Log Manager steps • Hardware Inventory steps • Inventory Management steps • Master Steps steps • Monitoring steps • Package Factory steps • Patch Management steps • Power Management steps • Process Management • Security Settings Inventory steps • Software Distribution steps • Tools steps • User Message Box steps • Virtual Infrastructure Management steps • Windows steps • Windows Device Management steps • Windows XP and 2003 Firewall steps
Review information about object specific parameters.	• Object parameters • Administrator parameters • Agent configuration parameters • Application Management parameters • Compliance Management parameters • Custom inventory object type parameters • The parameter of a device object • The parameters of a Device Group object • Directory Server parameters • Operational Rule parameters • OS Deployment parameters • Package parameters • Patch Management parameters • Query parameters • Report parameters • Resource Management parameters • Rollout parameters • Software License Management parameters • Transfer Window parameters • User parameters
Understand different parameters of all modules of BMC Client Management.	• Agent module parameters • Application Monitoring module parameters • Asset Discovery module parameters • Asynchronous Actions module parameters • AutoDiscovery module parameters • Custom Inventory module parameters • Custom Packages module parameters • Event log manager module parameters • File store module parameters • Hardware inventory module parameters • Host access module parameters • HTTP protocol handler parameters • Identity module parameters • MSI packages module parameters

Goal	Instructions
	• Operational rules module parameters • Patch management module parameters • Power management module parameters • Relay module parameters • Remote control module parameters • Rollout module parameters • RPM packages module parameters • Security settings module parameters • Security management product module parameters • Selfhealing module parameters • Snapshot packages module parameters • Software module parameters • Timer module parameters • Update management module parameters • User access module parameters • Virtual infrastructure management module parameters • Wake on LAN module parameters • Web API module parameters • Windows device management module parameters
Review the list of error codes for individual modules and objects in BMC Client Management.	• Error codes

Technical reference

The technical reference provides detailed information about the following topics:

- Autodiscovering your network
- Autodiscovery in BMC Client Management
- Bandwidth management
- BMC Client Management and SSL
- CM Ports
- Timer
- Working with a Super Master
- Updates to Security Products Inventory and Virtual Infrastructure Management

Autodiscovering your network

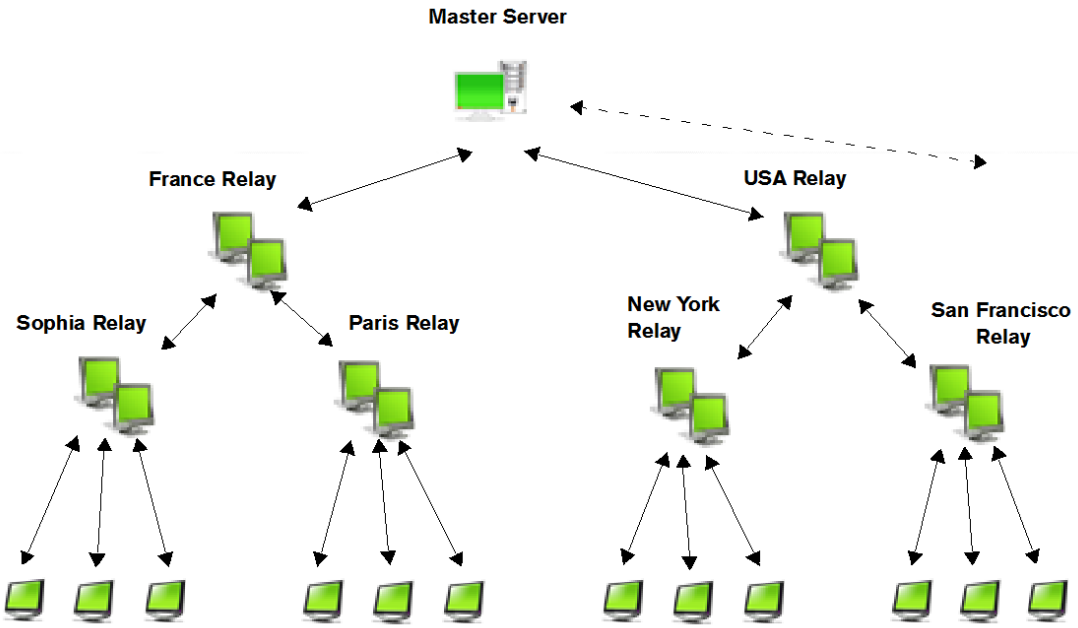
The Autodiscovery functionality of BMC Client Management allows you to scan your complete network and find all devices with some of their available information. To discover the network the following steps must be executed:

1. Configure the AutoDiscovery module.
2. Run an autodiscovery on one or more devices.
3. Upload all local autodiscovery results to the master database.

Autodiscovery in BMC Client Management

The device topology is an automatically created hierarchy that represents the way servers and clients are logically linked together, that is, the cascaded architecture of BMC Client Management itself.

The Autodiscovery feature of BMC Client Management maintains the topology of your network up-to-date.



All agents communicate with each other via a XML/RPC connection, which means that contrary to the classical architecture there is no permanent connection between the agents. Furthermore there are no typical modules such as servers and clients. Each agent can execute both roles, depending on the current requirements, therefore the resulting architecture is more of a Peer-To-Peer type. The queries are structured like XML and they are transferred via the HTTP protocol, which assures standard communication.

A key concept of BMC Client Management is that although the master server needs to know how to reach a client system, this is not set in stone and can dynamically evolve, if, for example, a client moves from one relay to another. This is especially useful for mobile systems that often move from one site to another and therefore need to be managed from a different relay server.

The Autodiscovery module is used by the Relay module and the Autodiscovery module of other managed devices and by the Rollout function. If the Autodiscovery module is disabled on a client with all other modules still independently working, the client will only be able to find the relay which was defined as its parent at installation time or in its configuration file. If the managed device moves, for example, if it is a laptop, it will not be able to find its new parent, because the auto-select function will not work.

A basic rule of the cascaded architecture is that a client is located under only one relay and a relay can only be under one other relay of the master server, thus ensuring that no device has more than one parent. The Autodiscovery module of BMC Client Management allows for constant updates of the topology of your network.

Autodiscovery establishes and maintains a local list of IP addresses and their state. Only the Relay, Autodiscovery and Agent Rollout modules of the CM agent use the list created by autodiscovery and maintained by the other agents.

The autodiscovery modules of the agents can exchange their lists at regular intervals, which maintains the network load and the load of the local CPU at a very low level. Effectively, all discovered addresses and their corresponding information are transferred between the modules, avoiding unnecessary PINGs or HTTP requests. Each list manages the difference between an address of which it has the control of and all others addresses, which were created via the interrogation of another list.

The Relay module does not only exist on relays (intermediary servers) but also on all BMC Client Management agents. This module manages the Automatic Relay Selection function, which searches, depending on its settings, the relay which was chosen for the local agent. This is executed according to the information stored in the autodiscovery list, specifically through the RouterHopCount parameter which measures the distance between the client and its relay and the speed with which it answers.

Each BMC Client Management system be it a master, relay or a client, within a range of IP addresses has the ability

- to discover its neighborhood or its neighbors
- to discover its parent server and
- to report itself to and communicate with its parent
- to limit its autodiscovery list to its own part of the network.

Whenever a client system notices that it has changed location, it is responsible for informing its closest parent of this change (Automatic Selection option of the relay must be set to Yes) and so on until the master is notified and updates its topology database.

The Autodiscovery module executes the following operations:

- Establishing the autodiscovery list
- Verifying individual addresses
- Merging device entries
- Purging the autodiscovery list

Establishing the autodiscovery list

The Autodiscovery module's work is centred on a list of IP addresses and device names which is continuously updated and verified. The list contains the following information for each entry:

- Name of the device. This is obtained either through the Windows Network Neighbourhood API or a DNS name lookup using the IP address. If both methods fail, the name is set to be the same as the IP address.
- IP address of the device.
- Entry Status (`Unverified` , `Verifying` , `Verified` , `Learned` , `Invalid`).
- HTTP port used to communicate with agent on device.
- Discovery date, expressed as seconds since midnight 01 Jan 1970 UTC (epoch).
- Response time to ping/TCP connect, in milliseconds.
- Router hop count established through ping. This can only hold the values 1, 2, 4 or 8.Relay enabled.
- Agent version.

The Entry Status for each address in the device list can have any of the following values. The integer value next to the name is the value used in the `Autodiscovery.sqlite` database file:

Parameter	Description
`Unverified` - 0	The entry IP address has not been verified as being a real device on the network. The verification is done by using either the network name or the IP address of the device.
`Verifying` - 1	Currently verifying if this device exists on the network.
`Verified` - 2	The device exists on the network.
`Learned` - 3	The entry was learned from another Autodiscovery module. When reading the device list from a remote module, only those entries which are `Verified` or `Learned` are returned. Therefore when an entry is `Learned` , it means that its validity was verified by at least one other device on the network.
`Invalid` - 4	The address did not respond to any pings or other network traffic and so is not a valid device on the network.

The Autodiscovery module updates the contents of the device list at three possible points during its operation:

1. At Agent Start-up
2. After ScanCount Verifications
3. At the Discovery of a Client Executing Autodiscovery

The Autodiscovery schema displayed further on details this process.

At agent start-up

When the Autodiscovery module is started on a device, it creates a list of devices in its database using three different sources as defined through the module settings in the module INI file. These sources are the defined through the following parameters:

Parameter	Description
Neighbours	

Parameter	Description
	defines the number of neighboring IP addresses to add to the device list. This defaults to 10, which means 5 addresses above and 5 addresses below the devices own IP address. If this is set to 0, no neighboring addresses are added to the list.
AddressRange	a list of static addresses to add to the device list. This can be individual addresses or device domain names or address ranges separated by ‘,'. This is empty by default.
UseNetworkNeighbourhood	on a Windows computer, use the network neighborhood APIs to populate the list. The default value for this entry is true. On a UNIX/Linux computer, this entry is not used.

You can also apply the following parameter to limit the list:

Parameter	Description
SameNetworkOnly	this value specifies if the list of discovered and learned clients is limited to those devices which are located on the same network as the device. The possible values are: 0 = There is no filter applied to any of the discovered devices, add all of them. 1 = All discovered client devices must be on the same network as us. 2 = All discovered devices which have their relay function enabled must be on the same network as us. 3 = All discovered devices must be on the same network as us.

The Autodiscovery module never adds the same address or device name to its list twice. If a duplicate entry is found when trying to add an address to the list, the two entries are merged together.

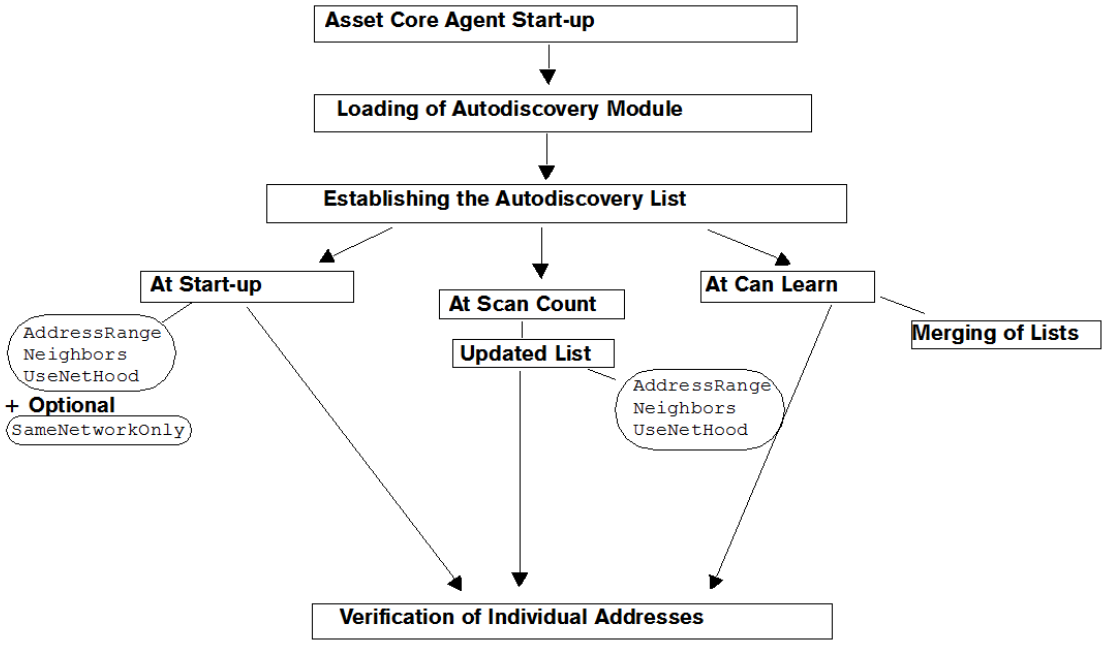
After ScanCount verifications

The Autodiscovery device list is constantly updated by the module by verifying the oldest address in the list. Each time an entry is verified, whether successfully or not, its update time is set to the current time which causes it to become the newest entry in the list. In this way all addresses are eventually verified in a round-robin fashion.

The module maintains an internal counter which is incremented every time an entry is verified. When this counter reaches the value configured in the ScanCount parameter, the list contents are refreshed in the same way as at agent startup, taking care to correctly merge any duplicate entries. This ensures that any changes to the INI file settings or the network environment are taken into account. For example, if the ScanCount parameter is set to its default value of 30, the list will be refreshed after every 30 verifications. Note, that the existing list contents are not deleted during a refresh.

At the discovery of a client executing autodiscovery

Part of the verification process for an address includes checking to see if there is a CM agent running on the remote device. If an agent is found and the local agents CanLearn parameter is enabled, the discovering module attempts to read the device list of the remote module to integrate it into its own list. As the contents of the read list are being added to the local database, all entries added are marked as Learned to avoid having to verify them in the future. Also, if a new entry is found in the local list, the two entries are merged together to avoid duplicates.



Verifying individual addresses

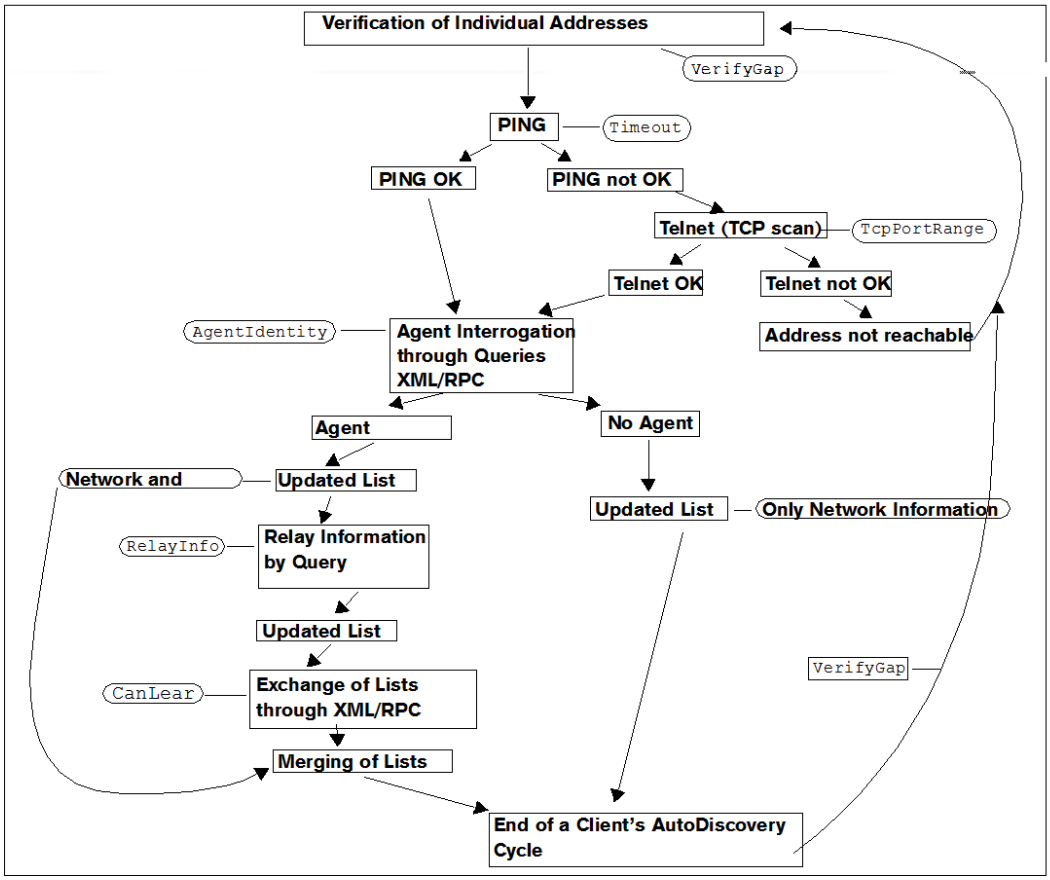
The main background task of the Autodiscovery module is to regularly verify the entries in its device list. The list is sorted by the timestamp of the last update for each entry which places the most recently update or verified entries at the end. To avoid overloading the network and the CPU, only one entry at a time is verified. The delay between the verification of consecutive entries is defined by the VerifyInterval parameter which is by default set to 30 seconds. To ensure that the addresses closest to the device are scanned and verified first, they are added to the list before entries coming through the **Use Network Neighborhood** parameter. The initial verification is executed according to the following rules, the schema at the end of the topic details this further:

1. Select the oldest entry in the database to be verified. The age of an entry is based on the entry Update time which is the last time the entry was verified or merged with another.
2. If the entry to be verified has its status value set to Learned and it is not a relay (RelayEnabled = 1), it is not verified. In this way, entries which are learned and already verified by other devices are not re-verified unless they are relays.
3. The first part of the verification is to establish whether the IP address is valid by "ping"ing it. This is done by sending an ICMP echo request and waiting for a reply. The timeout period limiting the wait for a reply is set through the INI file Timeout parameter. As well as verifying the presence of a device at the given address, the ping is also used to establish the number of router hops to that device and its response time. This is done through the use of the IP standard TTL field in the request which cycles through these values in order:
    - TTL = 1. If the device is on the same network and present, a reply will be received and will verify the address. If no reply is received, go to next step.

- TTL = 8. The request with TTL=1 did not respond which does not mean that the device does not exist but could be across many router hops. The maximum number of hops measured is 8 so send a new request with this value. If no reply comes back, then the address is considered invalid. If a reply is received, the address is valid so we need to try and get a more accurate hop count value.
- TTL = 4. The request with TTL=8 had a response, so now try with 4. If no response is received, the hop count for the address is 8 and no more requests need to be sent. Otherwise try a new request with a lower TTL value.
- TTL = 2. If a reply is received, a hop count of 2 is recorded for the address. A new request with TTL=1 is not sent as that is known to fail. If a reply is not received, the recorded hop count is 4.

4. In some rare cases (such as the agent not running as root on UNIX) a raw socket needed for ICMP operations cannot be created. If so, the address is instead verified by attempting a TCP connection to a number of commonly used ports. The ports used are defined in the configuration file through the TcpPortRange parameter (the default values are 23, 25, 139). The module will step through the ports until one is connected or there are no more left in which case the address is considered invalid.
5. If the ping or TCP connection attempt was successful, this indicates that the IP address is that of a real, online device. In this case the module tries to establish whether there is a CM agent running on that device by sending XML/RPC requests to the ports specified in the HttpPortRange parameter (the default values are 80, 1610, 8080). The calls executed are the following in the given order:
    - The AgentIdentity action is called first as all agents support this action regardless of which modules are loaded. If successful, all read information about the client is used to update the entry in the device list. If the call fails, the remote address is not a CM agent and no other actions need to be called.
    - The RelayInfo action is then executed to find if the agent has its relay function enabled or not. This is very important as the information is integrated into the device list and is later used by the local Relay module in selecting a parent device for communicating with the Master.
    - Finally, if the CanLearn parameter is enabled, the AutodiscoveryListDevices action is called to retrieve the list of verified devices from the contacted computer to be added to the current device's list. All read entries are marked as having been ‘Learned' which avoids the re-checking of the same computers.

After the list is scanned and verified, the Autodiscovery module can start a new cycle. It will then integrate possible new elements which are provided by NetBIOS (Use Network Neighbourhood parameter) and start a new verification at a rhythm of one element every 30 seconds.



Merging device entries

When a new device is learned or at the time of refreshing the list contents, the module takes care to not create any duplicate entries in the list. To avoid duplicates but at the same time keep as much useful information as possible, two matching entries are merged into one which is then kept in the list.

The matching of two entries to see whether they are copies of one another is done using the device name and IP address. Two entries are considered to represent the same physical device if there is a match between EITHER the IP address or device name of one and the IP Address or name of the other. This means that there are 4 checks done and only one needs to be satisfied for there to be a match:

- Name 1 = Name 2?
- Name 1 = IP Address 2 ?
- IP Address 1 = Name 2 ?
- IP Address 1 = IP Address 2 ?

After two entries are matched, they are merged together. The result of the merge operation is an entry with attribute values derived from the two merged entries. The rules used to decide which of the two possible values to use differ for each attribute. The following table shows the attributes and how their merged value is obtained:

Attribute	Merged Value
Device Name	As this is used for matching the 2 entries, it should be the same. In case of the entries has a blank name, the non-blank value is used.
IP Address	Same rule as for the **Device Name** .
Entry Status	If one of the entries is `Verified` , the value stored is `Verified` . Otherwise if one is `Learned` , the value is `Learned` . If neither of the preceding, the status of the entry with the later discovery time (more recent) is used.
HTTP Port	The higher of the two values is kept.
Discovery Date	The later date (more recent) of the two entries is kept.
Response Time	The value of the entry with the later discovery time (more recent) is used.
Router Hop Count	The value of the entry with the later discovery time (more recent) is used.
Relay Parent Name	If one of the entries is blank, the non-blank value is used, otherwise whatever is in the database already is kept.
Relay Enabled	If either entry has its **Relay Enabled** flag set, the merged entry value will also be set.
Agent Version	The version information of the entry with the later discovery time (more recent) is used.

Purging the autodiscovery list

To optimise the maintenance of the Autodiscovery list and avoid having old or out of date entries in there, the contents of list are purged according to the following rules:

Invalid	All entries which have a status set to Invalid are removed from the list when the list is being refreshed according to the rules previously described (Start-up, ScanCount).
Time To Live	Each entry which has a status of Unverified status is removed from the list if its age reaches the value configured in the MaxDeviceAge parameter. This is also done when the list contents are being refreshed.
Device IP Address Change	If the IP address of the device on which the agent is running changes, the Autodiscovery module purges ALL entries in its list and immediately starts to refresh the contents. The reason for this is that typically an address change implies connection to a new network and so the existing contents of the device list are almost certainly unusable.

Bandwidth management

Bandwidth management is a means of allocating bandwidth resources to critical applications on a network. Without bandwidth management, an application or a user can take control of all available bandwidth and prevent other applications or users from using the network.

In BMC Client Management two operations are necessary to calculated how much bandwidth should be used for download by a single client:

1. To measure the currently available bandwidth, some TCP/IP packets are sent to the bandwidth management port (which by default is 1609) at the rate defined via the **Bandwidth Check Frequency (sec)** parameter, by default every 60 seconds, for the period time defined by the Bandwidth Check Duration parameter, which is defined in milli-seconds, by default 200 ms. The data is sent once per **Bandwidth Check Frequency (sec)** unit for **Bandwidth Check Duration (ms)** interval. The currently available bandwidth is then calculated by dividing the amount of data sent by the duration.
2. For clients to adapt to the total number of downloads being currently performed, the clients request of their relay the number of download threads currently running. They do so by calling a specific action on their relay at the interval specified by the Client Check Frequency parameter, the default interval is every 10 seconds.

Therefore, the total amount of data sent for one package on port 1609 depends on:

- **Bandwidth Check Duration (ms)**
- **Bandwidth**
- **Package Size**
- **Bandwidth Check Frequency (sec)**
- % Transfer Window

If the parent relay does not reply, for example, due to network issues, there are two possible options:

1. If previous measurements succeeded, this data will be used for calculation
2. If no measurement ever succeeded the transfer will be blocked until it works again.

If the **Client Check Frequency (sec)** parameter is set to 0, that is, the checking is disabled, each client will consider that it is alone on the network. Be aware that using this value will not work with the global bandwidth percentage unit (% available) for the transfer window. In this case, if, for example, 10% are specified for available bandwidth the 1st client will take 10%, the 2nd client will also take 10%, and the third client, and so on. In the end this will end up with much more than 10% bandwidth used on a single network link.

Syntax Example:

This example details the calculation for the following data:

- **Bandwidth Check Duration (ms)** = 200 ms
- **Bandwidth** = 256 Kbps
- **Package Size** = 1MB
- **Bandwidth Check Frequency (sec)** = 60 s
- % Transfer Window = 30%

For the data provided before a raw estimation would be:

Bandwidth	256 * 1024 * 30% = 78643 bps
Theoretical time to download	1024*1024*8 / 78643 = 106 s
Number of measurements	1 at download startup + 1 after 60 s = 2
Amount of data transferred on 1609	2 * 256 * 0.2 /8 = 12.8 KB

This calculation is obviously rather theoretical, as parameters such as the correlation between the bandwidth and the number of connected clients can have an influence on this calculation.

BMC Client Management and SSL

The BMC Client Management uses the SSL (Secure Sockets Layer) protocol for transmitting any type of data. SSL uses a cryptographic system that uses two keys to encrypt data - a public key known to everyone and a private or secret key known only to the recipient of the message. It creates a secure connection between the client and its server, over which any amount of data can be sent securely. The CM agent can act as both a client and a server. A client is the one that initiates the communication (performs the connection) while the server is the one that provides a service (accepts the connection).

The following topics are provided:

- Using SSL for Connections
- Certificates
- Recommendations for SSL and Certificates
- Advanced SSL and Certification
- SSL=2 and SSL=3
- Generating Certificates with the mtxcert.exe Tool

Using SSL for Connections

If SSL is to be used for connections between the CM agents this must be defined at the installation of the respective agents. There you also define which type of SSL connection is used via the following parameter and its options. This parameter is also applicable for connections between the CM console and its server:

Parameter	Description
Secure Communication	This parameter defines if the agent will communicate in secure format. The possible values are:

Parameter	Description	
Parameter	No (0)	With this option the agent accepts both securized and non-securized communication, however it will send only non-securized communications.
Parameter	Securised Send, Receive Both (1)	This value indicates that the agent accepts both securized and non-securized communication, however it will send only securized communications.
Parameter	Yes (2)	When this option is selected the agent only communicates in secure mode, that is, it only receptions and send securized communication.
Parameter	Yes with mutual authentication (3)	With this option the agents communicate in secure mode and in addition will authenticate each other via SSL.

This parameter is defined at installation time of the components, or in case of the console, when it is launched. However, it can be modified at any time via the agent parameter settings in the Console or in the respective configuration files. The way the console connects to the server can be newly defined each time a connection is established.

If all agents communicate only in secure mode (mode SSL=2 or SSL=3) the console also must be activated with SSL when connecting to a device by checking the respective box in the console launch window. Otherwise, if a non-SSL connection is established between console and agent, it will immediately be closed again by the agent.

Certificates

Normal usage of the SSL standard is the server authentication. When connecting to a secured Web server with a browser (HTTPS instead of HTTP) often a pop-up displays with a warning because the received certificate is not trusted. Then it must be decided if the connection is to be accepted or the handshake stopped. This is because a secured server is responsible for sending its server certificate at the beginning of the SSL handshake. The client is then responsible for allowing or not the connection depending on the certificate issuer. The certificate issuer is the authority that signed (delivered) the certificate. If an authority is trusted, all those certificates are trusted that are signed by this authority. SSL connections themselves between the agents are managed by certificates. These allow an agent to access all other agents it needs to. However, via these certificates it is also possible to completely isolate a part of the network, for example a subnet or even the whole network.

The following topics are provided:

- Certificate types
- Related topics

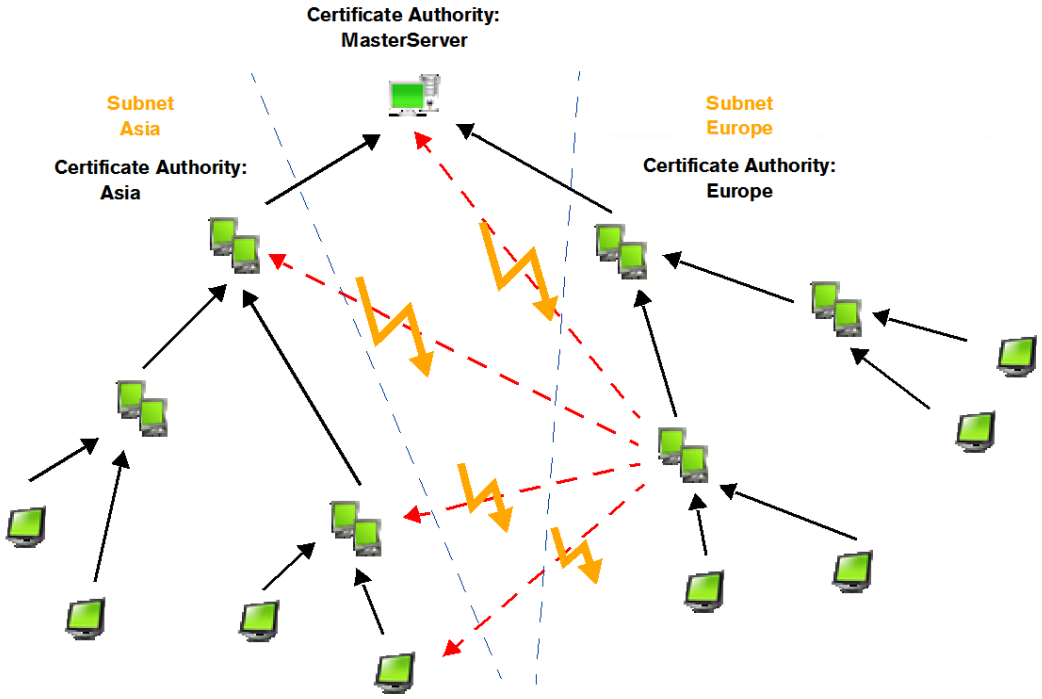
Certificate types

The following different types of certificates are used for agent communication:

- **Certificate Authority (CertAuth)**
  The certificate authority is the authority signing the agent certificate (client CM server).

- **Trusted Certificates (CertTrusted)**
  An agent requesting a connection with another agent accepts the connection if the certificate was signed by one of the trusted authorities which is listed in its parameter for trusted certificates. If the returned certificate is signed by an unknown authority the requesting agent will abandon the connection.

These certificates are specified via the respective parameters in the Security section of the agent configuration file (mtxagent.ini). If no certificates are defined the default BMC certificates will be established as the authority and used for certification. The parameters must be modified individually on the device agents in the .ini file or they can be modified in bulks via the operational rule that allows to modify a configuration file.



The preceding graphic shows an example with two subnets with separate certificate authorities, Asia and Europe. The agents from the subnet may contact all other agents in their subnet, but *not* those of the rest of the network.

Related topics

- Certificate Example
- Certificate Logging

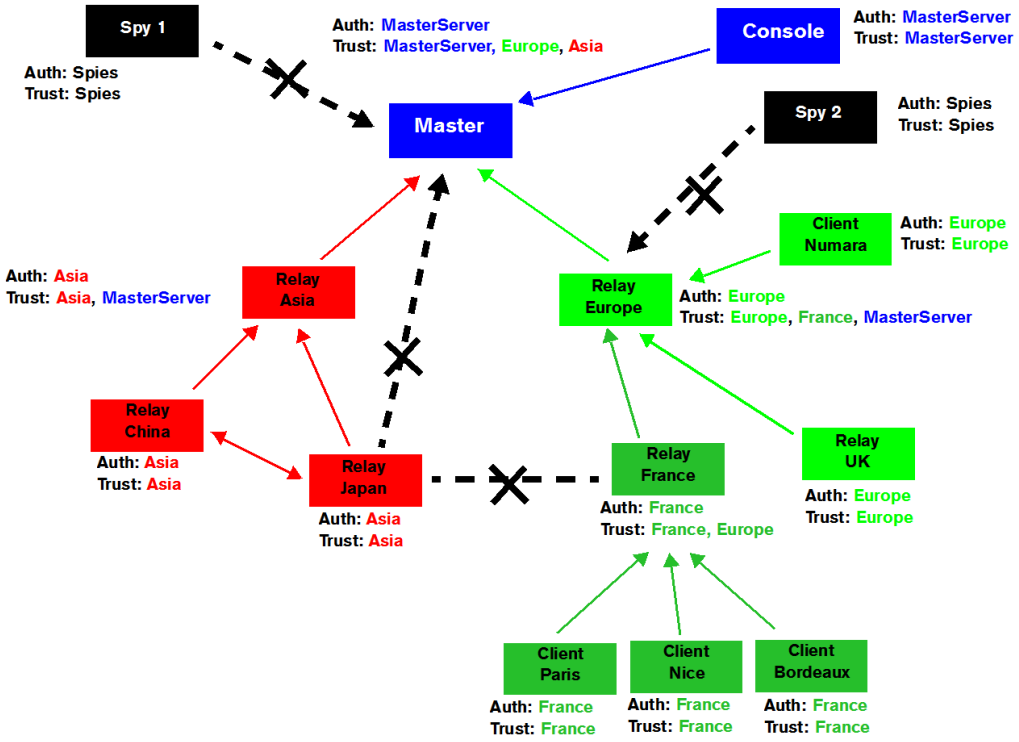
Certificate Example

If the example previously shown is split up in its individual parts, the following authorities and certificates must be established for proper communication within the subnets and the complete network:

The network has three certificate authorities: MasterServer, Asia and Europe.

- The master server must have the following certificates to connect to all its children:
  CertAuth : MasterServer
  CertTrusted: MasterServer, Asia, Europe
- The console in the following example can only connect to the master server with its certificates:
  CertAuth : MasterServer
  CertTrusted: MasterServer
  If the console also needs to connect to other devices via remote control or direct access it will also need to trust the other authorities, otherwise these devices cannot be accessed via the previously mentioned functionalities. It therefore requires the following certificates:
  CertAuth : MasterServer
  CertTrusted: MasterServer, Asia, Europe
- All devices located in subnet Asia must have the following certificates to be able to communicate with each other:
  CertAuth: Asia
  CertTrusted : Asia
- All devices located in subnet Europe must have the following certificates to be able to communicate with each other:
  CertAuth: Europe
  CertTrusted : Europe
- The main Asia relay must have the following certificates to communicate with all its children and its direct parent, the master server:
  CertAuth : Asia
  CertTrusted : Asia, MasterServer
  If it should also be able to communicate with the european main relay (and thus all its children) the trusted entry should contain the following entries:
  CertTrusted : Asia, MasterServer, Europe.
  This means that the Asia relay can contact any device in the subnet Europe, but not vice versa, that is, the devices in this subnet cannot contact the Asian relay.

- The main relay Europe must have the following certificates to communicate with all its children and its direct parent, the master server:
  CertAuth : Europe
  CertTrusted : Europe, MasterServer



To completely isolate a subnet, for example the European subnet France, another authority must be created for the main French server: *France* .

The French relay and all its children has the following certificate configuration, then they will not be able to contact any other device outside their subnet:

CertAuth : France

CertTrusted : France

For the preceding example the main European relay will now need another trusted authority to be able to contact this subnet, otherwise no communication is possible between the subnet France and the rest of the network:

CertTrusted : Europe, France

The way the connections are shown now in the preceding graphic, the French network can be contacted by one device only, the European relay, not even the master server can contact this subnet. For the master server to be able to the French subnet must also be added to its list of trusted authorities:

CertTrusted : MasterServer, Asia, Europe, France

Certificate Logging

The agent log mtxagent.log protocols also the authorities and certificates that are created. An entry would look like the following, which represents the default BMC certification, the generated name of the authority is BMC , the only trusted authority is the BMC authority:

- Certificate Authority:
- Server Certificate:
- Trusted Certificate:

Certificate Authority:

```
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Root   : certs/auth/
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Name   : Numara_ca
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Home   : fde4b4e9dbd690bd2c56d60f061598da
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Hash   : f061c793e7f33e6d04f12cf8c2c9cec3
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Issuer : <emailAddress=info@Numarasoftware.com;
    CN=Numara CA; OU=Numara AMP; O=Numara Software; L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Subject: <emailAddress=info@Numarasoftware.com;
    CN=Numara CA; OU=Numara AMP; O=Numara Software; L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Valid  : Yes
2008/01/21 14:39:03 AgentSecurity   I   Cert[000] Active : No
```

Server Certificate:

```
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Root   : certs/server/
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Name   : Numara_agent
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Home   : d862892c0c275bd377ff77d2b83c4345
2008/01/21 14 :39:03 AgentSecurity   I   Cert[001] Hash   : dd8d10f9bc9c4cc5b1bff423072848b0
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Issuer : <emailAddress=info@Numarasoftware.com;
    CN=Numara CA; OU=Numara AMP; O=Numara Software; L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Subject: <CN=192.168.1.229; O=Numara Software;
    L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Valid  : Yes
2008/01/21 14:39:03 AgentSecurity   I   Cert[001] Active : Yes
```

Trusted Certificate:

```
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Root   : certs/trusted/
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Name   : Numara_ca
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Home   : 33c402d87af0a0359db2c73339b013e4
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Hash   : f061c793e7f33e6d04f12cf8c2c9cec3
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Issuer : <emailAddress=info@Numarasoftwaren.com;
    CN=Numara CA; OU=Numara AMP; O=Numara Software; L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Subject: <emailAddress=info@Numarasoftware.com;
    CN=Numara CA; OU=Numara AMP; O=Numara Software; L=Sophia Antipolis; ST=PACA; C=FR>
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Valid  : Yes
2008/01/21 14:39:03 AgentSecurity   I   Cert[002] Active : Yes
```

Recommendations for SSL and Certificates

When using SSL and thus certificates BMC Software strongly recommends you to carefully plan your authority and certificate strategy before actually putting it in place. You can also make modifications later on, but if you are not VERY careful, all communication may break down.

If all components are installed with SSL activated they are initiated with the default BMC authority and certificates; the agent rollout by default does not include any customised certificates. As soon as you make changes to one single agent it is quite possible that no agents might communicate anymore. We therefore recommend you to prepare your complete SSL setup. This means:

- preparing all operational rules via the **Update INI File** modifying the `Security` section of the `mtxagent.ini` files of ALL network devices to their respective new authorities and certificates
- creating the queries and groups required to send and execute these operational rules
- creating the packages to distribute the new certificate files and
- assigning the operational rules with a common schedule to these groups to ensure that the large majority of rules, that is, the ini file modifications, are executed pretty much at the same time. This will limit the down time in communication as much as possible.

After the operational rules are launched you need to give the system some time to receive and execute them, so for some time part or all your network cannot be able via the CM agents , until all rules are executed on all devices. Depending on the up situation of devices, parts of the network might still not be reachable until they connect again to then receive and update to the new scheme.

Advanced SSL and Certification

Following you can see some more advanced information on the combination of SSL with certification in BMC Client Management .

CertAuth Parameter

In BMC Client Management an agent authority can be overridden. The CertAuth parameter in agent configuration file (`mtxagent.ini`) includes the name of the authority certificate to be used for signing the agent certificate.

When starting, the agent scans this directory and installs any new certificate as new available authorities. All the files must have the same common name (only the extension is different). This common name is the one to use in the configuration file in order to elect the new authority.

In order to change the certificate authority, the required files must be moved first to the `${AGENT_BIN}/certs/auth` directory. These files are:

- the authority X509 certificate (extension `.crt`)
- its attached RSA Private Key (extension `.key`)
- an optional Key Encrypted Password file (extension `.kep`)

The KEP (Key Encrypted Password) file is a feature offered by BMC , as it has the capability to cipher the RSA Private Key with a password that need not to be deployed, and the CM agent can retrieve the password depending on different elements. The automatic password generation is based on different pieces of information, including the file names. It is therefore not possible to rename any of the files once the KEP functionality is in use.

CertTrusted Parameter

The CM agent must know which authorities to trust, therefore the second parameter `CertTrusted` in the agent configuration file (`mtxagent.ini`) includes a comma separated list of authority certificates to trust. Here also, a certificate must be installed before being referenced in the configuration. Unlike the authority, only the X509 certificate is required (extension `.crt`) in order to trust an authority.

Then, in order to add a new trusted certificate authority, the required file, the authority X509 certificate (extension `.crt`), must be moved first to the `${AGENT_BIN}/certs/trusted` directory. When starting, the agent scans this directory and install any new certificate as new trusted authorities. As for the previous authority section, any certificate referenced in the configuration file must not include any extension.

From version 6.1.2 onwards users may use end user certificates (not those of authorities). In this case the certificate chain is not verified. If an agents presents such a trusted end user certificate the default verification mechanism is not required and the certificate is accepted.

SSL=2 and SSL=3

Now the real difference between SSL=2 and SSL=3 becomes clear. With SSL=2, the agent authenticates the server agent on which it performs a connection. With SSL=3, the verification is mutual as the agent still authenticates the server agent on which it perform a connection but the agent server also performs this verification on the client. This way ensures that both client and server are part of a common network.

SSL=3 and the console agent interface

As the agent performs a verification on the client actually connecting, this impacts also the console and any browser in case of HCHL trying to connect.

The following topics are provided:

Console

For the console to connect the following must be configured:

- a list of trusted authorities
- a console certificate to be used in case of SSL=3 on one of the connected agents

In order to allow the console trusting new authorities, the files (X509 certificates with extension `.crt`) must be copied in the directory `${CONSOLE_MAIN_DIR}/certs/trusted` . When starting, the console scans this directory and configures its communication layer in order to trust all the listed certificate authorities.

In order to allow the console using a certificate, the file (PKCS12 with extension `.p12`) must be copied in the directory `${CONSOLE_MAIN_DIR}/certs/console` . When starting, the console scans this directory and configure its communication layer in order to use this certificate when connecting to an agent performing client authentication (SSL=3).

Agent Interface

For the HCHL agent interface to connect the following must be configured:

- a browser certificate to be used in case of SSL=3 on one of the connected agents

This is more or less browser dependant but in any case, the browser raises a pop-up when connecting to a server performing client authentication. This pop-up is dedicated to the selection of an installed client certificate. With IE, such a client certificate can be installed with the corresponding PKCS12 file (the one used in the preceding console).

Example

Finally, it is important to understand that a certificate is signed by an authority which is itself a certificate, and so forth until a root certificate is reached. We talk about certificate chain in this case. For instance, we might think about the following:

- Starfleet Root Level (0)
- Enterprise Root Level (1) - issued by level (0)
- Enterprise EMEA Level (2) - issued by level (1)
- Enterprise Nice Level (3) - issued by level (2)

If we supply the level 3 certificate to an Enterprise agent, this last will emit its agent certificate signed by the third level. A client agent will accept the connection if and only if it trusts the server agent certificate (3) and all its ancestors up to (0).

Generating Certificates with the mtxcert.exe Tool

mtxcert.exe is a command line tool aimed at easing the creation of RSA keys, x509 certificates and PKCS12 files. Concerning the certificates, the tool can be used for creating new root authorities, intermediate authorities or final certificates. **mtxcert.exe** does not echo anything on the standard output. Instead, the **mtxcert.log** file is used each time the tool is executed. **mtxcert.exe** returns 0 on success and something different otherwise. The section concerns this new binary **mtxcert.exe** (**mtxagent** for linux) in the **${AGENT_BIN}** directory. It generates the following certificates:

- X509 Certificates (extension .crt)
- RSA Private Keys (extension .key)
- Kep files (extension .kep)
- Pkcs12 files (extension .p12)

Any standard can be used for generating authorities such as the command line tool openssl. However, this tool makes the process easier with an already deployed binary and it already includes the KEP functionality.

Syntax:

```
mtxcert.exe [-hqbdcg] [-i <input>] [-o <output>]
```

Related topics

- Command line switches
- SSL=3 and the console

Command line switches

The following command line switches can be used:

cmd	cmd long	Description
-q	--quiet	Do not display anything.
-b	--no-banner	Do not display the banner.
-d	--debug	Enable debug output.
-c	--configure	Generate a default configuration file. This option must be combined with -o or --output.
-g	--generate	Generate the files (RSA key, x509 certificate and PKCS12 file) from a configuration. This option must be combined with -i or --input.
-i	--input	The input file with the required configuration for generating the different objects.
-o	--output	The output file that will include the generated configuration to be used once updated.
-h	--help	Display this help and exit.

To create new certificates, a configuration file must be generated. This file must be updated with the user configuration. Then, the mtxcert.exe tool must be executed again for building the final files. The configuration file is a standard .ini file with sections. Following are the available parameters:

- Section [Common]
- Section [Rsa]
- Section [Ca]
- Section [CertObj]
- Section [CertExt]
- Section [Pkcs12]

Section [Common]

Parameter	Description
CommonName=mtxcert_out	This defines the common name to be used for generating the files. Each file will be created with this common name and a dedicated extension (.key, .kep, .crt or .p12). It is important not to include special characters. The names should remain ascii names, that is, A-Z, a-z, 0-9 and the underscore (_).

Section [Rsa]

Parameter	Description	
RsaModulus=512	This defines the RSA private key modulus (part of the key strength). Common values are 512, 1024 and 2048.	
RsaExponent=65537	This defines the RSA private key exponent (part of the key strength). Common value is 65537.	
RsaSymCipher=Aes_256_Cbc	This defines the symmetric cipher to be used for encrypting the private key. It is possible not to cipher the key in which case the special Null value must be used. In this case, no key password should were supplied. BMC recommends to encrypt the private key with one of the following symmetric cipher:	
	• Null • Des_Cbc • Des_Ecb • Des_Cfb • Des_Cfb64 • Des_Ofb • Des_Ede_Cbc • Des_Ede • Des_Ede_Ofb • Des_Ede_Cfb • Des_Ede3_Cbc • Des_Ede3 • Des_Ede3_Ofb • Des_Ede3_Cfb • Desx_Cbc • Rc4 • Rc4_40 • Rc2_Cbc • Rc2_Ecb • Rc2_Cfb • Rc2_Ofb • Rc2_40_Cbc • Rc2_64_Cbc • Bf_Cbc • Bf_Ecb	• Bf_Cfb • Bf_Ofb • Cast5_Cbc • Cast5_Ecb • Cast5_Cfb • Cast5_Ofb • Aes_128_Cbc • Aes_128_Cfb • Aes_128_Cfb1 • Aes_128_Cfb8 • Aes_128_Ecb • Aes_128_Ofb • Aes_192_Cbc • Aes_192_Cfb • Aes_192_Cfb1 • Aes_192_Cfb8 • Aes_192_Ecb • Aes_192_Ofb • Aes_256_Cbc • Aes_256_Cfb • Aes_256_Cfb1 • Aes_256_Cfb8 • Aes_256_Ecb • Aes_256_Ofb
RsaKeyPwd=	This defines the password to be used for encrypting the private key. If this password is blank and if the symmetric cipher is Null, the private key will not be ciphered. If this password is blank and if the symmetric cipher is not Null, the private key will be encrypted using the Kep algorithm. Otherwise, the private key will be encrypted using the defined symmetric cipher and the supplied password. In this case, no .kep file will be created.	

Section [Ca]

Parameter	Description
CaCommonName=level_2	This defines the common name of the authority to be used for signing the certificate. As for the CommonName, no extension must be supplied. If the CaCommonName and the CommonName are equal, the certificate will be self signed. This way, a new root authority can be created. If the special value "Numara" is used, the certificate will be signed with the BMC authority. Otherwise, the certificate will be signed with the supplied authority. In this case, the RSA private key (extension . key) and the x509 certificate (extension .crt) must be available. An optional Kep file (extension .kep) might be available if the authority is managed with the Kep algorithm.

Parameter	Description
CaKeyPwd=	This defines the password to be used for decrypting the authority private key. If this password is blank, an optional Kep file (extension .kep) is searched. In case of success, the Kep algorithm will be used. Otherwise, the tool assume that the authority private key is not ciphered.

Section [CertObj]

Each line defines an entry in the specification of the target for which the certificate will be generated. It is possible to remove one or more lines and to add new ones. Also, the current parameters can be updated. It is important to have at least a well defined and unique commonName. Anyway, the details about certificates content and extensions is out of scope.

```
countryName=FR stateOrProvinceName=PACA localityName=Sophia Antipolis organizationName=BMC Software
commonName=BMC Authority Level 3 - BMC Software Sophia Antipolis
```

Section [CertExt]

Each line defines an entry in the x509v3 extensions specification of the target for which the certificate will be generated. It is possible to remove one or more lines and to add new ones. Also, the current parameters can be updated. It is important to have at least a well defined basicConstraints. In case of authority, the value CA:TRUE should be defined. In case of final certificate, the value CA:FALSE should be used instead. Anyway, the details about certificates content and extensions is out of scope.

```
;subjectAltName=DNS:192.168.1.121,DNS:NOAH,DNS:NOAH.sophia.metrixsystems.com
;subjectKeyIdentifier=hash
;authorityKeyIdentifier=keyid,issuer:always
;keyUsage=nonRepudiation,digitalSignature,keyEncipherment basicConstraints=CA:TRUE
```

Section [Pkcs12]

Parameter	Description
Pkcs12Pwd=	This defines the password to be used for creating the PKCS12 file. The PKCS12 file is often used with the console or a browser when the SSL=3 parameter is in use. If the password is blank, no PKCS12 file will be generated.

SSL=3 and the console

When using SSL=3 (on master or any agent where console is supposed to connect), we need to supply a client certificate to the console. We already documented this process. The certificate is embedded in a `PKCS12` file generated by the `mtxcert.exe` (or any other) tool. But this file is protected by a password. In order to be able to load this file registered in the `$(CONSOLE_MAIN_DIR)/certs/console` directory, the console needs this password. We just need to update the file `$(CONSOLE_MAIN_DIR)/config/ConsoleConfig.properties` .

Add (or update if existing) the following line:

```
ssl_pwd=[password]
```

where [password] is replaced by the correct password protecting the PKCS12 file.

CM Ports

This topic lists the ports used by the CM agent for all different modules and provides some details on each.

Port overview

Component	Source	Destination	Direction	TCP/UDP	Service	Port number	Description
Database connection *	Master Server	Database Server	Bi-directional	TCP	TCP	Oracle: 1521 Postgres: 5432 SQL Server: 1433	For communication between the master server and the database. (* only if the database is on another server than the master)
Asset Discovery	Master Server	Client Devices	Bi-directional	TCP	SSH, WMI	22,135	The master server will communicate with agentless devices for Asset Discovery.
Agent Rollout	Master Server	Client Devices	Bi-directional	TCP	SSH, SMB	22,139	To install the CM agent on the client devices.
Client Agent communication	Client Devices	Master Server	Bi-directional *		HTTP	1610	The default agent communication port. * Communication must be possible in the direction from the client to its parent, the downwards direction can be replaced by a tunnel.
CM console	Administrative computer	Master Server	Uni-directional		HTTP	1611 (1610)	The default console management port.
Bandwidth Throttling *	Relay	Client	Bi-directional	TCP	TCP	1609	The bandwidth management port on relay servers. (* only used if transfer windows are defined with a percentage)
MyApps						1611 (1610)	The MyApps port on the master server.
AutoDiscovery				TCP	TCP, HTTP	135,22, 23,139, 1610	TCP ports scanned for auto-discovery.
Multicast Traffic	Relay	Client	Uni-directional	UDP	UDP	2500 *	The multicast transfer agent listen port as configured. * An IP range must also be configured.
Active Directory LDAP	Master Server	LDAP Server		TCP	LDAP	389	To synchronize data from LDAP server to CM .

Component	Source	Destination	Direction	TCP/UDP	Service	Port number	Description
Email Server	Master Server, console	Email Server	Uni-directional	TCP	SMTP	25	To send alerts and reports on email to users. This port must be open on all devices from which emails are sent via the console.
WebAPI	Browser, Web service caller	Master Server	Bi-directional	TCP	HTTP	1616	The port for the web services.

Notifications

XML-RPC packets are sent between the communicating agents as notifications to execute actions.

Direction	Parent Server	Client	Description
Parameter	Any	Agent	Downstream notification
Parameter	Agent	Any	Upstream notification

HTTP Files Transfer

File transfer is executed via the HTTP protocol and passes via the FileStore, it concerns all types of inventories, synchronizations, packages, files, assignments, status, and so on.

Direction	Parent Server	Client	Description
Parameter	Any	Agent	Downstream (Package/Assign/Delete/Scripts ...)
Parameter	Agent	Any	Upstream (Status/Identity/Inventories...)
Parameter	Any	Multicast	Multicast

Bandwidth Calculation

To measure the currently available bandwidth, some TCP/IP packets are sent to the bandwidth management port at the defined rate, by default every 60 seconds, for the defined period of time, by default 200 ms.

Direction	Parent Server	Client	Description
Parameter	Bandwidth	Any	Data sent to calculate available bandwidth
Parameter	Any	Broadcast	Wake-on-LAN notification

Wake-On-LAN

The Wake-On-LAN sends a magic packet to the target devices to wake them up.

Direction	Parent Server	Client	Description
Parameter	Any	Broadcast	Wake-on-LAN notification

Remote Control

Remote control communication passes via images for the actual remote control connections, and uses notifications for access right verifications.

Direction	Console PC	Client	Description
Parameter	Any	Agent	Images transfer / keyboard orders
Direction	**CM Master**	**Client**	**Description**
Parameter	Any	Agent	Downstream notification for Privacy check + client answer

HCHL Web Interface

The agent web interface allows to access agent data via a browser.

Direction	Web Browser	Client	Description
Parameter	Any	Agent	General web interface features

MyApps Application Kiosk

MyApps is part of the agent web interface and allows to execute specific operations and install software packages via a browser and per user.

Direction	Web Browser	Client	Description
Parameter	Any	Kiosk	Web interface for user application kiosk

Direct Access

The Direct Access functionality provides access to specific areas (file system, Registry, services, Task Manager, ...) of a device via the console.

Direction	Console PC	Client	Description
Parameter	Any	Agent	Direct access functionalities

AutoDiscovery

The AutoDiscovery functionality scans the network for a any type of hardware (PCs, printers, servers, firewalls, routers, ...).

Direction	PC1	PC2	Description
Parameter	Any	ICMP	Ping
Parameter	Any	TCP	TCP port scan
Parameter	Any	Agent	Check for the presence of the CM agent (AgentGetIdentity)
Parameter	Any	Agent	Ask for the Autodiscovery list of other devices if the parameter CanLearn is enabled (AutodiscoveryListDevices)
Parameter	Any	Agent	Check if the device is a relay (RelayGetValue)

Ldap Synchronization

The CM master acts as a client to the LDAP server to synchronize its groups with those of the LDAP server, that is, devices and users (translated in CM into administrators and users).

Direction	CM Master	LDAP Server	Description
Parameter	Any	LDAP	LDAP synchronization

Timer

Timer

The **Timer** module is a flexible general-purpose module used for all timing functions within an agent. The basic functional principle is that of a list of timer entries each of which invokes an action when the timer "fires". There are many applications internal to the agent which need access to a timer service, not to mention the need for a flexible scheduler for general external use. Types of actions include **Hardware** and **Software** uploads, generating **Reports** , managing **Alerts and Events** or **File Store** functions.

List

The **List** tab of the **Timer** module table displays the list of all currently existing timers with the following information:

Parameter	Description	
Name	The **Name** field specifies the name given to a specific **Timer** .	
Description	The **Description** entry is optional. If it is used it should be a brief descriptive entry of the respective **Timer** and what it relates to.	
Enable Type	This entry defines when the timer will be enabled, possible values are:	
Parameter	**Never**	If the entry is set to this value, the timer will never be enabled and its **Status** value will automatically be `Disabled` .
Parameter	**Immediate**	If the entry is set to this value, the timer will be activated immediately.
Parameter	**Next Agent Startup**	

Parameter	Description	
		Through this value the timer will be activated at the next startup of the agent on the local client.
Parameter	**Every Agent Startup**	This value activates the timer at every startup of the agent on the local client.
Parameter	**Enable Time**	If you select this value, the timer becomes enabled or activated at a specifically defined date and time.
CronSpec	The **CronSpec** field specifies the frequency of execution for each particular **Timer** . The time specification is a crontab-like string made up of the following ranges: secondsminuteshoursdays monthsweekdays Each set of ranges can be preceded by a % sign which will change the meaning from absolute to relative number. For instance if seconds equals 29 the timer will get fired each time the absolute time ends with a number of seconds equal to 29 (for example, 11:43:29) whereas %20 means every 20 seconds every minute, that is, at 13:25:00, 13:25:20, 13:25:40, 13:26:00, and so on. Ranges are comma-separated lists. A range is made of a number eventually followed by a '-' sign and another number or a '*' sign for any value. Number of seconds can vary from 0-59 (max. resolution of 5 seconds). Number of minutes can vary from 0-59. Number of hours can vary from 0-23. Number of days can vary from 1-31. Number of months can vary from 1-12 (1 is January). Number of week days can vary from 0-6 (0 is Sunday). Examples: Every 30 seconds: %30 * * * * * Every December 31st at 0:00: * 0 0 31 12 * At 8:15 and 12:15 every Monday: * 15 8,12 * * 1 Timer fires every day at midnight: 0 0 0 * * * Timer fires every odd month at noon during the week: 0 0 12 * 1,3,5,7,9,11 1-5.	

Working with a Super Master

Working with a Super Master

A super master is limited in its functionality and the objects it provides in the console via its database, because it only consolidates and reports on the data provided by the site masters, which will execute all network management tasks in their part of the organization's infrastructure. The super master stores the inventory data uploaded at regular intervals by the "normal" master servers at the different locations of the organization, and then can generate reports on these.

Depending on the configuration of the site masters, part or all of the following types of inventory data can be consolidated in the super master's database, the data will be uploaded by the site masters right after it was integrated in the local database:

- Device information (name, IP address, domain name, etc.) from the list of autodiscovered devices
- Hardware Inventory
- Software Inventory
- Custom Inventory
- Patch Inventory
- Security Inventory

The super master in itself is completely autonomous, that is, it may create its own configurations for a number of specific objects:

- objects that are required for reporting: queries, device groups, patch groups and reports
- device settings such as when a client is lost.

Connecting to a Super Master console

Connecting with a console to a super master works in exactly the same way as connecting to a site master server. After the console opens on the screen, however the objects displayed will be limited to those you are used to see, because the super master is restricted in its license and thus functionalities.

The dashboard displays only those elements required by the super master, that is, no scanned devices in the Device Distribution, no wizards, and the license box of course includes the license for the super master.

The following top nodes are displayed which again will only display a reduced number of their regular subnodes:

- Search
- Global Settings
- Device Topology
- Device Groups
- Patch Management
- Queries
- Reports
- Events

Super Master Agent Interface

The agent interface is available with its basic tabs apart from the maintenance and MyApps functionalities and the task creation page. Neither is the rollout page accessible however the report portal can be called.

Updates to Security Products Inventory and Virtual Infrastructure Management

BCM supports OPSWAT Endpoint Security Integration SDK (OESIS) framework v4, an OEM technology, that is used to gather security inventory information from BCM managed devices. OPSWAT v4 introduces support for some new Security Products Inventory types, no longer supports some of the earlier inventory types, and has updated the Virtual Infrastructure Management.

See the OESIS v4 website for more detailed information.

This topic lists the changes as a result of upgrading the OPSWAT v4.

What's changed in BCM after upgrading to OPSWAT v4?

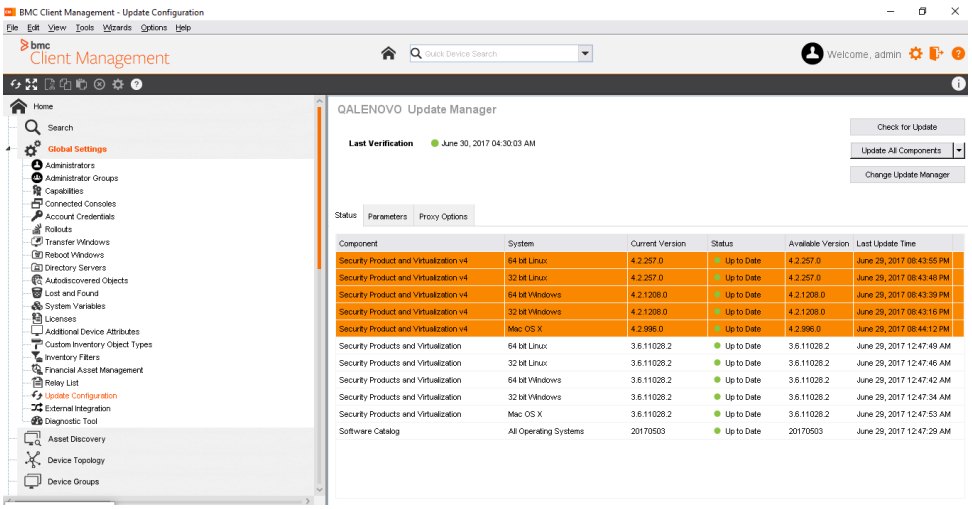
- New Security Products Inventory types
- Unsupported Security Products Inventory types
- Operational rules using new Security Products Inventory types
- Operational rules using new browser operations
- Unsupported browser operations in operational rules
- Queries using new inventory types
- Compliance rules using new inventory types
- Reports using new inventory types
- Virtual Infrastructure Management
- View database log files

Operating systems affected

- Linux (64 bit and 32 bit)
- Windows (64 bit and 32 bit)
- MAC OS X

Viewing OPSWAT v4 entries

After upgrading to BCM 12.6, verify that the **Update Manager** displays the Security Product and Virtualization v4. The status must be Up to Date.



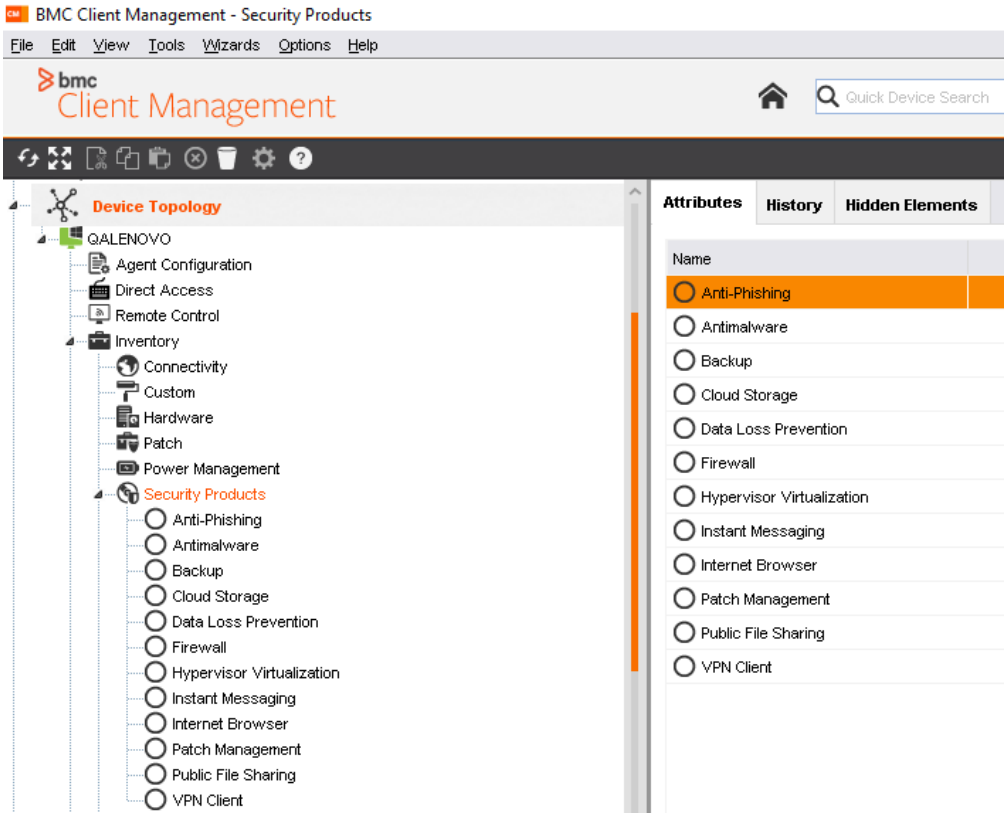
Updates to Security Products Inventory types with OPSWAT v4

This section lists the updates to the Security Products Inventory types after upgrading to OPSWAT v4.

The Security Products inventory list is updated to add some new inventory types, while some existing inventory types are no longer supported in OPSWAT v4.

OPSWAT v3	OPSWAT v4	What's changed in OPSWAT v4
P2P	Public File Sharing	Renamed
Antivirus/Antispyware	Antimalware	Categories merged
URL Filtering		Not supported
DeviceAccessControl		Not supported
SoftwareSuite		Not supported
DesktopSharing		Not supported
SystemManagement		Not supported
	CloudStorage	New Inventory type

The Security Products list reflects the updated categories that are supported by OPSWAT v4.



Operational rules

This section explains the changes to operational rules that are defined with the Security Products Inventory types.

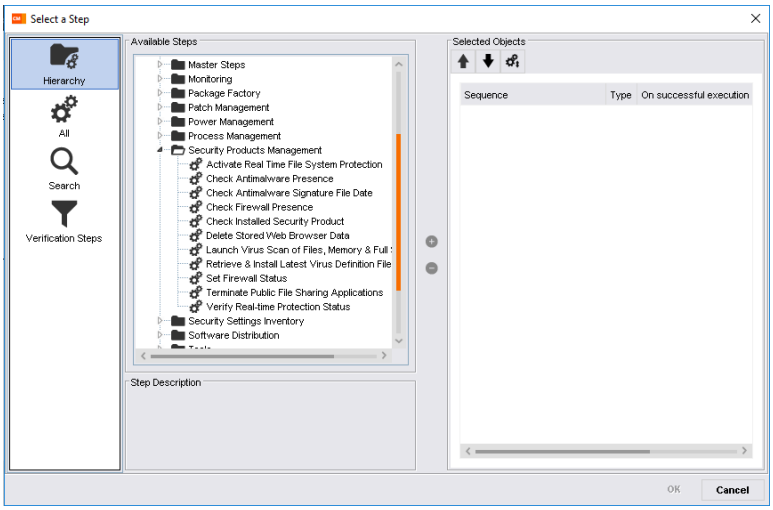
> ⚠ Operational rules created in BCM 12.5 or earlier will continue to work only on devices that are running BCM 12.5 or earlier. These rules cannot be executed on devices that are upgraded to 12.6.

With OPSWAT v4, some browser operations are not supported, while some browser-related parameters are merged into new parameters.

The following steps that are used to create operational rules are not supported:

- Set Browser Home Page
- Set Default
- Check Antivirus presence
- Check Antivirus signature File Date

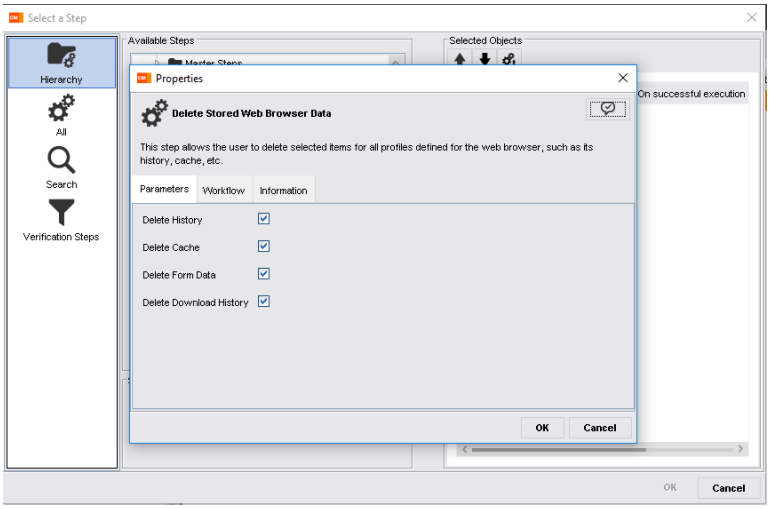
While creating operational rules from the steps listed under Security Products Management, BCM displays the supported steps.



The following browser-related parameters that you see while defining operational rule steps have changed:

OPSWAT v3	OPSWAT v4	What's changed in OPSWAT v4?
Delete History	Delete Browsing History	No Change
Delete Cache	Delete Cache	No change
Delete Addresses		Merged with Delete Browsing History
Delete Passwords		Merged with Delete Forms and Passwords Data
Delete Form Data	Delete Forms and Passwords Data	No Change
Delete Download History	Delete Download History	No Change

The Operational rule step displays the new browser-related parameters.



Queries

This section describes the changes to queries because of some changes to the Security Products Inventory type.

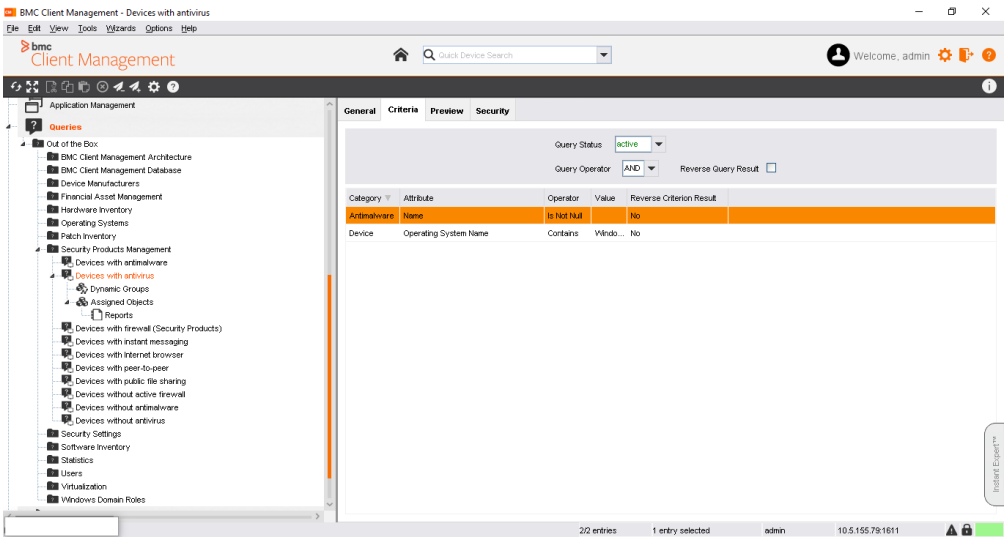
BCM ensures that queries based on criteria that not supported by OPSWAT v4 are retained in BCM 12.6.

Queries built on inventory types that are merged into a new inventory type. The antivirus and anti-spyware inventory types are merged into the antimalware inventory type in OPSWAT v4. BCM ensures that merged inventory types (antivirus/anti-spyware) point to the corresponding new inventory type (antimalware) in BCM 12.6. During the upgrade, BCM merges data from the Antivirus and Anti-spyware into the Antimalware table.

Queries built on inventory types that are not supported in OPSWAT v4, are retained. The data is available in the BCM database, even though devices upgraded to BCM 12.6 do not upload information for the unsupported inventory types to the BCM database.

> ⚠ If a query impacted by the upgrade is assigned to a Dynamic Device Group, the group is set to inactive.

As a BCM administrator, there are no changes because of updates to the inventory type.



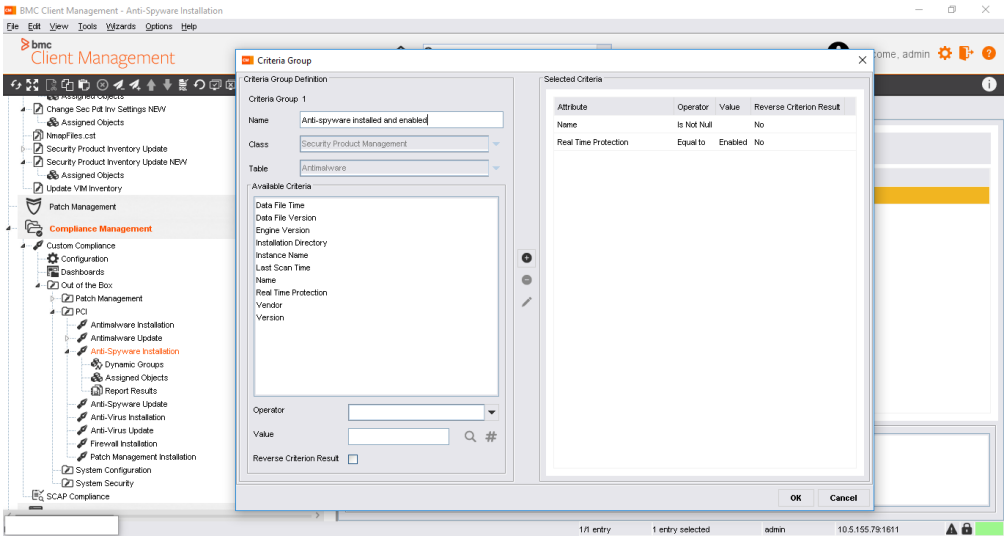
Compliance Management

This section describes the changes to compliance rules because of some changes to the Security Products Inventory type.

After upgrading to BCM 12.6, under the Out of the Box compliance rules, BCM ensures that older compliance rules are retained in addition to the new entries for Antimalware. During the upgrade, BCM merges data from the Antivirus and Anti-spyware into the Antimalware table.

BCM ensures that antivirus and anti-spyware inventory data is merged into antimalware in the BCM database. So, BCM 12.6 displays both inventory types with the same data. You can continue to use the same compliance reports either by renaming the rule name or creating a new one.

> ⚠ If a compliance rule impacted by the upgrade is assigned to a Dynamic Device Group, the group is set to inactive.

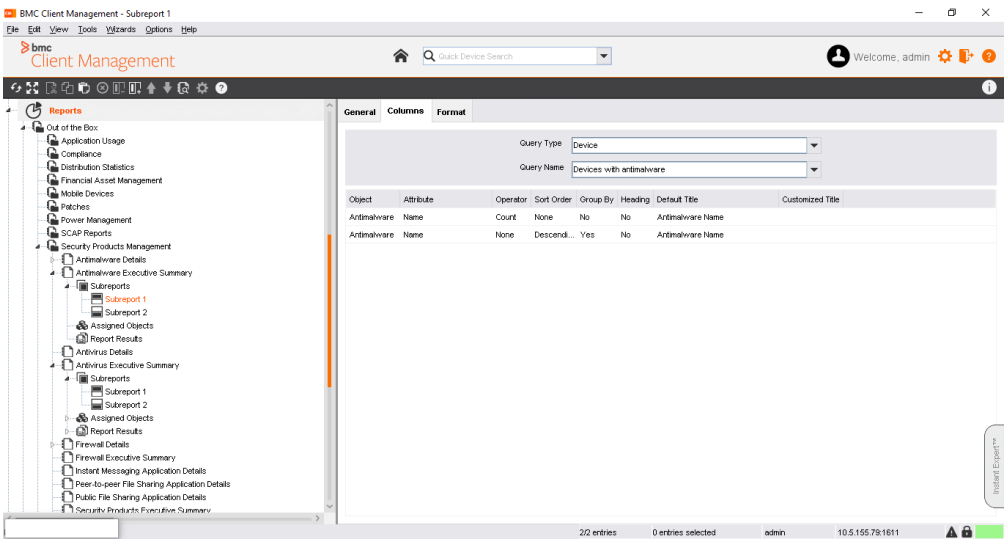


Reports

This section describes the changes to reports because of some changes to the Security Products Inventory type.

BCM ensures that older reports based on antivirus and anti-spyware are retained after upgrading to BCM 12.6. During the upgrade, BCM merges data from the Antivirus and Anti-spyware into the Antimalware table. The important change is that all report data for Antivirus and Anti-spyware data is now stored in the Antimalware table. The older reports can still be used after the upgrade.

For a BCM administrator, there are no changes to reports because of updates to the inventory type.



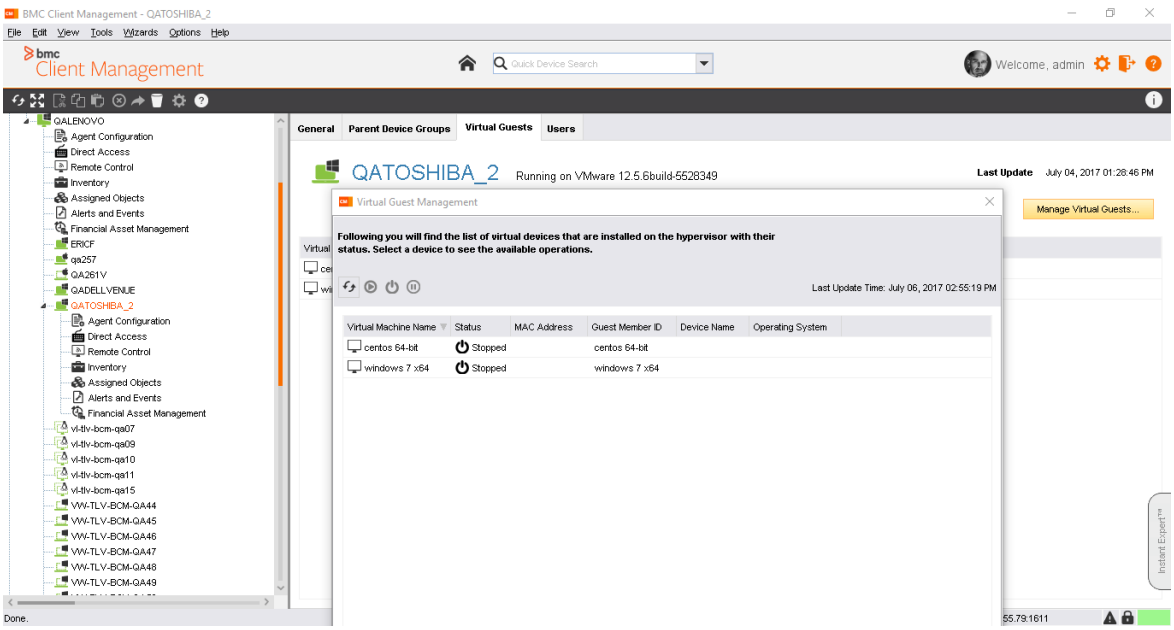
Security Products support matrix

The table shows the supported security products across different operating systems.

Security Products	Windows (BCM 12.6)	Windows (BCM 12.5)	Linux (BCM 12.6)	Linux (BCM 12.5)	macOS (BCM 12.6)	macOS (BCM 12.5)
PUBLIC FILE SHARING (P2P)	✓	✗	✗	✗	✗	✗
BACKUP	✓	✓	✗	✗	✓	✓
ENCRYPTION	✓	✓	✗	✗	✓	✗
ANTIPHISHING	✓	✓	✓	✗	✓	✗
ANTIMALWARE	✓	✓ (Antivirus)	✗	✗	✓	✗
BROWSER	✓	✓	✓	✓	✓	✓
FIREWALL	✓	✓	✓	✓	✓	✗
MESSENGER	✓	✓	✗	✗	✓	✓
CLOUD STORAGE	✓	✗	✗	✗	✓	✗
UNCLASSIFIED	✓	✗	✗	✗	✗	✗
DATA LOSS PREVENTION	✓	✗	✗	✗	✗	✗
PATCH MANAGEMENT	✓	✓	✓	✓	✓	✗
VPN CLIENT	✓	✓	✗	✗	✗	✗
VIRTUAL MACHINE	✓	✓	✗	✗	✓	✓
HEALTH AGENT	✗	✗	✗	✗	✗	✗

Virtual Infrastructure Management

With the upgrade to OPSWAT v4, there is improvement in the BCM agents performance to discover virtual machines on a device that hosts a hypervisor.



View Database log files

The DatabaseUpgrade.log file logs the database changes that happened during the BCM upgrade. You can view the database log file after the upgrade is complete.

A sample log file.

2017/03/28 11:27:58 Vision64Database I [10004] -------- OpswatV4 Migration Start
2017/03/28 11:27:58 Vision64Database I [10004] Add a new table SPMInv_ObjType_819 for Cloud Storage object
2017/03/28 11:27:58 Vision64Database I [10004] Antivirus object is renamed Antimalware
2017/03/28 11:27:58 Vision64Database I [10004] Merge Antispyware and Antivirus data into Antimalware table
2017/03/28 11:27:58 Vision64Database I [10004] The compliance rule Anti-Spyware Installation has been modified to use Antimalware table/attributes instead of Antispyware
2017/03/28 11:27:58 Vision64Database I [10004] The compliance rule Anti-Spyware Update has been modified to use Antimalware table/attributes instead of Antispyware
2017/03/28 11:27:58 Vision64Database I [10004] The compliance rule AntiSpyware has been modified to use Antimalware table/attributes instead of Antispyware
2017/03/28 11:27:58 Vision64Database I [10004] The device group AntiSpyware (Compliant) has been set to inactive, it is dynamically populated with a modified compliance rule
2017/03/28 11:27:58 Vision64Database I [10004] The device group AntiSpyware (Not Compliant) has been set to inactive, it is dynamically populated with a modified compliance rule
2017/03/28 11:27:59 Vision64Database I [10004] The IAntispyware object has been removed

2017/03/28 11:27:59 Vision64Database I [10004] The SPMInv_ObjType_802 table has been dropped
2017/03/28 11:27:59 Vision64Database I [10004] The operational rule step Check Default Browser is disabled
2017/03/28 11:27:59 Vision64Database I [10004] The operational rule step Set Default Browser is disabled
2017/03/28 11:27:59 Vision64Database I [10004] The operational rule step Set Browser Home Page is disabled
2017/03/28 11:27:59 Vision64Database I [10004] The operational rule step Check Antivirus Presence is disabled
2017/03/28 11:27:59 Vision64Database I [10004] The operational rule step Check Antivirus Signature File Date is disabled

2017/03/28 11:27:59 Vision64Database I [10004 The database log files is stoed in master\log

2017/03/28 11:27:59 Vision64Database I [10004] -------- OpswatV4 Migration End

Agent Module Parameters

This section explains in detail all parameters of the different modules of the BMC Client Management that are accessible via the respective nodes in the console:

- Application Monitoring module parameters
- Asset Discovery module parameters
- Asynchronous Actions module parameters
- AutoDiscovery module parameters
- Custom Inventory module parameters
- Custom Packages module parameters
- Event Log Manager module parameters
- File Store module parameters
- Hardware Inventory module parameters
- Host Access module parameters
- HTTP Protocol Handler module parameters
- Identity module parameters
- MSI Packages module parameters
- Operational Rules module parameters
- Patch Management module parameters
- Power Management module parameters
- Relay module parameters
- Remote Control module parameters
- Rollout module parameters
- RPM Packages module parameters
- Security Settings module parameters

Application Monitoring module parameters

The Application Monitoring (ApplicationMonitor) module provides administrators with visibility on installed applications and link them to the business cycle. It allows for the correlation of software inventory data between purchased software to installed software and used software.

Parameter	Default Value	Description
Check Interval (sec)	10	Defines the interval in seconds at which the list of managed applications is monitored on the local client.
Stop Application if Prohibited	**Yes**	Defines if an application that is found to be currently executing is to be terminated if it is defined as being prohibited under the **Prohibited Applications** node.
Display a pop-up window when an application has been stopped	**Yes**	Uncheck this box to not display a pop-up window on the screen to inform the user that the application he just tried to launch was automatically stopped because it is prohibited.
Local Image File Path (bmp only)		The name and full path of the image file that is to be displayed in the pop-up window for a stopped application. The image file must be of type *.bmp* . If the image cannot be found, that is, because it is of another type, or it is too small, the default BMC image is used. If the image is too large it is cropped to fit the window. The default size of the BMC image is 460 x 310.
Popup Window Message Text		The text that is to be displayed on the remote screen on which the application was stopped if a message window is displayed.
Event Creation Delay for Unterminated Monitored Applications (hours)	24	Specifies the number of hours after which an event is created, even if the launched application has not yet been terminated. In this case the end date of the generated event is the same as the start date. Once the application is terminated a new event is generated with the proper end date filled in.

Asset Discovery module parameters

The Asset Discovery module of the BCM Inventory provides all necessary settings to configure a device to execute an asset discovery scan on a remote device on which no BCM agent is installed.

Parameter	Default Value	Description
Parallel Script Count	**Normal**	The maximum number of scripts that can be executed simultaneously, possible values for this are **Low** : 5 simultaneous scripts, **Normal** : 10 simultaneous scripts and **High** : 20 simultaneous scripts.
Max. Timeout	1m	Fine tunes the low level network packets sending, indicating the maximal time to use for scanning a single host. This allows to abort a device scan when it takes too long.
Max. Inventory Timeout	6h	Indicates the global timeout for the whole session. The special value of 0 can be used to deactivate this option, that is, there is no timeout limit for the duration. Otherwise, the scan is aborted once the threshold value has been reached. The value in an integer followed by s for seconds or m for minutes or h for hours.
IP Address Range	80,1610,8080	Indicates the device range to be scanned. The expected format is a comma separated list of IP addresses or IP ranges. For instance, IP ranges must be supplied using different notations such as complete address range (*192.168.0.0-192.168.5.254*), a CIDR range (*192.168.1.0/24* or *2001:db8:85a3::8a2e:370:152/896*), a byte range notation (*192.168.0-5.0-254*) or single named devices (DNS, NetBIOS).nIt is strongly recommended not to specify complete subnet IPv6 address ranges, scanning these is extremely time consuming.
Excluded IP Address Range		Indicates the device range to be excluded from the previously defined range. The expected format is the same as for the included address range. This makes it possible to disable the scan for sensible devices even when using a short notation concerning the included device range (include: *192.168.1.0/24* and exclude: *192.168.1.255,mailserver,fileserver*).
Hardware Inventory	**Yes**	Defines if a hardware inventory is to be executed on the remote device.
Software Inventory	**Yes**	Defines if a software inventory is to be executed on the remote device.
Upload Policy	**Immediate Upload**	Indicates how and when to process the information upload. When set to **Immediate Upload** , the module does upload the inventories as soon as they are supplied by a scan. When set to **Upload at Scan End** , the inventories is uploaded when the scan is completed or aborted (except if the abort operation indicates not to upload). When set to **No Upload** , the module does not upload the inventories at all until specifically called for via the operational rule step.
Nmap Installation Path	../bin	Contains the relative installation path to the BCM software, relative to the agent installation directory, for example, *../bin* if it is located in the bin directory of the agent.
Use Nmap for Port /OS Detection	**Yes**	Defines if BCM, if installed, is used to detect the ports and operating system of the remotely inventoried device.
Prevent NMAP from sending	**No**	Check this box if some of your network devices have problems with IGMP traffic. In this case BCM is prohibited from sending IGMP packets on the network.

Parameter	Default Value	Description
IGMP packets on the network		

Asynchronous Actions module parameters

The asynchronous actions module allows to call asynchronous actions used for inter-agent communication to recover information, such as the operational rule status or the latest identity upload. This module propagates XML/RPC calls through the BCM topology instead of transferring files. It is multithreaded, but will never wait for threads. It also memorizes all information, to save the database read times It however maintains a database, to be able to recover its status and pending actions in case of an agent stop or crash.

Parameter	Default Value	Description
Number of threads	5	Enter the number of threads to use for asynchronous calls
Retry Delay (Priority 0)	300	Enter the retry interval for calls of priority 0 in seconds (highest priority, currently not in use)
Retry Delay (Priority 1)	300	Enter the retry interval for calls of priority 1 in seconds (used for operational rule status and identity uploads)
Retry Delay (Priority 2)	300	Enter the retry interval for calls of priority 2 in seconds (used for operational rule assignments)
Retry Delay (Priority 3)	300	Enter the retry interval for calls of priority 3 in seconds (currently not in use)
Retry Delay (Priority 4)	300	Enter the retry interval for calls of priority 4 in seconds (lowest priority, currently not in use)
Prefer IP Addresses	Yes	Defines whether the identification for communication between the agents and with the master is effected via the agents' IP addresses or over their host names. This is to facilitate networking in environments that do not have DNS name resolution in place.
Object Time to Live (sec)	300	In order to prevent non-transferable data from remaining eternally in the queue, each object is assigned a specific time in seconds that it may stay in the queue and wait to be passed on its way to its destination.
Min Purge Delta Time (sec)	10	The minimum interval (in seconds) between two cleanup operations of the asynchronous actions database of all actions called since the last purge.
Maximum Action Count	100000	The maximum number of actions that can be stored. The module refuses all incoming remote actions until the number of stored actions drops below this value.

Parameter	Default Value	Description
Maximum File Count	100000	The maximum number of files that can be stored. The module refuses all incoming remote files until the number of stored files drops below this value.

AutoDiscovery module parameters

Allows you to access the list of autodiscovered devices and the Autodiscovery module configuration.

Parameter	Default Value	Description
Maximum Device Age (sec)	3600	The maximum age in seconds for an entry in the device list. This is the maximum time a device can stay in the list of devices after last being verified.
Timeout (sec)	5	Defines the timeout value in seconds for pings sent to check for other machines in the neighbourhood.
Address Range		The list of addresses to be verified. The IP addresses can be listed in the following different notations: • Dotted notation, for example, 94.24.127.24 • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24, scotty.enterprise.com* .If the complete IP address range declaration is incorrect, the current subnet is scanned by default from address x.x.x.1 to x.x.x.254. If no IP address range is specified, the current subnet is scanned by default from address x.x.x.1 to x.x.x.254.
HTTP Port Range	80,1610,8080	The range of ports to scan for an agent HTTP server. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 1610 and 8080 is scanned.
Address Verification Interval (sec)	30	The gap in seconds between each address verification.
Number of Neighbors	10	Defines how many neighboring addresses to scan. The default value is 10, meaning 5 addresses below the device's own address and 5 addresses above it.
TCP Port Range	23,25,139	The range of ports to scan for a TCP connection. This is used in place of ping when raw sockets are not available. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 23, 25 and 139 is scanned. Each port range can consist of: • only one port number • one port range with the start and end port numbers separated by a dash  , • several port ranges and/or individual port, for example: 10000-10100,20000,21000-22000

Parameter	Default Value	Description
		• Several port ranges must be separated by either a space, a comma (,), a semicolon (;) or a colon (;). If the whole range declaration is incorrect only default port 10000 is scanned.
Use Network Neighborhood	**Yes**	Defines whether the network neighbourhood should be used to get machine names and addresses.
Same Network Only	3	Specifies if devices found on other networks are to be accepted. The possible values are the following: • **No filter applied** : There is no filter applied to any of the discovered devices. • **Clients only** : All discovered client devices must be on the same network as the discovering device. • **Relays only** : All discovered devices, which have their relay function enabled, must be on the same network. • **All devices** : All discovered devices must be on the same network.
Scan Count	30	Each time **Scan Count** addresses have been verified, the module refreshes the list of addresses to verify by using the **Address Range, Number of Neighbors** and **Use Network Neighborhood** settings.
Can Learn	**Yes**	Specifies that the agent can get other agents' autodiscovered devices in order to establish its list.
Maximum Hop Count	2	The maximum number of routers which may exist between the device providing the list and the device being read. The hop count is determined at discovery time using the ping. It provides an indication of the distance between the two devices and is used at the time of relay selection to sort the devices which are farther to the end of the list of relays being contacted.
Upload on Startup	**No**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Upload Interval (sec)	3600	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Fast Address Verification Interval (sec)	10	Defines a fast search option to find the client's relay. If the list of devices is empty, the **Fast Address Verification Interval** value is used to verify devices until the **Scan Count** value is reached and all devices have been verified or a relay was found. If the client has a relay the **Address Verification Interval** value is used. If the IP address is modified, the **Fast Address Verification Interval** value is used to verify devices. The option is deactivated if the value is set to the same value as the **Address Verification Interval** value. As long as the AutoDiscovery is at the research for the device's relay, the **Parent Selection Retry Interval** to find the backup server is ignored.
Operating System Detection	**Yes**	Specifies that the operating system is discovered on the device found by autodiscovery.
	Yes	Defines if the objects discovered by the autodiscovery are uploaded,.

Parameter	Default Value	Description
Upload AutoDiscovery Module Objects		
Operating System Detection	**Yes**	Specifies that the operating system is discovered on the device found by autodiscovery.

Custom Inventory module parameters

Permits to access the device's custom inventory.

Parameter	Default Value	Description
Data File	../data /CustomInventory /CustomInventory. xml	Specifies the location and name of the custom inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/custominventory. xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the custom inventory may not longer work.
Upload on Startup	**Yes**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Upload Interval (sec)	86400	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Minimum Gap Between Two Uploads (sec)	0	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.

Custom Packages module parameters

The parameters of the Custom Packager module define the default settings for the creation of custom packages in BMC Client Management - Deploy.

Parameter	Default Value	Description
Archive File Extension	.zip	Defines the type of extension for the custom package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.

Parameter	Default Value	Description
Delete Package after Publication	**No**	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Maximum Number of Retries	5	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Retry Interval (sec)	300	Defines the minimum amount of time between each retry for publishing in seconds.

Event Log Manager module parameters

The Event Log Manager tracks events, stores them on the local agent's database, uploads them to the master database according to defined settings and then provides different possibilities to access their content and render it. The following parameters define the standard behaviour of this module.

Parameter	Default Value	Description
Enable Upload of Persistent Events	**Yes**	Defines whether the upload of the events generated for the monitored models is enabled. This value is global for all the managed event log models. When upload is executed for a model (automatically using model policy or manually using an operational rule), the module checks this value. If it is disabled, all events up to the current date are not uploaded. This prevents huge amounts of events to be uploaded on activation.
Enable Aggregation of Persistent Events	**Yes**	Defines whether aggregation of the events generated for the monitored models is enabled. This value is global for all the managed event log models. Aggregation computes automatic models content so disabling this option is recommended if such models should not be handled.
Minimum Upload Gap between Identical Alerts (min)	60	Defines the minimum interval between two same alerts that needs to pass before another alert is sent in minutes.

File Store module parameters

Allows you to access the File Store queue and the module configuration.

Parameter	Default Value	Description
Timeout (sec)	300	The time to wait in seconds before re-notifying a device when the notification failed. This thread is only used by the Notify thread.
Push Timeout (sec)	300	

Parameter	Default Value	Description
		The time to wait in seconds for the push thread if it did not manage to contact the relay. Note that this timeout is randomised between (value - (value/2)) and (value + (value/2)) to smooth the relay load.
Pull Timeout (sec)	300	The time to wait in seconds for the pull thread if it did not manage to contact our relay. Note that this timeout is randomised between (value - (value/2)) and (value + (value/2)) to smooth the relay load.
Object Time to Live (sec)	86400	In order to prevent non-transferable data from remaining eternally in the queue, each object is assigned a specific time in seconds that it may stay in the queue and wait to be passed on its way to its destination.
Queue Delay (sec)	30	Whenever the File Store receives an object to be transported up or down in the hierarchy it puts it in a queue, and this queue is worked through in chronological order. This field here defines the interval in seconds between each check of the queue of objects to move.
Prefer IP Addresses	**Yes**	Defines whether the identification for communication between the agents and with the master is effected via the agents' IP addresses or over their host names. This is to facilitate networking in environments that do not have DNS name resolution in place.
Enable Dialup Downloads	**Yes**	Specifies if downloads are authorised via a RAS (Remote Access Service) connection. If this option is unchecked, then if a dialup connection is detected, the FileStore does not download any information such as inventory. It still receives information about files being available on its relay but it does not make any attempts to download them. Note that on a system which has a LAN connection AND a Dialup connection active at the same time, the module considers itself in dialup mode and behaves as described above. This entry is only valid for Windows devices.
Enable Dialup Uploads	**Yes**	Specifies if uploads are authorised via a RAS (Remote Access Service) connection. If this option is unchecked, then if a dialup connection is detected, the FileStore does not upload any information such as inventory. It still receives information about files being available on its relay but it does not make any attempts to download them. Note that on a system which has a LAN connection AND a Dialup connection active at the same time, the module considers itself in dialup mode and behaves as described above. This entry is only valid for Windows devices.
Threshold for Downloads (bit /sec)	0	Defines whether downstream transfers are blocked if a connection (whatever its type) is too slow. 0 indicates no restriction is imposed on interface speed. The thresholds must be indicated in bits/s such that *10000000* means *10Mbits/s* .
Threshold for Uploads (bit/sec)	0	Determines whether upstream transfers are blocked if a connection (whatever its type) is too slow. 0 indicates no restriction is imposed on interface speed. The thresholds must be indicated in bits/s such that 10000000 means 10Mbits/s.
Frame Size (Bytes)	1492	Defines the frame size of the network type which the device uses for communication. This parameter must only be modified for devices using non-ethernet networks, such as token ring, frame relays or ATM networks.
Multicast Block Size (Bytes)	4096	Defines the rate used for data transfer. The value must be increased as the transfer rate increases. The default value (16384 byte) is the optimum value for 128KB/s transfers. The minimum value is 1024, the maximum 64000.
Multicast Transfer Delay (sec)	3	The delay in seconds before the notification is sent and before sending multicast data. This delay is based on the network resources as well as on the number of clients waiting for distribution. This delay allows the clients to demand the file from the relay.
Multicast Listen Port	2500	Defines the multicast port.

Parameter	Default Value	Description
Multicast Transfer Address	238.4.4.1 - 238.4.4.100	Defines the range of multicast IP address. The server scans the address range and then uses the first available address for the multicast. The address range must be within the following range: 238.4.4.1 and 238.4.4.100.
Multicast Retry Number	5	The number retries to transfer the file, if clients report missing frames. This parameter is reinitialised at each new window transfer slot. If the number of retries is set very high, File Store ensures that the frames are continuously sent through the network. A reasonable value for this behaviour would be 1000 retries for a medium sized network.
Multicast Minimum Success Rate (%)	50	Defines the minimum success rate in percent from which on the transfer is stopped. This parameter is reinitialised at each new wave of clients. To ensure that the retries continue throughout the network as long as possible, this value must be set very high, such as between 85 and 95% per wave of clients.
Multicast Minimum Requests	1	Specifies the minimum number of answers from target clients before launching a multicast transfer. If the number of answers is below the fixed threshold the file is sent unicast to the targets.
Multicast Minimum File Size (Bytes)	65535	The minimum file size for a multicast transfer in bytes.
Multicast Time To Live	32	The multicast Time To Live, that is, the maximum number of nodes the frames can pass before arriving on the target. This is normally set to 1 for local networks up to 255 for worldwide network. To deploy to a national network 32 nodes should be enough and for worldwide distribution 128 nodes normally make sure that the whole network is delivered.
Multicast Differential Retry	**No**	Specifies if differential package retry is to be used. If activated, only those frames that have not yet been received by the client are re-transferred. The differential retry is recommended for a smaller number of target clients (<50).
Unicast Recovery on Multicast Failure	**Yes**	Defines if unicast recovery is to be done if the multicast delivery fails.
Package Time to Live (days)	0	Defines the time to live in days for package files relative to the last time the respective package was asked for by a client. This option is also applicable to the rollout post install files which are kept as a .zip file on the file store. 0 deactivates this option.
Synchronize Packages at Startup	**Yes**	Check this box if the packages are to be synchronized at every startup of the agent. Package synchronization allows a device to send its current list of packages it is assigned to as well as their checksum. The master compares the checksum and if it is different to its own, it sends the master list of packages to the device. In this case the local agent compares its list of packages assigned to the device with the master list and updates it accordingly by deleting the unassigned packages and adding the newly assigned ones.
Minimum Gap between Two Automatic Synchronizations (sec)	43200	Defines the minimum interval in seconds at which the package synchronizations are to be done. This means that if a default synchronization is executed at 23:00 at night and the client is started at 6 am with agent startup synchronization defined, no synchronization is executed until at least 11 am even if the agent is started/restarted before, as the interval is fixed for 12 hours minimum.
Trusted Address		Defines a number of IP addresses from which the local agent is to accept communication in addition to its relay. This allow NAT and VPN communication to work within in the network and the BCM agent, as it recognizes VPN addresses also. Trusted addresses may be entered as single IP addresses or in form of address ranges:

Parameter	Default Value	Description
		• Dotted notation, for example, *94.24.127.24* or *2001:db8:85a3::8a2e:370:7334* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24,2001:db8:85a3::8a2e:370:7334,scotty.enterprise.com* .Several ranges must be separated by a comma (,) or a semi colon (.
Request for Notifications Interval	300	Defines the interval in seconds which may elapse without communication from the relay after which the client re-activates its RequestThread to inquire for new notifications from the relay. After the first received notification, the thread is deactivated.
Immediate Start of Notification Request Process	**No**	Defines if the thread is to be launched without its initial pause.
Package Repository Path		Defines the path to the storage location of referenced packages on the relay, for example, D:Packages, D being the local CD/DVD or USB drive. It is also possible to list more than one path, each path separated by a comma (,) from the next.
Copy from Repository to File Store	**Yes**	Defines if the package is copied into the filestore. If the option is deactivated this means that the medium on which the package is stored must be available on the relay until the last target has collected and installed the package.
Max. Size for Package Conservation (MB)	0	Defines the maximum size that a package may have to be stored in the database in MB. If a package is larger than the indicated value it is stored until no more devices are in its target list and then it is deleted. If all packages are always to be kept and this option is to be deactivated enter 0 into this field.
Concatenation Mode	none	Defines if the file concatenation mode is active for the upload and if yes which one is used. Possible values are **No Upload** ; **Automatic** concatenation means that all files to be uploaded are packed into one archive file and uploaded, **Manual** concatenation indicates that all files are packed to be uploaded as in automatic with the exception of those specified in the **Excluded File Types** parameter which are uploaded separately.
Excluded File Types		Defines all types, separated with a comma (,), which are to be uploaded separately. It is only required for manual concatenation.
Maximum Number of Files to Concatenate	50	Defines the maximum number of files that can be concatenated.
Check for Available Free Space before Downloading a Package	**No**	Check this box if the agent is to verify if there is enough disk space available before actually downloading the package. If not enough space is available an error is logged.

Hardware Inventory module parameters

Allows to access the device hardware inventory.

Parameter	Default Value	Description
Translation File		Defines the .xml format file used to post process the inventory data. The path to the file may be entered as a local path or as a URL such as _ftp://master/hwinvcfg.xml_

Parameter	Default Value	Description
	../data /HardwareInventory /hwinvcfg.xml	. The .xml file contains the list of all Hardware WMI classes available for scanning, but it is only enabled for WMI compliant systems.
Upload on Startup	**Yes**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Upload Interval (sec)	86400	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Minimum Gap Between Two Uploads (sec)	0	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.

Host Access module parameters

The Host Access (HostAccess) module is used to manage the list of IP addresses and host names which are allowed access. Its role is to provide a simple yet efficient lookup service for the HTTP Protocol Handler which uses it to verify whether a request, regardless of content, from a given host is permitted or not. The module only provides a lookup for the host addresses and does not pay attention to what is actually contained in the request. This module is required for the basic functioning of the software and cannot be unloaded.

Parameter	Default Value	Description
Order	1	Specifies the order in which the user access is handled. This order is important, because the Http Protocol Handler goes through this list and accepts the first match it finds.
Host Name		Enter the name of the device on which the proxy is installed.
Permission	**Yes**	Indicates whether a given address or address range is allowed to make requests or not. This, together with the ordered comparison of entries, can be used to implement a "reject most, accept a few" or "accept most, reject a few" policy as desired.

HTTP Protocol Handler module parameters

The HttpProtocolHandler is an HTTP Server. It manages requests from various sources such as the Console, HTML and the remote agent. It rejects requests from sources which do not have the relevant authorizations, capabilities or access rights to execute actions or handle objects.

Parameter	Default Value	Description
Host Name	1610	Enter the name of the device on which the proxy is installed.
Maximum Thread Count	200	Defines the maximum thread counts. The maximum number of threads limits the number of requests which is handled. Requests received whilst there are no free threads available are dropped.
Console Port	1611	The number of the port that the console uses for communication with the agent.
Console Thread Count	200	The maximum number of threads that are reserved exclusively for console communication. For a client at least 4 threads are recommended.
Maximum Number of Retries	3	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Retry Interval (sec)	7200	Defines the minimum amount of time between each retry for publishing in seconds.

Identity module parameters

Allows to configure the Identity module.

Parameter	Default Value	Description
Identity Time (sec)	7200	Defines how often a device is to send its identity up to its parent relay.
Short Identity Time (sec)	300	A special short timer which is setup and executed once after startup to make sure each object is registered in the database right away. This timer can be disabled by setting it to 0.
Check Identity Time (sec)	100	Defines the interval in seconds at which the device's identity is verified via its IP address and GUID.
Execute Script on Changed IP		Allows to execute a specific script when the agent is launched for the first time and every time the IP address of the agent's device is changed, with the exception of *127.0.0.1* or *::1* . Enter here the absolute path to the script.
Launch Script if IP Address Changes to 127.0.0.1	**No**	Defines if the script is also to be executed for the 127.0.0.1 address.
User Time To Live (h)	30	Defines the time to live of the user record in hours. Every detected user entry with a detection time older than this threshold is removed.
Primary User Period (h)	1	Indicates the period in hours to use for computing the primary user.

MSI Packages module parameters

The PackagerMsi module (PackagerMsi) is the method used by BMC Client Management to create Microsoft packages for software distribution. MSI offers the possibility to manage multiple patch application, override default Windows Installer policies if necessary, and optional product features via a simple yet efficient request & delivery service, among other things. This module is loaded by default only on the master if it is a Windows device.

Parameter	Default Value	Description
Archive File Extension	.zip	Defines the type of extension for the custom package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.
Maximum Number of Retries	5	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Retry Interval (sec)	300	Defines the minimum amount of time between each retry for publishing in seconds.

Operational Rules module parameters

The operational rules module defines how and which BMC Client Management function is to be run. These rules are made up of a series of commands called steps executed by the agent. A series of ready-to-use steps are loaded upon startup. Operational rules can run single or multiple actions according to their schedule on individual devices or on the device groups they are assigned to.

Parameter	Default Value	Description
Status-Check Interval (sec)	120	The interval in seconds at which the status values of the operational rules are updated. Any file which has is not yet in transfer is requested again.
Resume rule execution at startup	**Yes**	Defines if any not terminated operational rule is to be continued after a restart of the client.
Delete package after successful distribution	**Yes**	Check this option to delete the package on the client (to free up disk space) once the software distribution has executed successfully.
Enable Simultaneous Rule Execution	**Yes**	Defines if operational rules may be executed in parallel mode.
Synchronize at Startup	**Yes**	Check this box if the operational rules are to be synchronized at every startup of the agent. Operational rule synchronization allows a device to send its current list of operational rules it is assigned to as well as their checksum. The master compares the checksum and, if it is different to its own, it sends the master list of operational rules to the device. In this case the local agent compares its list of operational rules assigned to the device with the master list and updates it accordingly by deleting the unassigned operational rules and adding the newly assigned ones.
Additional Automatic Synchronization Hour	23	Enter here the hour at which an additional synchronization is to be effected, that is, the comparison of locally available operational rules with the operational rules master list. The format is 24-hour format, for example, *23* for *11 pm* .
	43200	

Parameter	Default Value	Description
Minimum Gap between Two Automatic Synchronizations (sec)		Defines the minimum interval in seconds at which the rule synchronisations are to be done. This means that if a default synchronisation is executed at 23:00 at night and the client is started at 6 am with agent startup synchronisation defined, no synchronisation is executed until at least 11 am even if the agent is started/restarted before, as the interval is fixed for 12 hours minimum.
Proceed with Added Rules	**Yes**	Check this box to check for new rules in the base.
Proceed with Updated Rules	**Yes**	Check this box to check for updated rules in the base.
Proceed with Deleted Rules	**Yes**	Check this box to check for deleted rules in the base.
Proceed with Published Rules	**Yes**	Check this box to check for published rules in the database.
Proceed with Operational Rules	**Yes**	Check this box to check only for operational rules in the database.
Proceed with Software Distribution Rules	**Yes**	Check this box to check only for distribution rules in the database.
Proceed with Quick Link Rules	**Yes**	Check this box to check only for Quick Link rules in the database.
Only Proceed with Not Received Rules	**Yes**	Check this box, if only rules for which the assignment has been sent but after 12 hours still have not been received by the local agent.
Output File	../log /OperationalRules.log	Defines the path to the log file relative to the installation directory: • **none** : There is no debugger output regardless of the other settings. • **stdout -sa -cw** : The debugging output is sent to the standard output. • **file** : The debugging output is written to a file whose name is to be specified in this field with a path relative to the agent installation directory, for example, *../../logs/namp.log* for a file located on the same level as the installation directory, not below.
Maximum Agent Log Size (Byte)	5000000	The maximum size of the log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified at all, there is no limit check on the size of the file.
Maximum Agent Log File Count	5	Maximum number of log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Activate Operational Rule Publication for Users	**Yes**	Defines if rules may be published to users. If activated, the module checks on the master if rules are available to be published to a user, otherwise rules are not published.

Parameter	Default Value	Description
Automatic Status Upload	**Yes**	Defines if the current status of the operational rule is automatically updated. If the option is deactivated, no status value is updated, however status actualization can still be done via the *Update Operational Rule* step or via an operational rule synchronisation.
Recreate Local Database If Integrity Check Fails	**No**	Defines the actions to be executed if the database check fails at agent startup due to its corruption. If this parameter is activated, the local database is recreated and the master reassigns all operational rules for the concerned devices, depending on the settings defined in the system variables (Automatic reassignment of all general operational rules if the local database is corrupted and Automatic reassignment of all software distribution rules if the local database is corrupted). If it is deactivated that no status values is updated any more and no synchronisations be performed.
Failed to check the chronological dependencies if the rule execution is failed	**No**	Check this box if an operational rule that depends on another rule is not executed if the rule it depends on does not have the status *Executed OK* . If this option is not activated, the depending rule is executed even if the first rule's execution failed.

Patch Management module parameters

The Patch Management (PatchManagementPremium) module is completely automated to make patching painless: it scans, remediates and reports on your whole network autonomically to keep security patches on a large number of applications of different manufacturers up to date. This module is loaded by default only on the master if it is a Windows device.

Parameter	Default Value	Description
Scan machine on startup	**No**	Defines if the device is scanned for the current patch situation at agent startup.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Synchronize at Startup	**No**	Patch synchronization allows a device to send its current list of patch groups it is assigned to as well as their checksum. The master compares the checksum and if it is different to its own it sends the master list of patch groups to the device.
Additional Automatic Synchronization Hour	23	Enter here the hour at which an additional synchronization is to be effected, that is, the comparison of locally available operational rules with the operational rules master list. The format is 24-hour format, for example, *23* for *11 pm* .
Minimum Gap between Two Automatic Synchronizations (sec)	43200	Defines the minimum interval in seconds at which the rule synchronisations are to be done. This means that if a default synchronisation is executed at 23:00 at night and the client is started at 6 am with agent startup synchronisation defined, no synchronisation is executed until at least 11 am even if the agent is started/restarted before, as the interval is fixed for 12 hours minimum.
	Yes	Check this box to activate the verification for new versions of the Knowledge Base via the Internet. This value is only applicable to the Patch Manager, for all other devices this value should be deactivated.

Parameter	Default Value	Description
Enable Internet Check for Knowledge Base Update		
Internet Check Schedule for Knowledge Base Update	**Every Day** , **at** , 23:00	Click the **Edit** icon to the right of the field to define or modify the schedule for the Knowledge Base update via Internet. Select the desired values from the options in the appearing window.
Automatic Knowledge Base Update after Check	**Yes**	Check this box to automatically update the configuration files with the newly found version of the files. If activated this option only downloads the file if the file is of a newer version than the version currently available on the Patch Manager, or if the **Force Parse** parameter is activated. It then directly updates the local file.
Upload New Inventory if New Version is Detected	**No**	If a new version of the Knowledge Base is detected on the Patch Manager, it automatically launches a new patch inventory scan via the respective operational rule and uploads the results.
Patch Process Interval (sec)	60	Manages the patch module thread execution, defining the interval in seconds at which requests on the database are executed.
Archiving of Downloaded Patches after Publication		Defines if the patches are stored in the **download** directory of the Patch Manager after the patch custom package was created and successfully published to the Master. If the option **Move** is selected, you need to fill in the following field **Path for Local Patch Repository** which defines the path to the local storage location.
Path for Local Patch Repository		Defines the local path which the patch module checks if the patch to be downloaded is already available locally there before actually downloading it from the Internet.
Download Retry Count	1	Specifies the number of retries for a patch download.
Download Retry Interval (sec)	300	Defines the interval in seconds between each retry for the patch download.
Block Patch Installation	**No**	Check this box to prepare the patch installation on all targets of the group for execution, without launching the installation itself.
Maximum number of concurrent downloads	3	Defines the number of patches that can be downloaded simultaneously.

Power Management module parameters

This module (PowerManagement) provides the administrator with the necessary functionalities to implement power management, also known as GreenIT, policies within the organisation's IT infrastructure to reduce its overall energy consumption. These policies are implemented and applied via a special group of operational rules. The following parameters are available:

Parameter	Default Value	Description
Log Events	**No**	Specifies if the events that are generated are to be logged on the local database.

Relay module parameters

The Relay module is used to manage the client/relay relationship. A relay is a client machine which also acts as an intermediary between the client and the master server. It is located on the next higher hierarchy level than the client. Depending on the size of the network more than one level of relays may exist.This module is required for the basic functioning of the software and cannot be unloaded.

Parameter	Default Value	Description
Is Enabled	**Yes**	Displays if the current device is a relay. If the relay functionality is deactivated the device is only a simple client. Only a client which has been verified by the AutoDiscovery and received the status *Verified* may be a relay. This field defines if the current device is to be a relay. If the relay functionality is deactivated the device is only a simple client.
Child IP Address Range		The IP address range in which the children below the currently selected device may be found if it is enabled as a relay. If a client outside the IP range specified here, tries to define this device as its relay, it is rejected. The addresses may be entered as single IP addresses or in form of address ranges: • Dotted notation, for example, *94.24.127.0-94.24.127.24 - 2001:db8:85a3::8a2e:370:152-2001:db8:85a3::8a2e:370:896* , or *94.24.127.0-24 - 2001:db8:85a3::8a2e:370:152-896* or *94.24.127.0/24 - 2001:db8:85a3::8a2e:370:152/896* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24, 2001:db8:85a3::8a2e:370:152, scotty.enterprise.com* . Several ranges must be separated by a comma (,).
Rejected Relays		Defines a list of clients, which are NOT to be used as a relay for other clients, such as the master server or other specific devices. The devices may be listed with their short or long network names, such as *scotty* or *scotty.enterprise.com* or their IP address in dotted notation. The field may also contain a range of devices in the form of *192.1.1.1-192.1.1.4,2001:db8:85a3::8a2e:370:152-896,kirk, scotty* or *192.1.1.1-kirk* or *kirk-scotty* .
Parent Name		The name of the direct parent to which the target device is to be connected. This is either the master or the new device's relay on the next higher level. The name may be entered as the short or long network name, that is, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, that is, *192.168.1.1* or *2001:db8:85a3::8a2e:370:7334* . You may also select the parent from the list of available devices by clicking the **Add Device** icon and selecting the desired parent from the appearing list.
Parent Port		The port number of the direct parent to which the device is connected.
Tunnel to Parent	2	Defines if the agent creates and maintains a tunnel with its parent. Be aware that **Auto Detection** has a slight impact on the performance. Use **Yes** if the network configuration is such that the relay cannot directly connect to its clients.
Tunnel Compression Level	0	Defines compression level to use when building a tunnel to the parent, the possible values range from 0 to 9, 0 meaning no compression and 9 the highest compression.
	0	

Parameter	Default Value	Description
Lost Parent Verification Retry Count		The number of times a device tries to contact the device defined as its parent, if the contact cannot be established at the first try. If after this count the contact still cannot be established the agent moves on to the selecion mechanisms defined by the **Mechanism List** parameter for dynamic relay selection. For static relay selection this mechanism loops until a connection with the defined relay was established again if this value is set to *0* and the **Interval between Lost Parent Verifications** parameter is set to a value greater than *0* . If both values are set to *0* the reselection is disabled, which is NOT recommended.
Interval between Lost Parent Verifications (sec)	0	The time interval in seconds between each try to contact the parent.
Interval between Parent Verifications (sec)	0	Defines the timout delay in seconds after which the currently connected parent is to be verified. If the connection with the parent cannot be established, the parent resynchronization process defined via the **Lost Parent Verification Retry Count** and **Interval between Lost Parent Verifications** parameters is started. This process is disabled if currently no parent is connected or if the parameter value is set to *0* .
Reselection Interval (sec)	3600	Defines the interval in seconds between attempts at selecting a "better" parent than the current one. This selection is done even if the current parent is contactable. This option is disabled if the value is set to 0 or if currently no parent is connected.
Parent Selection Retry Interval (sec)	60	Defines the interval in seconds at which the client tries to locate the parent relay it belongs to. This option is only enabled if currently no parent device is connected, that is, the device is *orphaned* . It is disabled if a parent is connected or if the value is set to *0* .
Mechanism List	60	Defines the order in which the dynamic relay selection methods are applied. You must enter the methods in form of a comma (,) separated list, the list is read from left to right. The following relay selection methods are available: **dhcp, list, static, autodiscovery, script** and **backup** . If this parameter is empty the **Parent Name** and **Parent Port** parameters is used as static parent information.
Static Parent Name	60	The name of the direct parent to which the target device is to be connected in static mode. This value is ignored if the dynamic relay selection is activated, that is, at least one value is entered in the **Mechanism List** field. The direct parent is either the master or the new device's relay on the next higher level. The name may be entered as the short or long network name, that is, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, that is, *192.168.1.1* or *2001:db8:85a3::8a2e:370:7334* . You may also select the parent from the list of available devices by clicking the **Add Device** icon and selecting the desired parent from the appearing list.
Static Parent Port	60	The port number of the direct parent to which the device is connected in static mode. This value is ignored if the dynamic relay selection is activated, that is, at least one value is entered in the **Mechanism List** field.
List Server URL	60	The URL to the BCM agent on which the actions to find the appropriate relay are to be executed, generally this is the Master.
DHCP Extended Option	60	The number of the option defined in the DHCP Server that corresponds to the relay.
Script Path		Provides the relative or absolute path to the script. The path may also be entered as a valid URL starting with _ http://_

Parameter	Default Value	Description
		or _ https://_ , in which case the script is downloaded every time it is referenced. This parameter is mandatory of the **script** option is listed as a dynamic relay selection mechanism in the **Mechanism List** field.
Backup Relays		A list of backup parents to be scanned if during the auto selection no suitable parent is found through AutoDiscovery. The format is *host1:port1,host2:port2,* etc. *Host 1* is the closest alternative to the regular relay and the last host listed is typically the master. The host name can be entered either as its long or short network name, for example, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, for example, *192.168.56.4* or *2001:db8:85a3::8a2e:370:7334* . If the port number is not listed the default port *1610* is assumed.
Execute Script at Connection to Backup Relay		Allows to execute a specific Chilli script every time when a connection is established with a backup relay. Enter here the absolute path to the Chilli script.
Execute Script at Disconnection from Backup Relay		Allows to execute a specific Chilli script every time when the connection with a backup relay is terminated. Enter here the absolute path to the Chilli script.
Share Point Path for Administrative Install		The path to the administrative installation point for MSI packages. You may define the path as a UNC path with the following syntax: *UNC[IPAddress][MsiFiles]* , whereby *[IPAddress]* is the remote device and *[MsiFiles]* the remote network share. When using an UNC path the administrator login and password must be specified as they is used to perform a **Run As** on the machine. This option does not work if the agent is running under a *LocalSystem* account that cannot access network shares. If you are using IPv6 addresses you must use the following format: *FD43-0-0-0-8C84-4BAD-D413-DD68. ipv6-literal.net* .
Share Point Name for Administrative Install		The name of the administrative installation point for MSI packages.
Administrator Login for Administrative /Network Installation		The login name of the device's administrator who has all necessary access rights to log on to remote devices.
Administrator Password for Administrative /Network Installation		Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
Short Storage Path	**No**	Defines if the short or the long storage path for the network and administrative installation is used on the relay. If deactivated the package is stored under the location *[RelativePath]/[PackageName.msi] /checksum* , whereby *[RelativePath]* represents the directory structure in the Console under which the package was created. If it is activated, the package is stored directly under the *[RelativePath]* directory and a checksum subdirectory is created containing the *installpackage.zip* file.

Parameter	Default Value	Description
Share Point Path for Network Install		The path to the network installation point for custom packages. You may define the path as a UNC path with the following syntax: *UNC[IPAddress][CustomFiles]* , whereby *[IPAddress]* is the remote device and *[CustomFiles]* the remote network share. When using an UNC path the **Administrator Login** and **Password** must be specified as they is used to perform a **Run As** on the machine. If the agent is running under a *LocalSystem* account, this option does not work because this account cannot access network shares.
Share Point Name for Network Install		The name of the network installation point for custom packages.
Automatically Install Package on Network Share	1609	Defines if the packages are installed on the relay via an administrative and/or network install. At module startup, the relay performs a check on the disk to look for packages that are to be installed on the network share: • **None** : The relay only stores the packages but does not install them. • **Administrative** : The respective MSI packages is put on the share as defined in the **Share Point Name for Administrative Install** parameter and installed on their destination. • **Network** : The respective packages (MSI and custom) is put on the share as indicated in the **Share Point Path for Network Install** parameter and installed on their destination if they are MSI packages. • **All** : Both network and administrative packages is put on the shares as defined by the **Share Point Path** parameters above and installed on their destination if they are MSI packages.
Bandwidth Check Port	1609	Specifies the port number on which the bandwidth is calculated, which is available to the device for downloads from the relay.
Bandwidth Check Frequency (sec)	60	The delay in seconds between two calculation phase.
Client Check Frequency (sec)	10	Defines the interval at which the device verifies with the relay how many devices are currently downloading from the relay in seconds. If set to 0 the client check is disabled.
Bandwidth Check Duration (ms)	200	The calculation phase's duration in milli-seconds.

Remote Control module parameters

The Remote Control (RemoteControl) module provides remote access to managed devices within the network. The remote management of devices includes the access of remote services such as network applications, the transfer of files among servers and workstations, administering of servers or the taking control of managed devices to help users with problems.

Parameter	Default Value	Description
Automatic Disconnection	**Yes**	Specifies automatic disconnection, that is, if the Remote Control is left inactive for a given period of time, the administrator is automatically disconnected.
Hour(s)	0	The number of hours of inactivity after which the connection is automatically terminated.
Minute(s)	10	The number of minutes of inactivity after which the connection is automatically terminated.
Second(s)	0	The number of seconds of inactivity after which the connection is automatically terminated.
Install and use the Client Management video driver	**Yes**	Allows to activate the BCM video driver for improved speed performance, more precise display of the target screen and a less important CPU usage during the connection. This functionality also provides a larger choice of color systems which allows to considerably reduce the bandwidth consumption for slow networks while still clearly displaying the target screen in monochrome mode. This option is not available if the **Deactivate Hardware Acceleration** parameter is activated. If it is activated the driver is loaded at agent startup. It is strongly recommended to reboot the device if this option is activated.
Activate Remote Control Information in the Log	**No**	Defines if logging is enabled, If it is activated, logging is enabled in the agent log file, mtxagent.log.
Activate Detailed Logging	**No**	Defines the detail level of remote control logging. If activated, logging takes places with maximum information.
Activate Connection Logging	**Yes**	Defines if administrator connections are to be logged.

Rollout module parameters

The Rollout module is used to carry out agent installation, reinstallation or upgrade on the remote machines of your network. Two deployment methods can be used: Push and Pull, which can either be started immediately or scheduled. This module is loaded by default only on the master.

Parameter	Default Value	Description
Max. Number of Simultaneous Devices	10	The number of devices a rollout can install at the same time.

RPM Packages module parameters

The RPM Packages (PackagerRpm) module is the method used by BMC Client Management to create Linux specific packages for software distribution. RPM packages are capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc. This module is loaded by default only on the master if it is a Linux device.

Parameter	Default Value	Description
	.zip	

Parameter	Default Value	Description
Archive File Extension		Defines the type of extension for the custom package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.
Maximum Number of Retries	5	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Retry Interval (sec)	300	Defines the minimum amount of time between each retry for publishing in seconds.

Security Settings module parameters

The Security Inventory (SecurityInventory) module shows if the related device includes the Security Inventory module. By default, when the agent is installed, the Security Inventory module is configured to be loaded at start time if the required license is valid. The security inventory in BCM Inventory allows you to collect information pertaining specifically to the security and vulnerability aspect of your devices. The Security Inventory is collected via operational rules.

Parameter	Default Value	Description
Data File	../data /SecurityInventory /SecurityInventory. xml	Specifies the location and name of the security inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the security inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master /SecurityInventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the security inventory may no longer work.
Upload on Startup	**Yes**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Upload Interval (sec)	86400	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Minimum Gap Between Two Uploads (sec)	0	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.

Security Product Management module parameters

The parameters of the Security Products Management Inventory module define the default settings for the custom inventory of BCM Inventory, that is, the inventory generation and upload sequences and frequencies.

Parameter	Default Value	Description
Data File	../data /SecurityProductsManagement /SecurityProductsManagement. xml	Specifies the location and name of the security products inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the security inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/SecurityProductsManagement.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the security products inventory may no longer work.
Upload on Startup	**Yes**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Upload Interval (sec)	86400	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Minimum Gap Between Two Uploads (sec)	0	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Additional Anti-Virus Data	**Yes**	Check this box to collect advanced data on installed anti-virus software products (virus definition file date, etc.) and upload them to the Security Products Inventory.
Additional Firewall Data	**Yes**	Check this box to collect advanced data on installed firewall software products (firewall status) and upload them to the Security Products Inventory.
Additional Anti-Spyware Data	**Yes**	Check this box to collect advanced data on installed anti-spyware software products (anti-spyware definition file date, etc.) and upload them to the Security Products Inventory.
Additional Browser Data	**Yes**	Check this box to collect advanced data on installed browser software products (CERT compliance, etc.) and upload them to the Security Products Inventory.

Selfhealing module parameters

This module (SelfHealing) proactively detects unintentional application, file and configuration changes and automatically corrects errors on client systems, so that end-user quality is maintained. It increases the autonomy of the agent with the regards to software failure. The module is only applicable to Windows and Linux devices.

Parameter	Default Value	Description
Check Interval (sec)	30	Defines the interval in seconds at which the protected applications are verified for their integrity on the local client.

Snapshot Packages module parameters

The PackagerSnp (PackagerSnp) module is another of the methods used to create BMC Client Management packages. This method generates a *before* and *after* system snapshot, that is, before and after configuration changes or software installation, enabling administrators to thus customise packages to fit their needs. This module is used for basic package distribution. It is loaded by default only on the master if it is a Windows device.

Parameter	Default Value	Description
Archive File Extension	.zip	Defines the type of extension for the custom package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.
Maximum Number of Retries	5	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Retry Interval (sec)	300	Defines the minimum amount of time between each retry for publishing in seconds.

Software module parameters

The Software Inventory (SoftwareInventory) module provides the administrator with an inventory of all software packages installed on a specific device. By default, when the agent is installed, the software module is configured to be loaded at start time. This module is quite flexible and may be extended by the administrator as required.

Parameter	Default Value	Description
Translation File	../data/SoftwareInventory /swinvcfg.xml	Defines the .xml format file used to post process the inventory data. The path to the file may be entered as a local path or as a URL such as _ftp://master/swinvcfg.xml_ .
Scan Add /Remove Programs	**Yes**	Defines if registry entries for the Add/Remove Programs are to be scanned and added for the software inventory update.

Parameter	Default Value	Description
Scan MSI Database	**Yes**	Defines if the MSI Windows database is to be scanned for the software inventory update.
Excluded Directories	* /winsxs,${TEMP},${TMP}	Defines a comma separated list of directories to exclude during the scan for inventory. The entry is not case sensitive and may use the *?* and **wildcard characters, for example, **WINNT*,*AVG?.VAULT*** , ***Documents and Settings*** . The supplied list is removed from the scan list which itself is either specified in the Included Directories field or is automatically set to all the fixed disks. When excluding a directory from the scan, all of its sub-directories are excluded as well.
Included Directories		Defines a comma separated list of directories which are to be scanned for inventory. If nothing is supplied, the default behaviour is to scan the contents of all fixed drives. If anything is supplied, only the directories specified and their children are scanned.
File Extensions to Scan	exe	Defines the file types by their extension, which are included in the software directory scan.
Scan Hidden Files	**No**	Defines if files marked as hidden on the system are included in the file scan.
Scan Hidden Directories	**No**	Specifies if directories marked as hidden on the system are included in the directory scan.
Upload on Startup	**Yes**	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Upload Interval (sec)	86400	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Update Interval (sec)	43200	Defines the update period in seconds for inventory scans on the remote devices.
Differential Upload	**Yes**	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only the delta, that is, the modifications of the inventory. If the inventory template is changed the next inventory will always be a complete inventory, even if this option is activated.
Minimum Gap Between Two Uploads (sec)	0	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.

Timer module parameters

The Timer module is a flexible, general purpose scheduler used for all timing functions within an agent. It assures that specific actions take place at set times. This module is required for the basic functioning of the software and cannot be unloaded.

Parameter	Default Value	Description
Take Logged User into Account	**Yes**	Defines if the connected user is to be taken into account when executing an operational rule. By default the rule is executed when the user, who activated the rule in MyApps, is connected. If another user is connected to the device it is not executed.

Update Management module parameters

The parameters of the Update Manager module allow you to define if, which and when the automatic updates are executed.

Parameter	Default Value	Description
Retry Delta After Version Check Failure (sec)	0	Define in seconds the interval that must elapse before the agent checks for a new version again after a verification failure.
Retry Delta Between Two Synchronizations (sec)	0	Define in seconds the interval to elapse between two synchronizations.

User Access module parameters

The User Access (UserAccess) module displays the list of users who have access to a specific agent. This module is required for the basic functioning of the software and cannot be unloaded.

Parameter	Default Value	Description
Order		Specifies the order in which the user access is handled. This order is important, because the Http Protocol Handler goes through this list and accepts the first match it finds.
Name		The user access name. It is simply used as a display name, but it must be unique anyway.
Login		The login name for a specific user or group of users.
Authentication Type		The Authentication Type is related to the login and can be one of the following categories: • **Private** : Private should be used if the user is to log on with a proper name, for example, *Scotty, Kirk* , etc. A user logged on in this category is required to give a password which is to be defined below. • **System** : If this authentication is used the login and password are verified by the system. • **Action** : If an access is defined as Action, its login and password are verified by the call of the specified action.
Password		This parameter is not appliable if the value of the **Authentication Type** parameter is **Action** .
Action Name		This parameter is only appliable if the value of the **Authentication Type** parameter is **Action** .
Confirm Password		The type of operation which is monitored on the counter.

Virtual Infrastructure Management module parameters

The parameters of the Virtual Infrastructure Management module allow you to define the modules behavior.

Parameter	Default Value	Description
Local Inventory Check Interval (sec)	43200	Defines the interval in seconds between each upload of the inventory of the local virtual machine and its upload to the master.

Wake on LAN module parameters

This modules (WakeOnLan) permits to remotely power-on managed devices that have a LAN adapter which can activate the Wake On LAN function on supported motherboards being able to send and receive wake-up packets.

Parameter	Default Value	Description
Local Wake-up Mechanism	**Yes**	When enabled, the module checks whether the target and itself is part of a common subnet. In that case, the wakeup is performed by the module itself using the subnet broadcast address.
List of Wake Up Devices		Defines a comma separated list of devices elected for the wake-up process. In this case, the registered devices are used as static proxies and the module respects the list order (from left to right). There is no deep check concerning the wake-up devices such as IP address and network mask.
Automatic Wake-up Mechanism	**Yes**	Agents have the capability to monitor the data flow and remember the list of devices for which they are the direct relay. Therefore, modules are able to look up possible devices that share a common subnet with another device to wake up. This option enables the capability to look up this dynamic knowledge base and detect the list of possible wake-up devices. This is the dynamic version of the previous option.
Fallback Wake-up Mechanism	**None**	This fallback parameter allows trying a last wake-up mechanism. It is often used when none of the previous mechanisms have succeeded, or if some of them were disabled. The aim is to proceed to the wake-up using a blind method. When set to **Unicast** the module tries a simple host directed unicast wake-up (a simple UDP packet sent to the exact destination address). When set to **Broadcast** , the module tries a subnet-directed broadcast (a simple UDP packet sent to the entire network). When set to **DirectBroadcast** , the module tries a direct broadcast considering the target network address. When set to **None** , the fallback mechanism is disabled.

Web API module parameters

This module activates the SDK for using web services, which is required to integrate with BCM. Loading this module opens the respective port and the calls to the web services are accepted.

Parameter	Default Value	Description
Server Port	1616	Defines the TCP port dedicated to the web services.
Listening Addresses	0.0.0.0,::	Comma separated list of local addresses (ipv4 and/or ipv6) on which we will listen. By default, addresses are 0.0.0.0,::, which means listen on all IPV4 and IPV6 addresses.

Parameter	Default Value	Description
Trusted Address	1616	Defines a number of IP addresses from which the local agent is to accept communication in addition to its relay. This allow NAT and VPN communication to work within in the network and the BCM agent, as it recognizes VPN addresses also. Trusted addresses may be entered as single IP addresses or in form of address ranges: • Dotted notation, for example, *94.24.127.24* or *2001:db8:85a3::8a2e:370:7334* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24,2001:db8:85a3::8a2e:370:7334,scotty.enterprise.com* .Several ranges must be separated by a comma (,) or a semi colon (;).

Windows Device Management module parameters

The Device Management module (DeviceManagement) provides the administrator with the possibility to create specific policies for Windows devices and their peripherals.

Parameter	Default Value	Description
Log Events	**No**	Specifies if the events that are generated are to be logged on the local database.

Logging Parameters

The parameters in this view define the basic settings for log files of the software, that is, the values specify the contents of granularity of the log files as well as their output location for example. This also includes the log file sizes and numbers, which types of entries are to be logged, the time format, if alerts are to be sent in case of logged errors, etc.

Parameter	Description
Output File	Defines the path to the log file relative to the installation directory: • **none** : There is no debugger output regardless of the other settings. • **stdout -sa -cw** : The debugging output is sent to the standard output. • **file** : The debugging output is written to a file whose name is to be specified in this field with a path relative to the agent installation directory, for example, *../../logs/namp.log* for a file located on the same level as the installation directory, not below.
Enable List	A comma separated sequence of message filter names which are to be output to the log file. The special character * means all possible values, an empty string disables the list.
Disable List	A comma separated sequence of message filter names which are to be filtered from going to the log file. The special character * means all possible values. By default the disable list is applied AFTER the enable list and so has a higher precedence.
List to Load First	Defines if the debugging is executed according to the principle of everything being disabled with some exceptions or everything being enabled with some exceptions. This system is defined through two lists, the **Disable List** and **Enable List** , which are explained following.

Parameter	Description
Displayed Types	A comma separated list of debug message types which are to be output to the log file. The special character * means all possible values.
Maximum Agent Log Size (Byte)	The maximum size of the log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified at all, there is no limit check on the size of the file.
Maximum Agent Log File Count	Maximum number of log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Agent Log Clean Start	Defines if the specified log file is to be backed up at each start of the agent. If enabled the log file specified in **Output File** is backed up at agent start time.
Maximum Audit Log File Size (Bytes)	Controls the maximum size of the audit log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified the limit is the value of the **Maximum Agent Log Size** entry.
Maximum Audit Log File Count	Maximum number of audit log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Audit Log Clean Start	Defines if the specified audit log file is to be backed up at each start of the agent.
Column Separator	The separator character between the columns in the output. If no value is supplied, the output is padded out for readability. If a value is supplied, no text padding is done.
Time Format	A formatting string used to format the timestamp part of the logged output. This field may however contain any string of characters the administrator deems appropriate and the variables may be ordered in any desired way. The variables this entry may contain are the following: %y for the year part of the timestamp with 4 digits, for example, 2004, %m for the month as its number, for example, 01 for January and 12 for December, %d for the day of the month, %H for the hour indication, %M for the minutes of the hour and %S for the seconds of the minute.
Send alert when an error occured	Check this box if an alert is to be sent to the master when an error is added to the agent log file.

Modifying the Configuration Settings

To modify the settings of any aspect of the agent configuration, proceed as follows:

1. Select any line in the table in the right window pane of the respective topic.
2. Click **Edit > Properties** .
   The **Properties** window appears.
3. Make the appropriate modifications to the individual values.
4. Click **OK** to confirm the modifications and close the window.

SCAP compliance module parameters

Permits to access the device's custom inventory.

Parameter	Default Value	Description
OVAL Directives	Full With System Characteristics	This parameter defines the OVAL directives that must be applied to OVAL results. This has an impact on the level of detail for generated XML result files which are temporary files emitted during the scans.

Mobile device management module parameters

The following are the module parameters for a device designated as mobile device manager:

Parameter	Default Value	Description
Enrollment URL	***serverName:portNumber***	Displays the URL built based on the server name and port number specified. This URL is shared with the users who need to enroll their iOS mobile devices. The user enrolls their mobile devices by clicking this URL.
Server Name	IP address	Displays the name or IP address of the device designated as mobile device manager. This value should not change. If the Server Name is changed, it also modifies the enrollment URL. The mobile devices already enrolled with the original URL will not be able to communicate with the mobile device manager if the enrollment URL changes.
Server Port	1661	Displays the port number which is used to build the enrollment URL.
Server Certificate		Displays the server certificate used for authentication. If not available, a temporary certifiacte is issued each time the agent service is started.
Signing Certificate		Displays the signing certificate used for authentication. If not available, a temporary certifiacte is issued each time the agent service is started.
Notification Thread Count	2	Displays the number of notification threads to be opened. To disable notification, specify the value as 0. If two or more mobile device managers are configured with a value greater than 0, only one mobile device manager is used for notification.

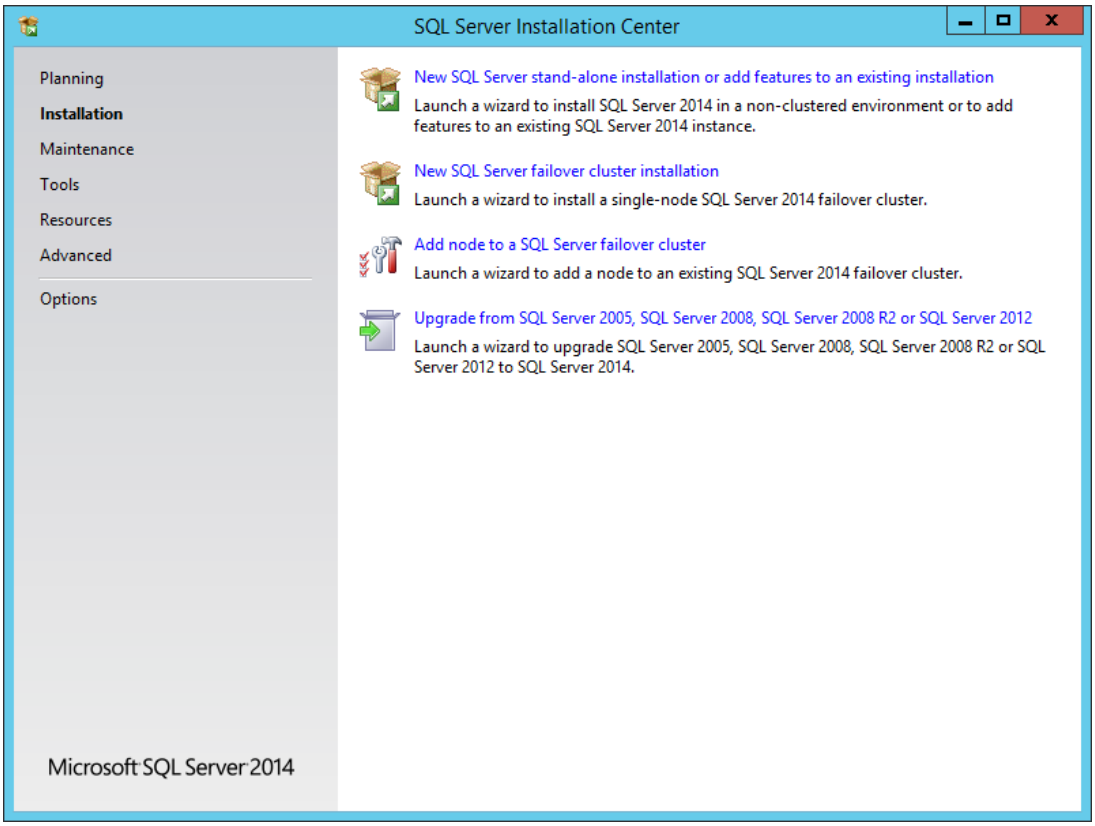
Database installation and configuration reference

This section guides you through the installation of the different types of database engines that can be used with Client Management . This section includes the specific installation options and configurations required to run the software on it:

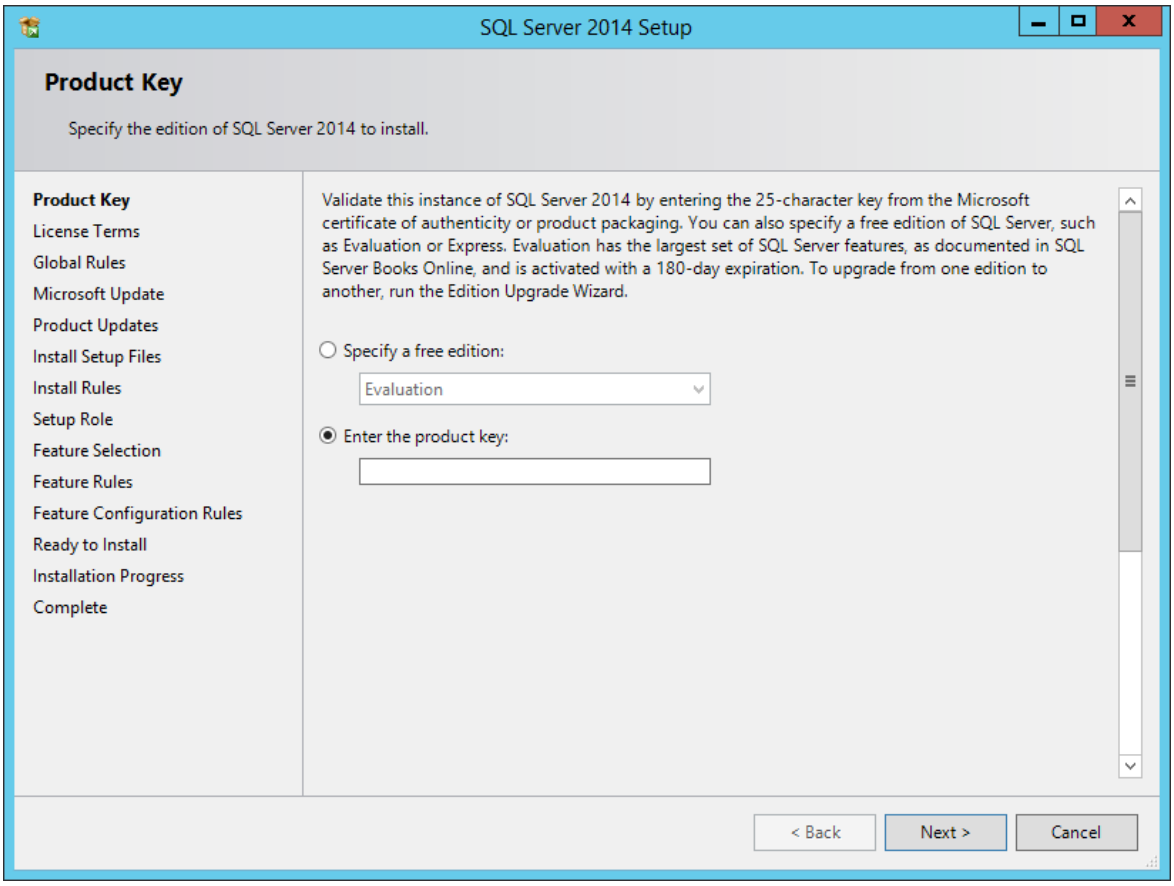
- Installing Microsoft SQL Server 2014
- Configuring Microsoft SQL Server 2014
- Installing PostgreSQL
- Configuring PostgreSQL
- Installation and configuration of Oracle 12c Release 1 (12.1.0.2) on Linux 6

Installing Microsoft SQL Server 2014

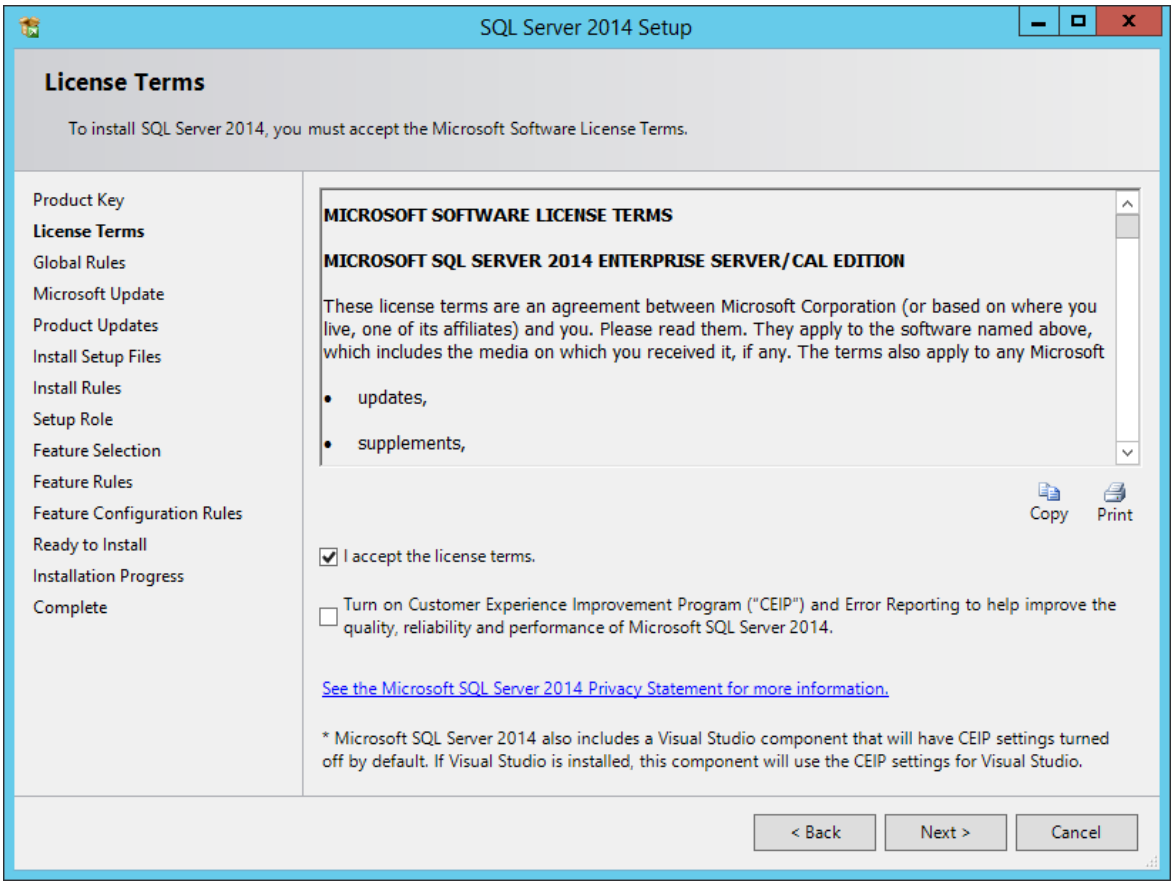
1. Start `setup.exe` .



2. Click **Installation** in the left window part and **New SQL Server stand-alone installation** ... at the right.
   The **SQL Server 2012 Setup** wizard is launched.
3. Enter your product key in the **Product Key** window and click **Next** .

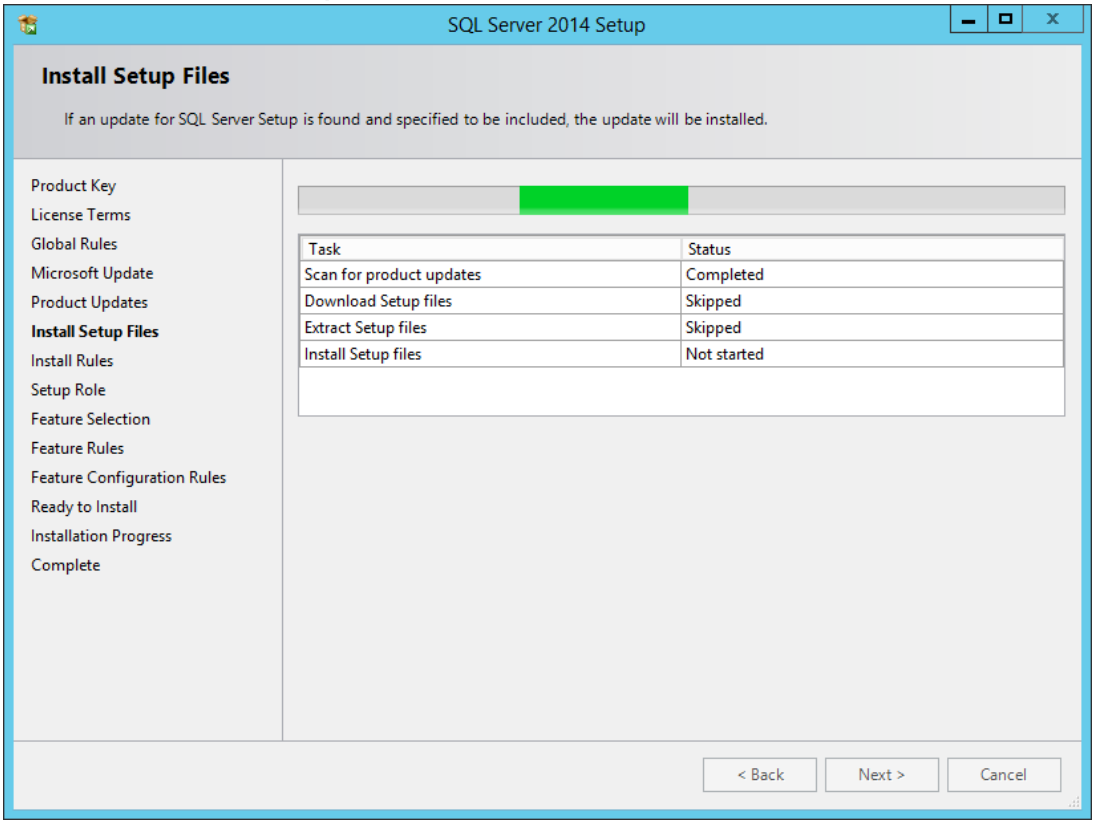


1. Check the **I accept the license terms** box in the **License Terms** window and click **Next** .



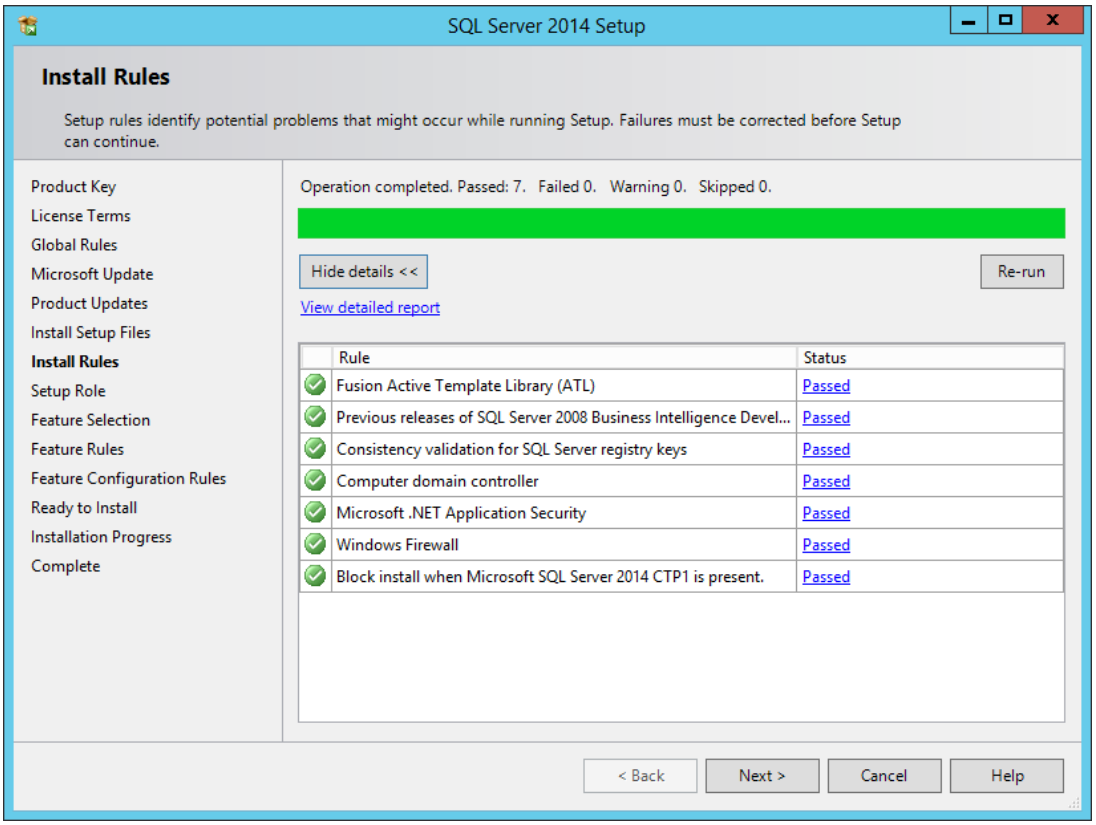
1. Check if there are any updates available after your computer has established the connection to the SQL Server internet. If there are no updates to be installed, click **Next** , otherwise install these and restart this procedure.

2. Click **Next** .The **Install Setup Files** window appears on the screen.

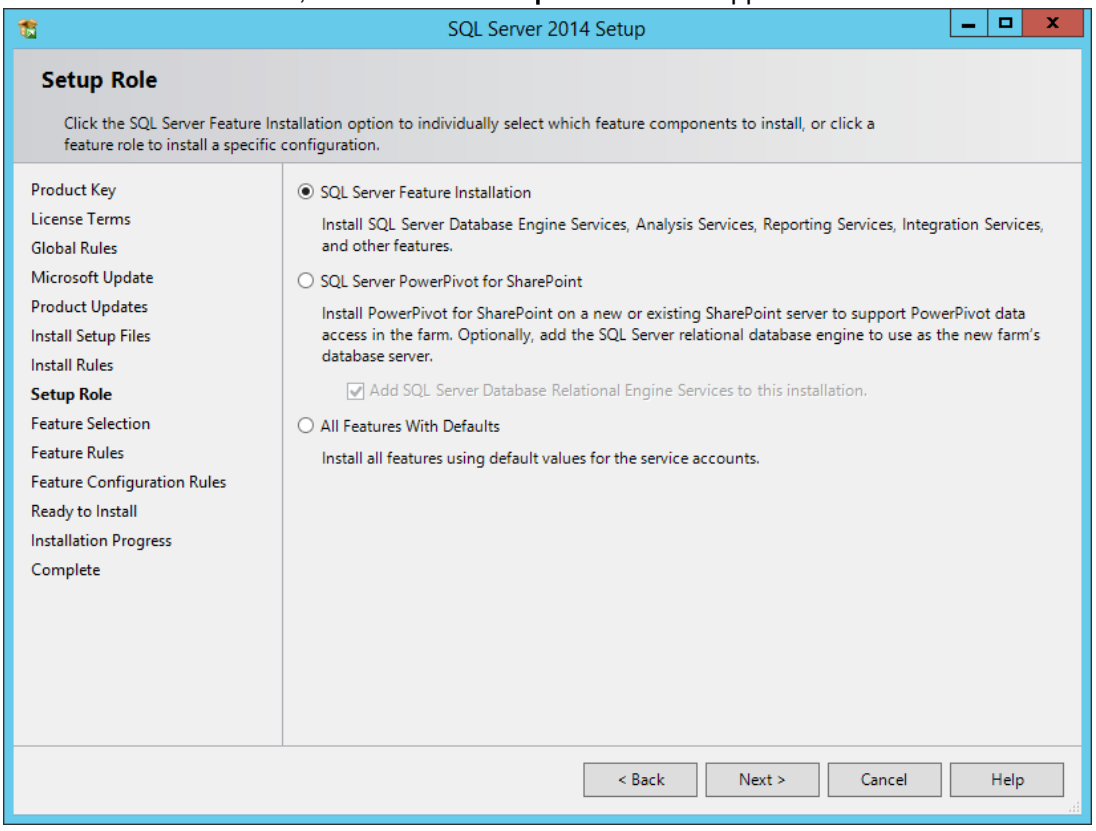


3. Click **Next** .The **Install Rules** window appears on the screen and starts some initial tests.

> **Note:**
>
> Click **Details** / **Hide Details** to display or hide the tests and test results.

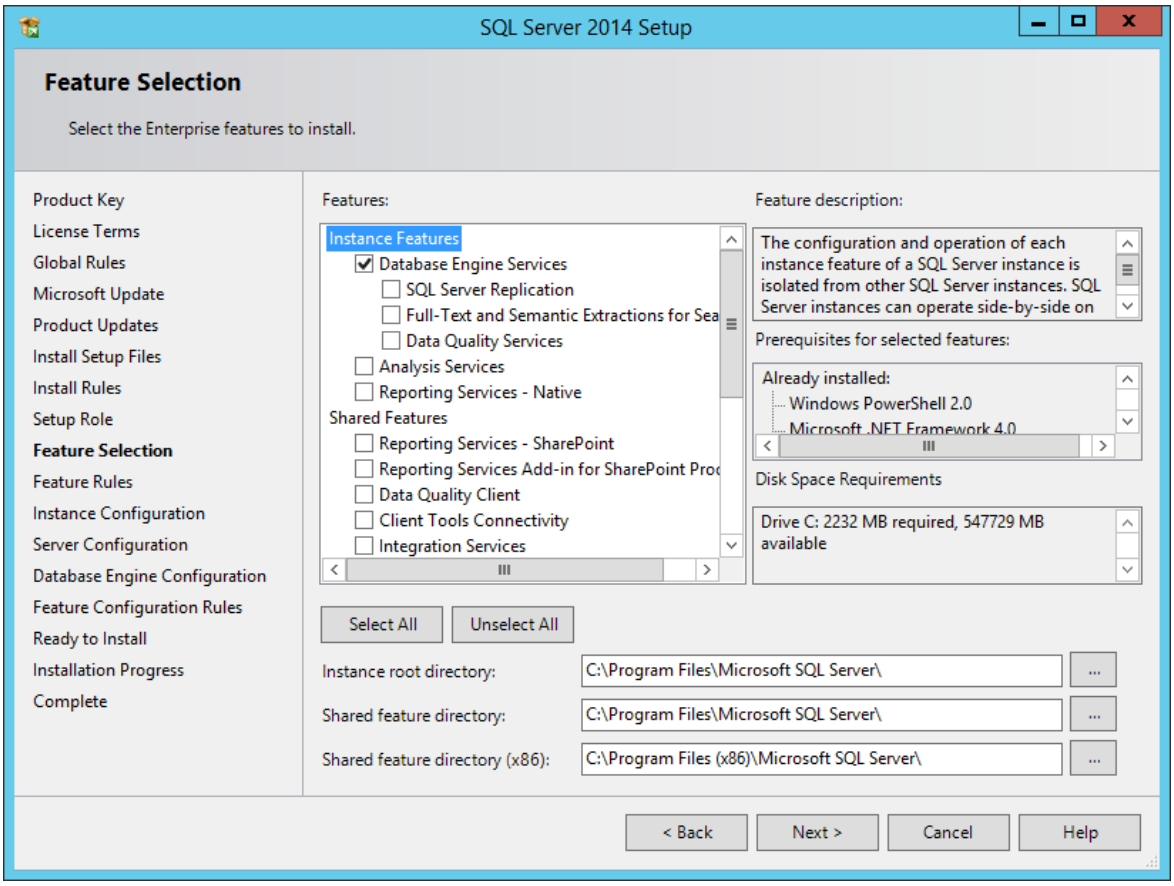


4. If no issues are indicated, click **OK** .The **Setup Role** window appears.



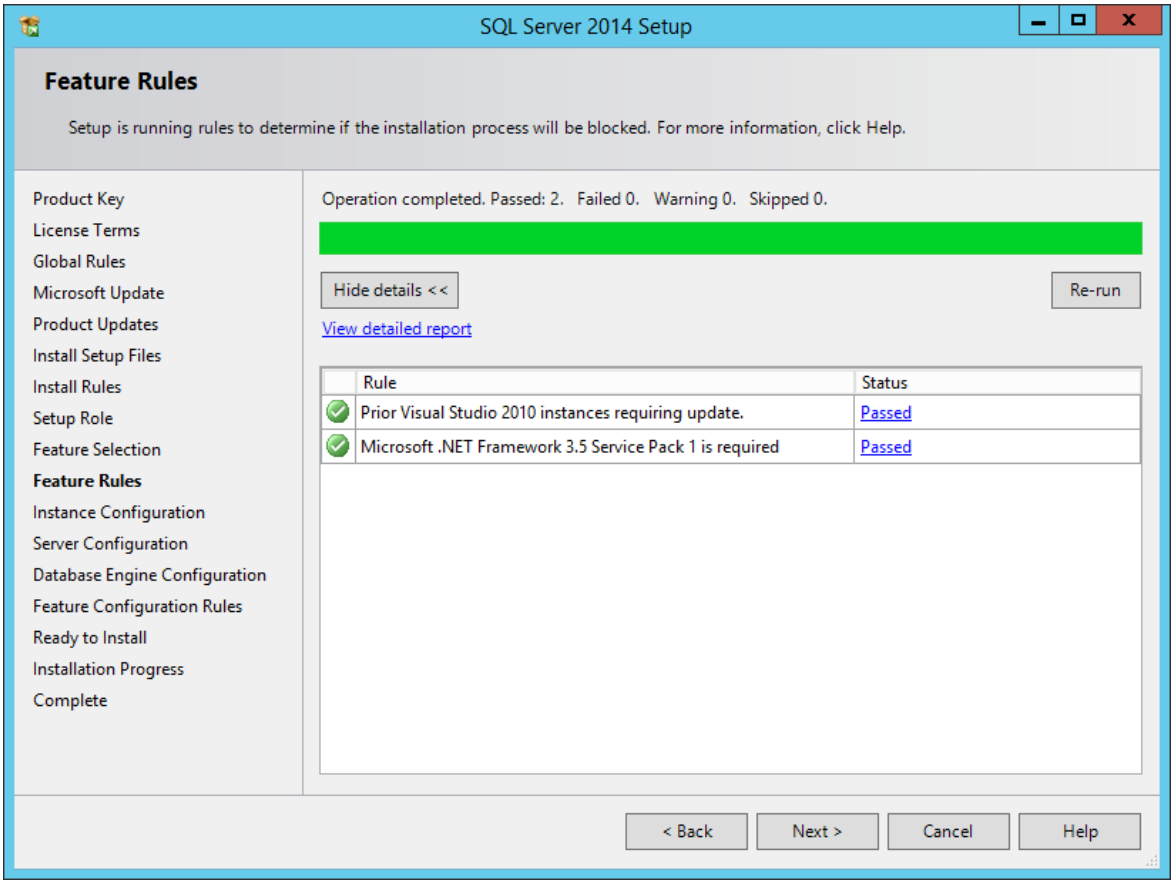
5. Select **SQL Server Feature Installation** .

6. Click **Next** .
7. Select the rquired functionalities and modify, if necessary, the setup procedure in the **Feature Selection** window.

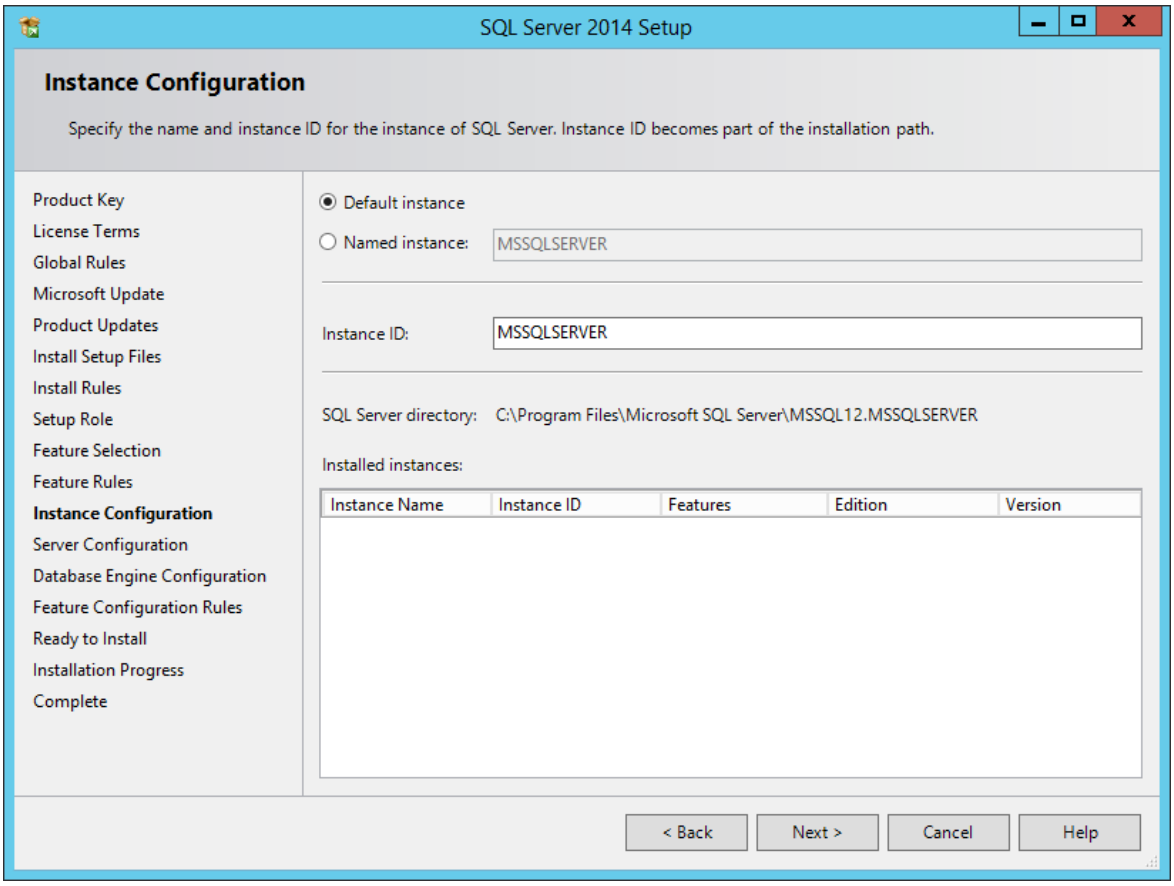


Do not forget to tick the two boxes concerning the **Management Studio** .

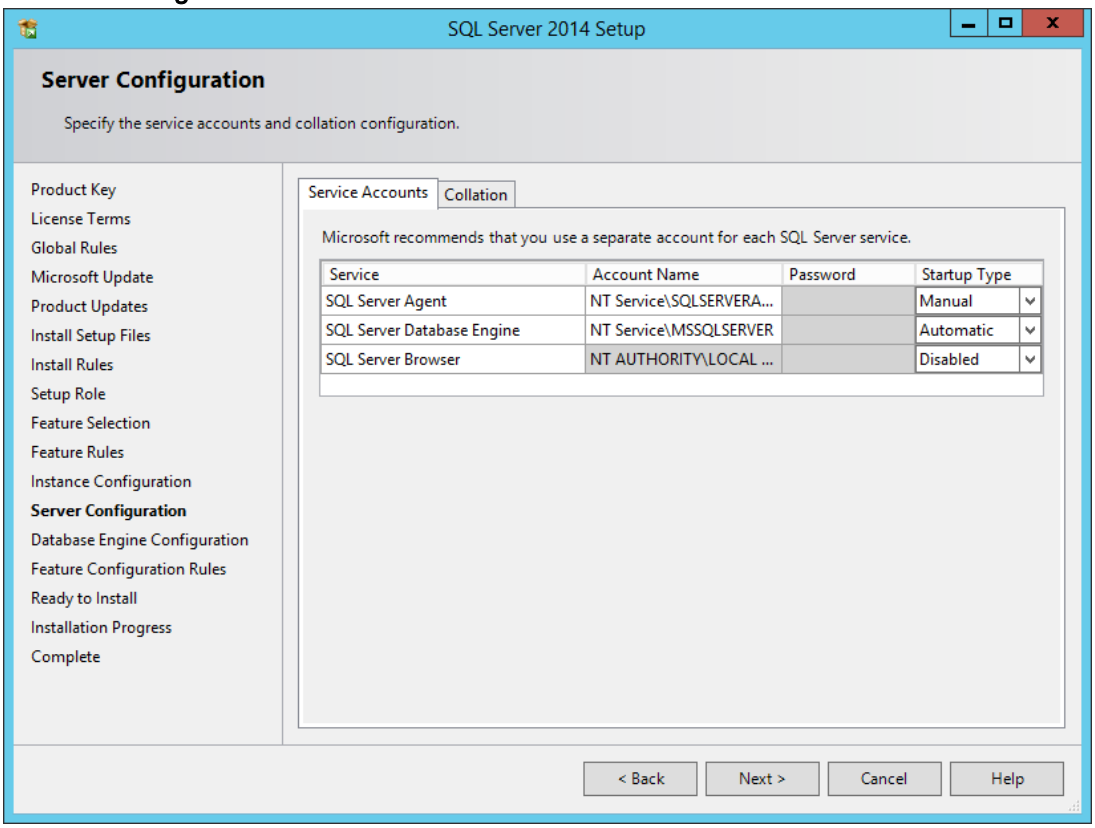
A test is executed and its results are shown in the **Features Rules** window.



1. If no issues are indicated, click **Next** .

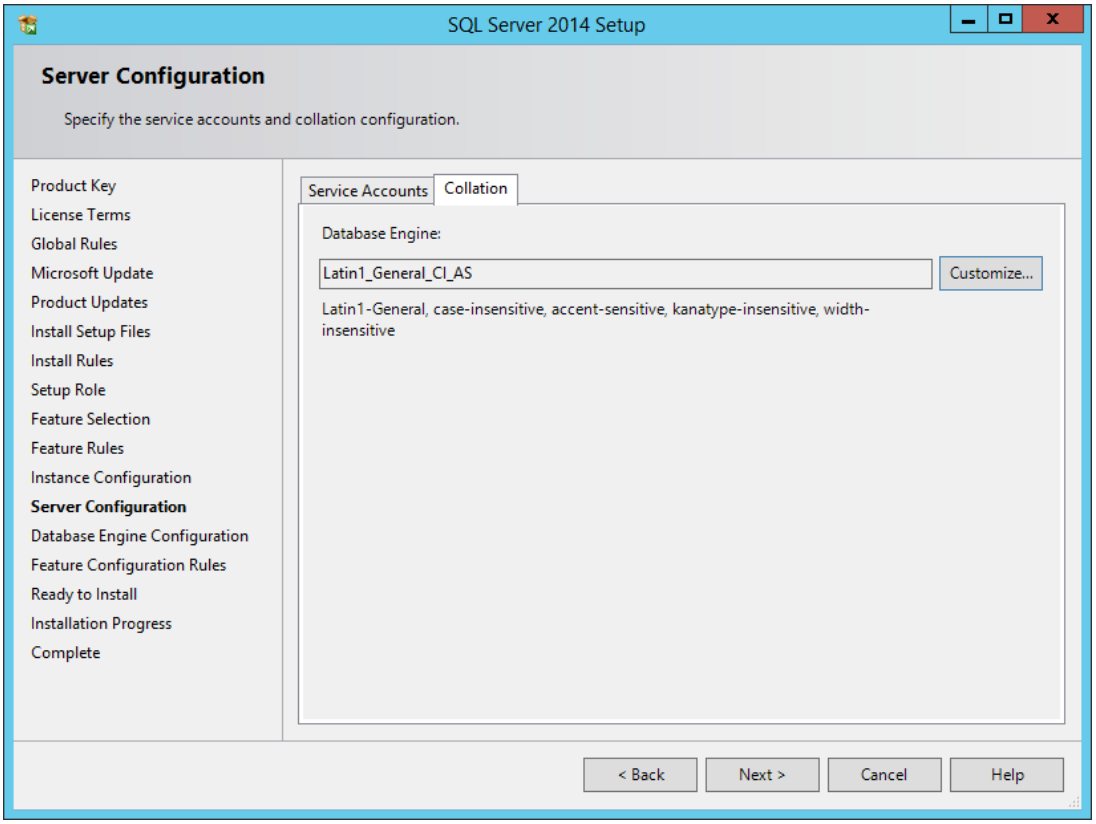

SQL Server 2014 Setup
Instance Configuration
Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Default instance
Named instance:
MSSQLSERVER
Instance ID:
MSSQLSERVER
SQL Server directory:
C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER
Installed instances:
Instance Name
Instance ID
Features
Edition
Version
< Back
Next >
Cancel
Help

1. Keep the first option selected or choose a named instance and enter your instance ID in the **Instance Configuration** window. Click **Next** to continue.

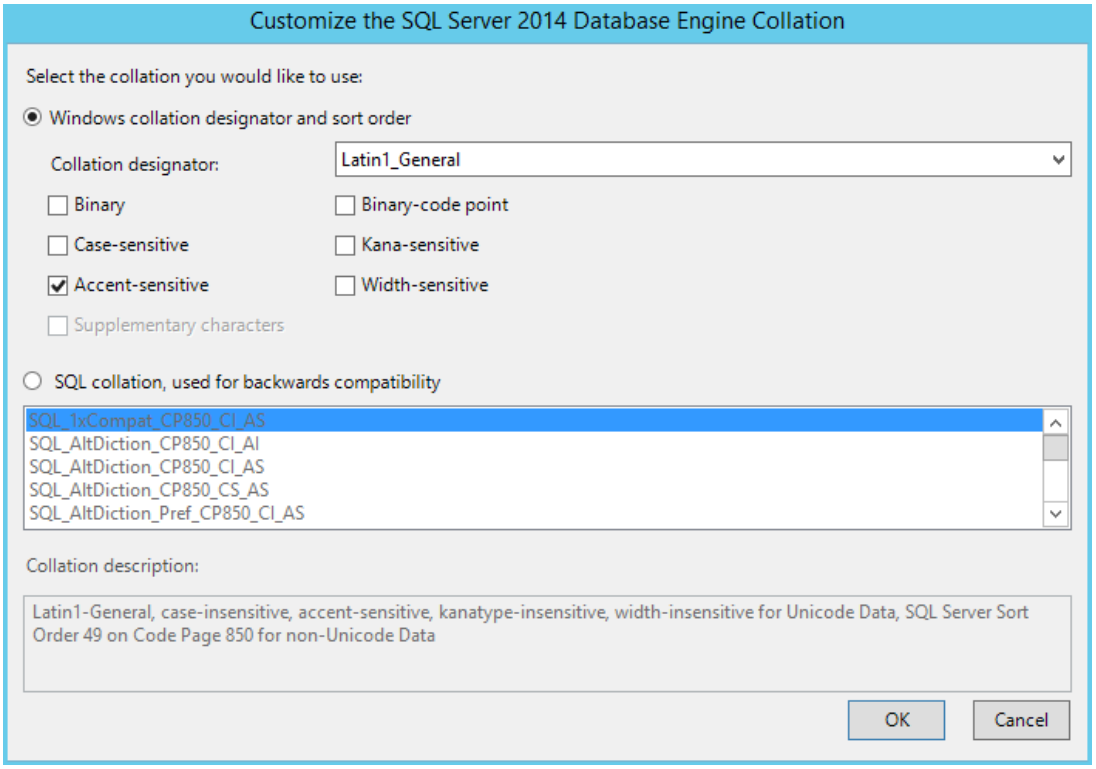


2. Configure the services as shown in the screenshot in the **Server Configuration** window.

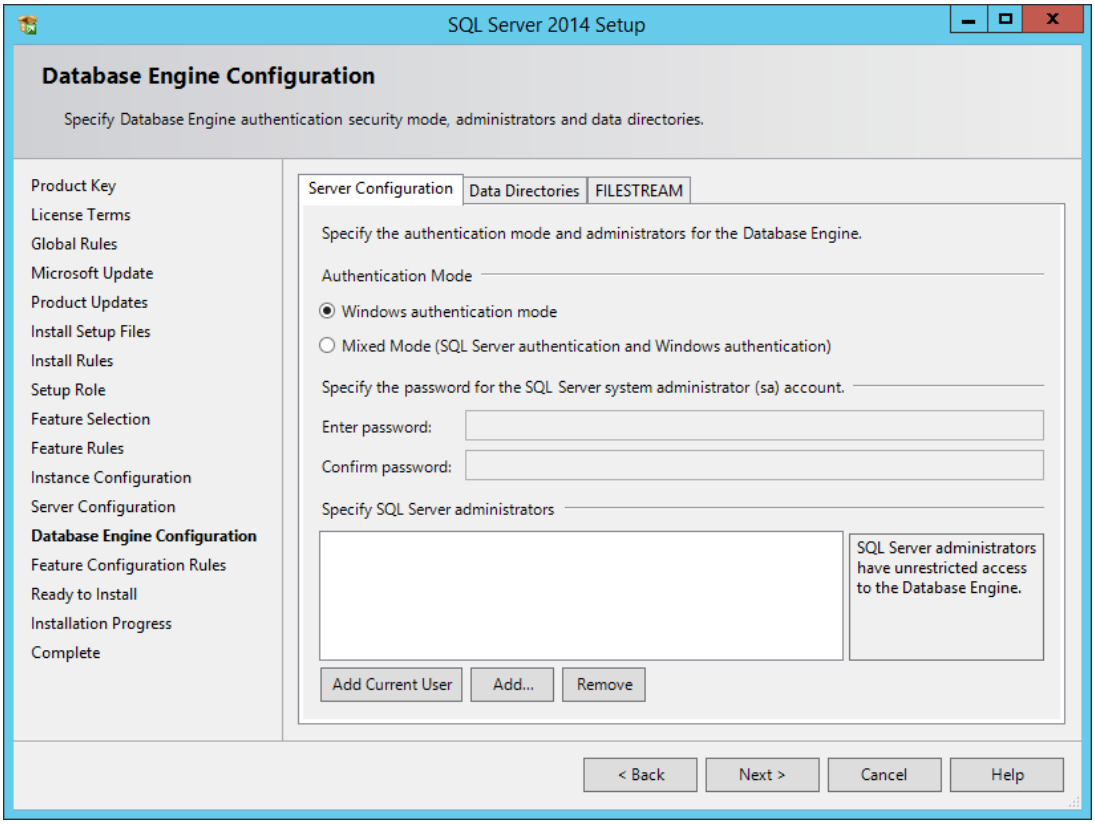
3. To configure the SQL Server collation as defined by Microsoft, click the tab **Collation** .



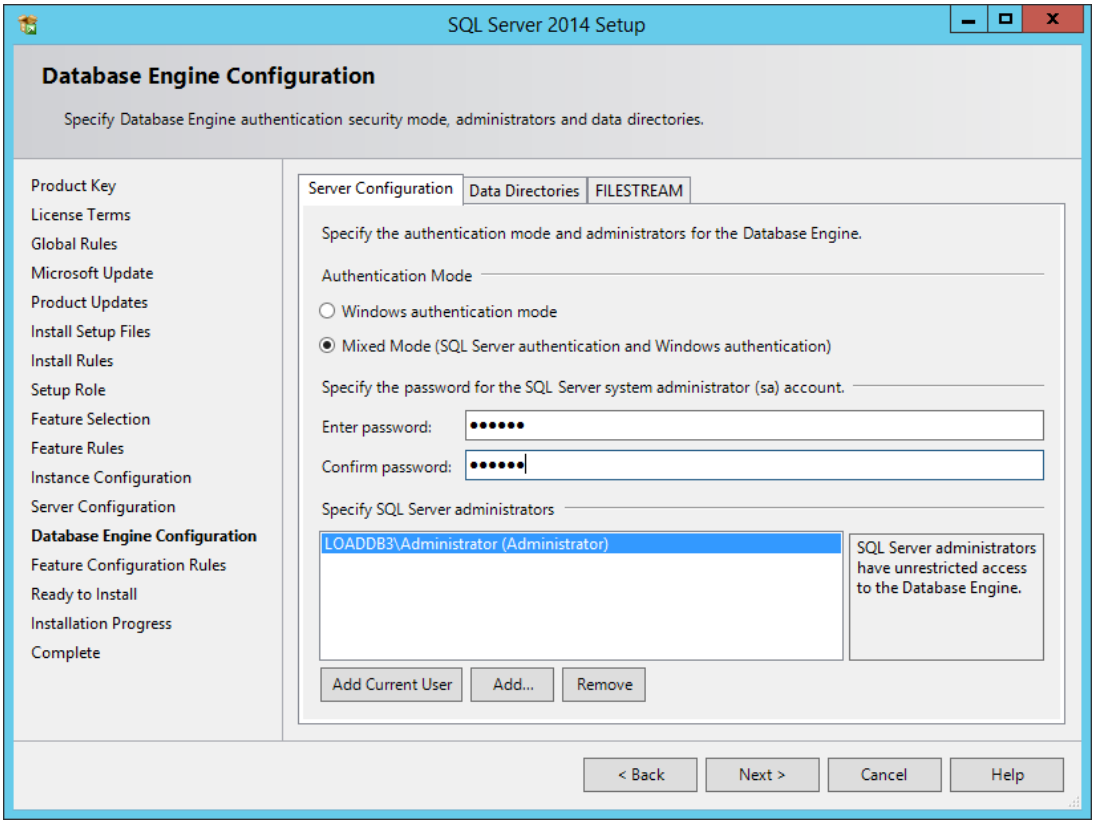
4. Click **Customize** and configure the SQL Server collation as defined by Microsoft, that is **Latin1_General_CI_AS_KS_WS** as shown in the screenshot below.



5. Click **OK** .
6. Click **Next** .

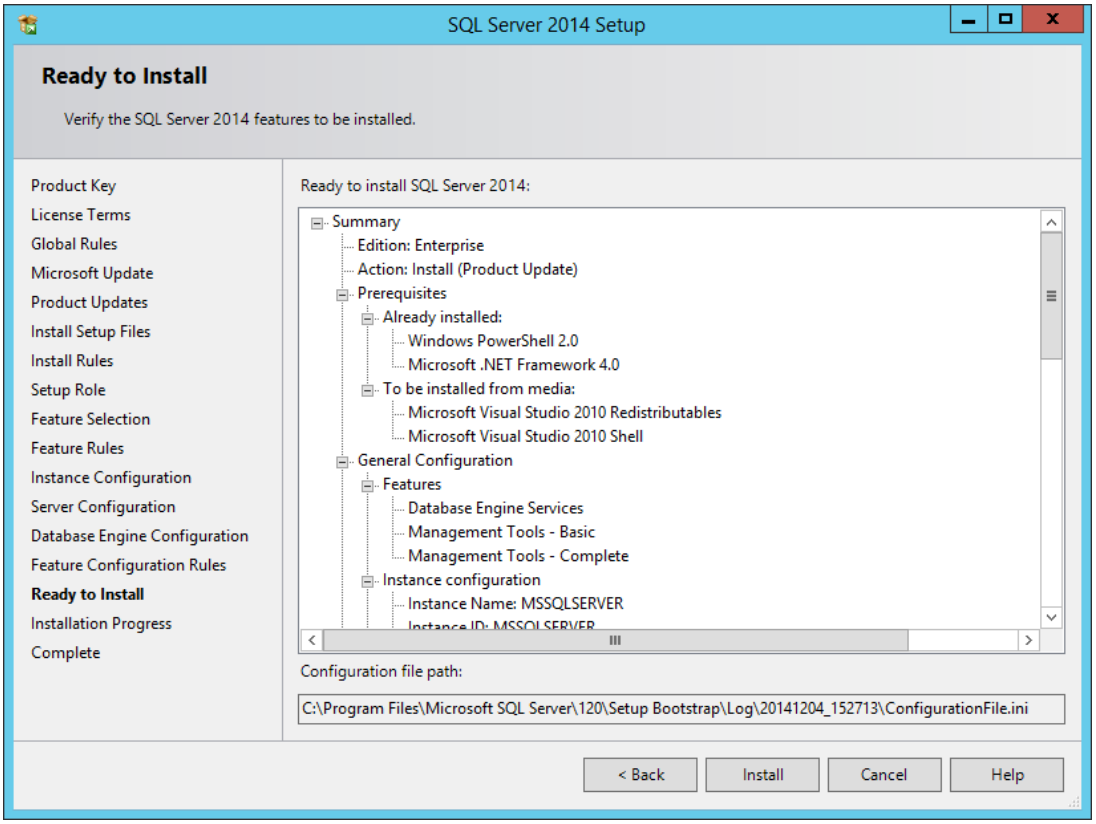


7. Select **Mixed Mode** and specify the password for the SQL Server system administrator (sa) account.



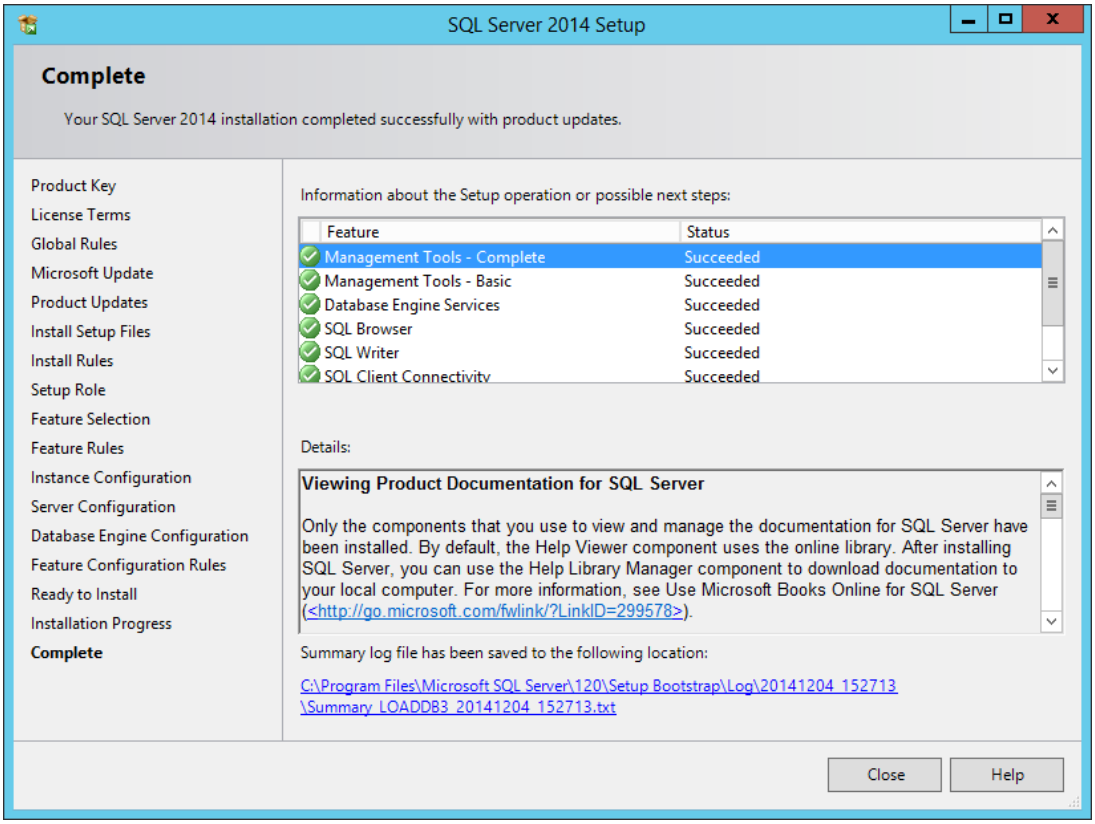
8. Click **Add Current User** to add your SQL Server administrator account.
9. *(Optional)* Click the **Data Directories** tab and modify the setup procedure.

10. Click **Next** .A summary of the elements to be installed is displayed.



11. If all selections displayed in the **Ready to Install** window are correct, click **Install** to launch the actual installation.

12. When all features are installed and their status is set to **Succeeded** in the **Complete** window, click **Close** .



The installation process executed successfully. You can now start the **Management Studio** from your desktop for further configuration.

Configuring Microsoft SQL Server 2014

From version 12.0 onwards the following parameters are automatically modified during the creation of the BCM database :

- Recovery model = Simple
- Parameterization = Forced
- Read Committed Snapshot = True
- Snapshot Isolation State = True

? Unknown Attachment

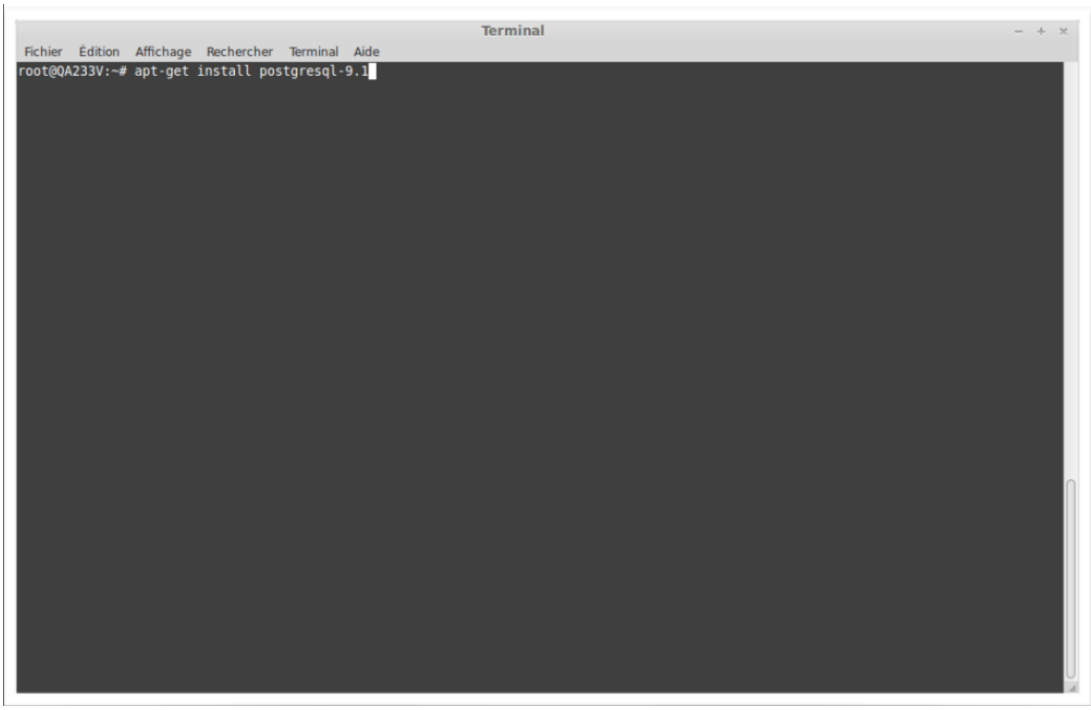
SQL_BASE_017.PNG

The database is now set up and configured for use with the BMC Client Management agent. However, before you can install the CM master on this computer, you need to ensure that the prerequisites that are listed in topic Database Prerequisites in the Windows installation section are fulfilled.

Installing PostgreSQL

To install the PostgreSQL database proceed as follows:

1. Open a Debian command terminal and log on as root.
2. Enter the command `# apt-get install postgresql-9.1`.



3. Type the letter **y** to confirm.

Debian automatically downloads the requested packages and launches the installation. This process can take a few minutes.

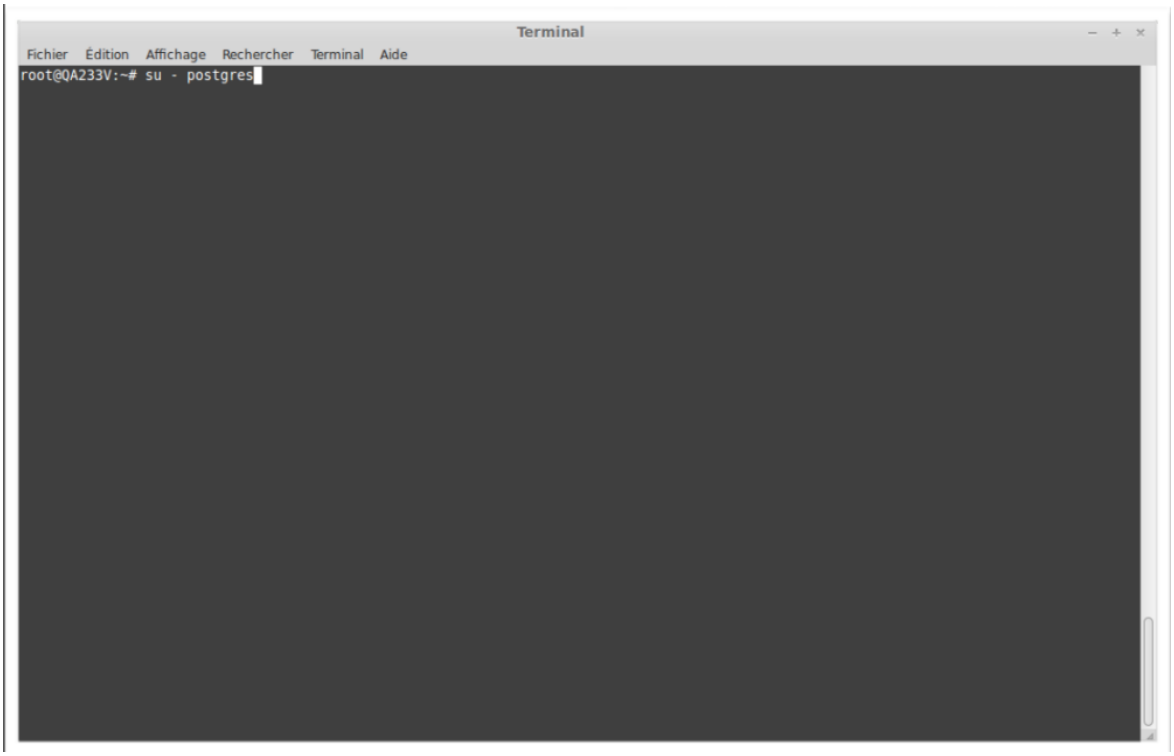
Configuring PostgreSQL

Configuring PostgreSQL is divided into the following steps:

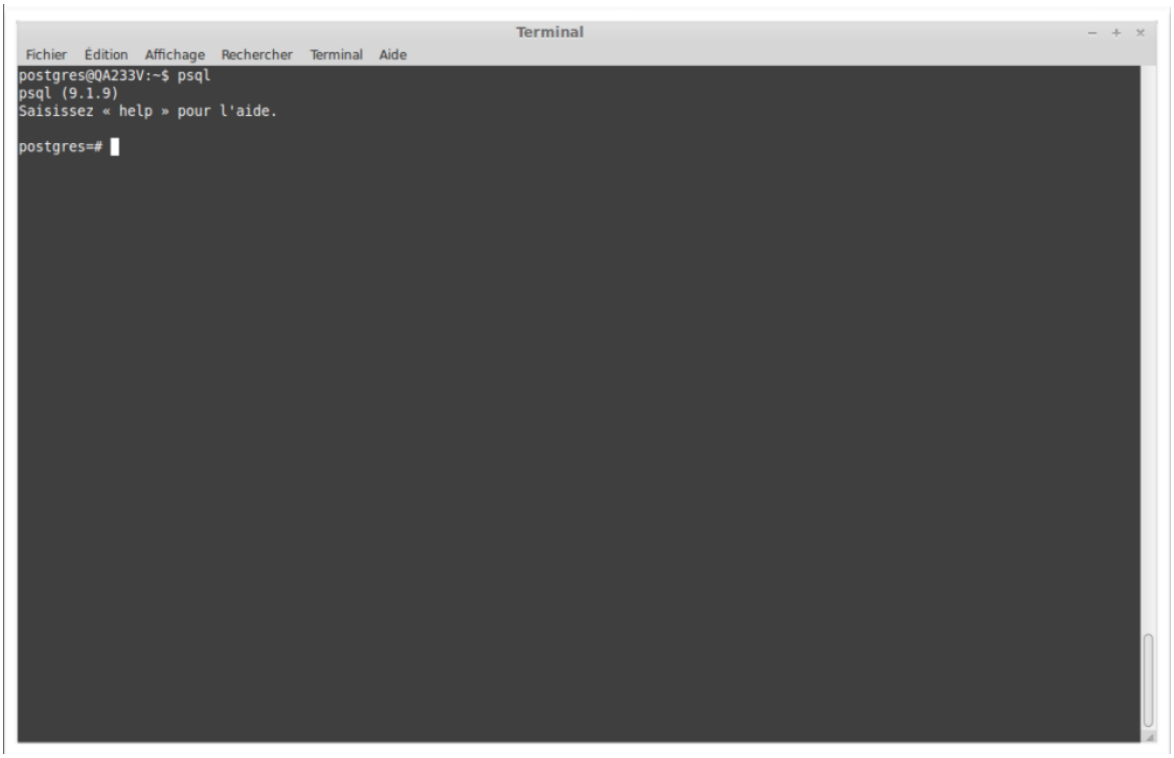
1. Connecting as a PostgreSQL user
2. Starting the **Administration Tool**
3. Creating a user for BMC Client Management

1. Type the command `# su - postgres` to activate the PostgreSQL user into a terminal window.

> All administrative operations are initially carried out by the PostgreSQL user. However, at the end of the installation process this user does not have a password, that is, the user account is blocked. You therefore need to activate the user to be able to carry out all required administratrive operations.



1. Type the command `# psql` to start the administration tool:



1. Type the command `# CREATE USER <username>;` to create the Client Management user.
2. Enter the command `# ALTER ROLE <username>;` .

   By doing so you provide the user the possibility to create new databases.

3. Enter the command `# CREATE DATABASE <database_name> OWNER <username>;` to create a database.

   If you give the database the same name as the user you connect to it with, the client connects with that database by default.

4. Enter the command `# ALTER USER <username> WITH ENCRYPTED PASSWORD <mypassword>;` to assign the user a password.

   Assigning the user a password is necessary to establish a connection with the database. The `ENCRYPTED` option allows the use of md5 in the `pg_hba.conf` file.

5. Enter `# \q` to quit pgSQL.
6. Enter `# exit` to log the PostgreSQL user off.

The database is now set up and configured for use with the BMC Client Management agent. However, before you can install the CM master on this computer, you need to ensure that the prerequisites that are listed in the Prerequisites for Postgres 9 and later topic in the Linux Installation section are fulfilled.

Installation and configuration of Oracle 12c Release 1 (12.1.0.2) on Linux 6

Installing Oracle 12c Release 1 (12.1.0.2) and configuring it to work with the CM agent on a Linux 6 system require the following steps:

Note:

The following procedure is applicable on systems on which the CM master is installed on the same computer as the database. If you install the master on another computer, you must also first install the Oracle client on that computer.

1. Downloading and unzipping the installation files.
2. Configuring the Hosts file.
3. Verifying the Oracle installation prerequisites.
4. Installing Oracle 12c.
5. Creating and configuring the CM database.
6. Configuring a LISTEN Process.

Downloading and unzipping the installation files

1. Download the Oracle software from OTN or MOS depending on your support status.

2. Unzip the downloaded files via the following commands:

```
unzip linuxamd64_12102_database_1of2.zip
unzip linuxamd64_12102_database_2of2.zip
```

You should now have a single directory called **database** that contains the installation files.

Configuring the hosts file

The **/etc/hosts** file must contain a fully qualified name for the server in the format `<IP-address> <fully-qualified-machine-name> <machine-name>` , for example:

```
127.0.0.1       localhost.localdomain  localhost
192.168.1.195   serverdb.localdomain   serverdb
```

Verifying the Oracle 12c installation prerequisites

1. Run the following command to perform most of the prerequisite setup tasks via the oracle preinstall package (**oracle-rdbms-server-12cR1-preinstall**):

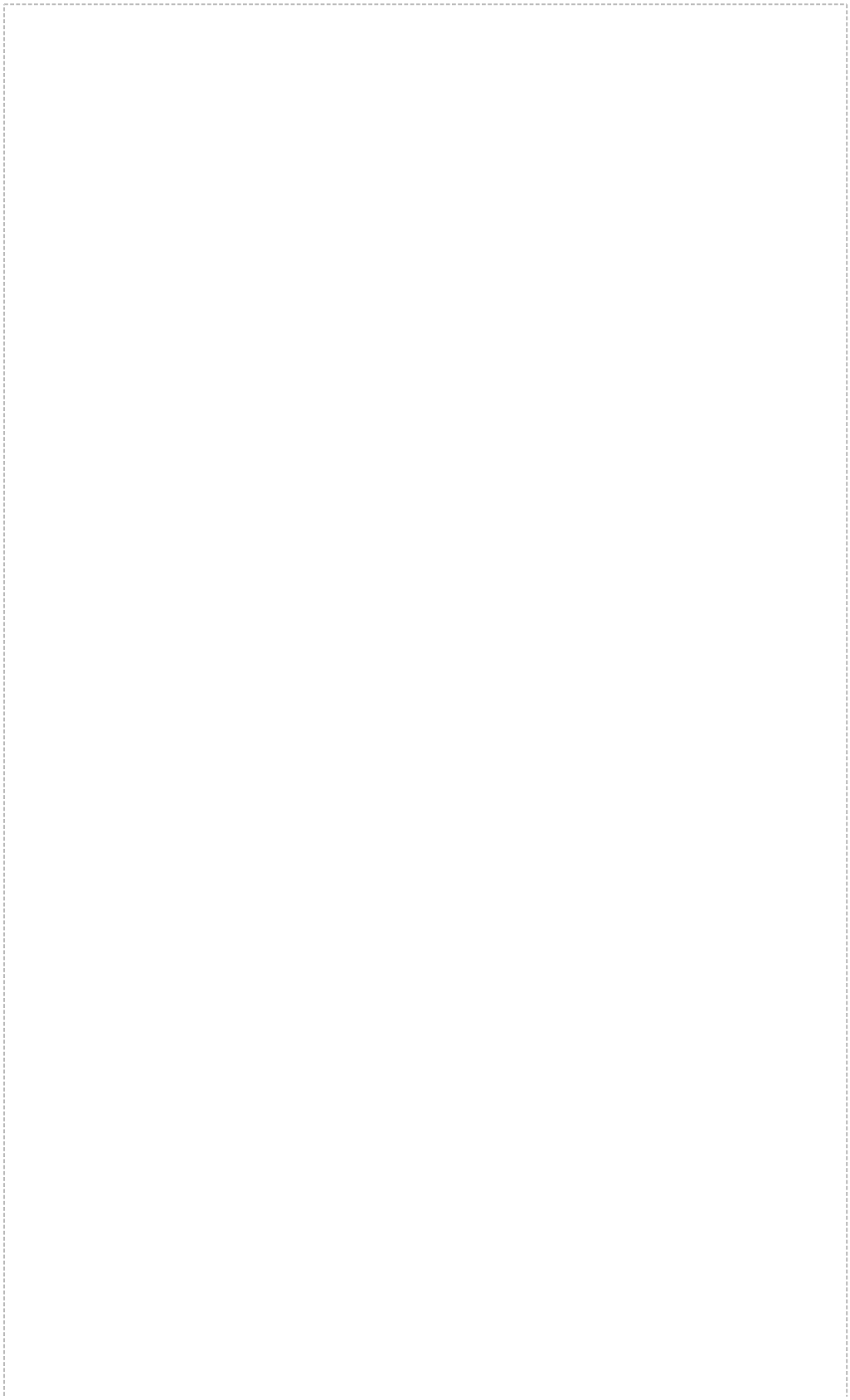
```
yum install oracle-rdbms-server-12cR1-preinstall -y
```

> **Note:**
>
> Earlier versions of Oracle Linux require manual setup of the Yum repository as explained in http://public-yum.oracle.com .

If you have not used the preinstall package to perform the prerequisites, you must manually perform the following setup tasks:

1. a. Add or modify the following lines in the **/etc/sysctl.conf** file,fs.file-max = 6815744 kernel.sem = 250 32000 100 128 kernel.shmmni = 4096 kernel.shmall = 1073741824 kernel.shmmax = 4398046511104 net.core.rmem_default = 262144 net.core. rmem_max = 4194304 net.core.wmem_default = 262144 net.core.wmem_max = 1048576 fs.aio-max-nr = 1048576 net.ipv4.ip_local_port_range = 9000 65500

b. Run the following command to change the current kernel parameters:

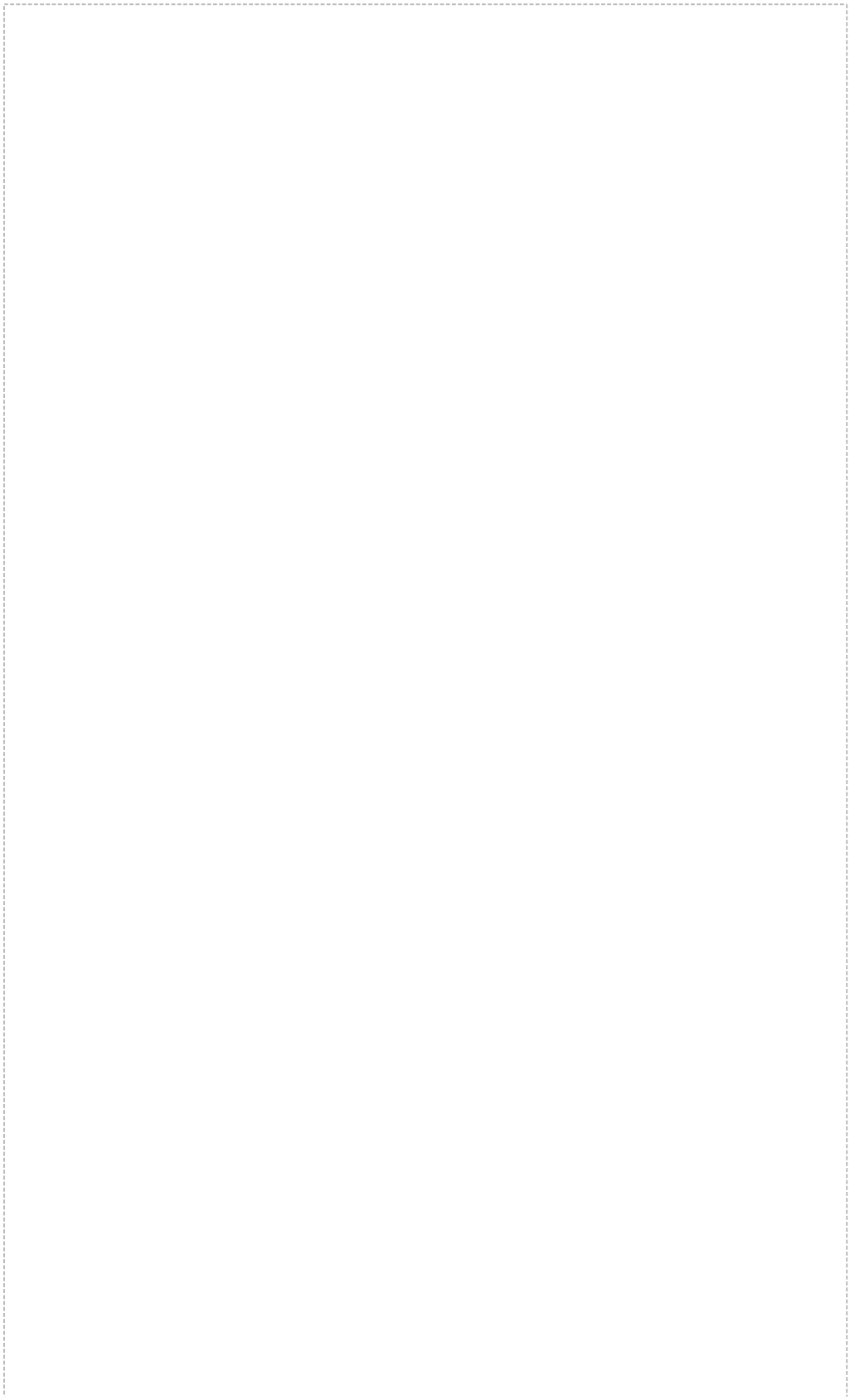


```
/sbin/sysctl -p
```

c. Add the following lines to the **/etc/security/limits.conf** file,

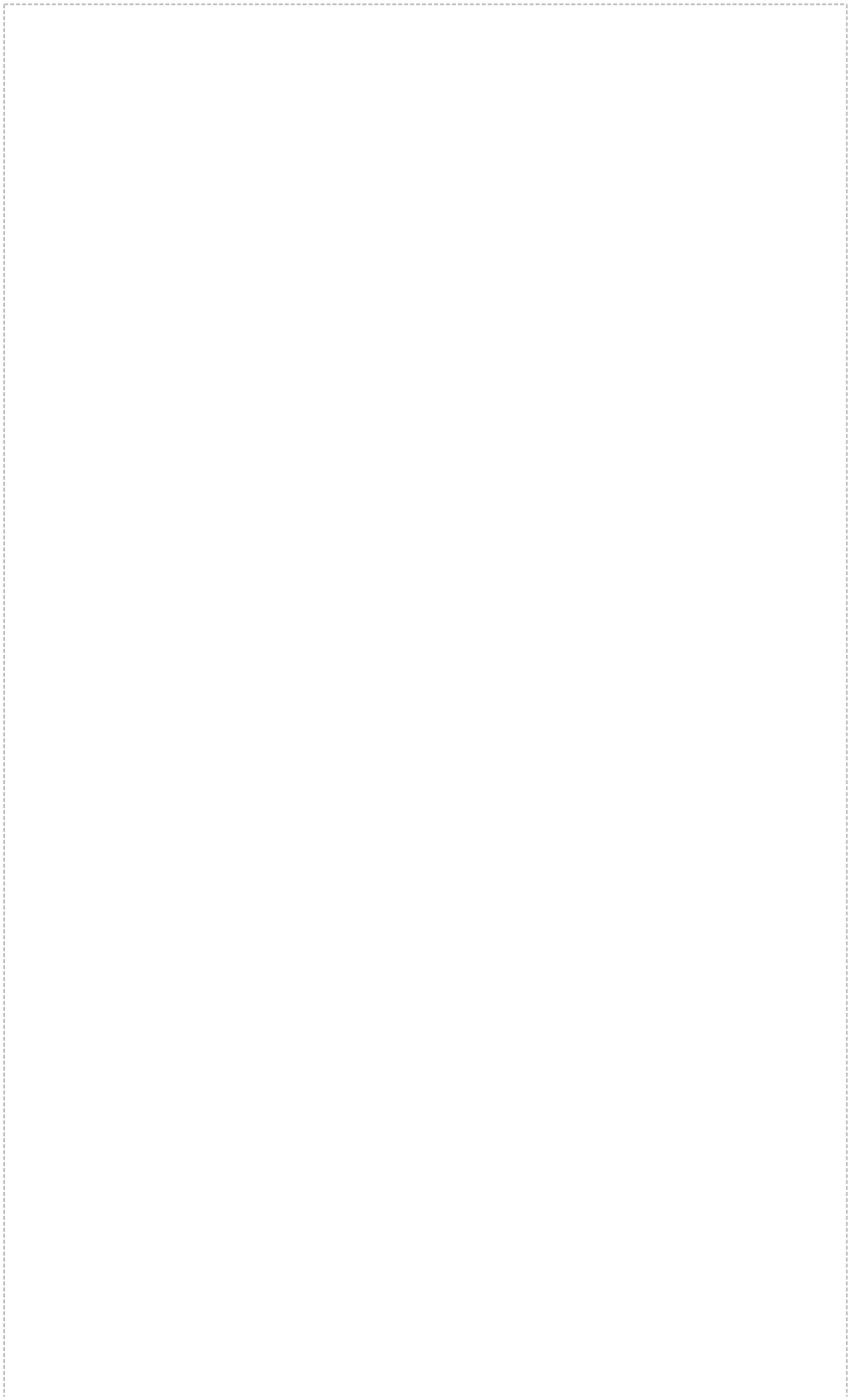
```
oracle              soft            nofile          1024
oracle              hard            nofile          65536
oracle              soft            nproc           16384
oracle              hard               nproc           16384
oracle              soft            stack           10240
oracle              soft            stack           32768
```

d. If the following packages are not already present, install them:



```
# From public Yum or ULN
yum install binutils -y
yum install compat-libcap1 -y
yum install compat-libstdc++-33 -y
yum install compat-libstdc++-33.i686 -y
yum install gcc -y
yum install gcc-c++ -y
yum install glibc -y
yum install glibc.i686 -y
yum install glibc-devel -y
yum install glibc-devel.i686 -y
yum install ksh -y
yum install libgcc -y
yum install libgcc.i686 -y
yum install libstdc++ -y
yum install libstdc++.i686 -y
yum install libstdc++-devel -y
yum install libstdc++-devel.i686 -y
yum install libaio -y
yum install libaio.i686 -y
yum install libaio-devel -y
yum install libaio-devel.i686 -y
yum install libXext -y
yum install libXext.i686 -y
yum install libXtst -y
yum install libXtst.i686 -y
yum install libX11 -y
yum install libX11.i686 -y
yum install libXau -y
yum install libXau.i686 -y
yum install libxcb -y
yum install libxcb.i686 -y
yum install libXi -y
yum install libXi.i686 -y
yum install make -y
yum install sysstat -y
yum install unixODBC -y
yum install unixODBC-devel -y
```

e. Create the following new groups and users:



```
groupadd -g 54321 oinstall
groupadd -g 54322 dba
groupadd -g 54323 oper
#groupadd -g 54324 backupdba
#groupadd -g 54325 dgdba
#groupadd -g 54326 kmdba
#groupadd -g 54327 asmdba
#groupadd -g 54328 asmoper
#groupadd -g 54329 asmadmin

useradd -u 54321 -g oinstall -G dba,oper oracle
```

Note:

Uncomment the extra groups you require.

2. Set the password for the **oracle** user:

```
passwd oracle
```

3. Modify the **/etc/security/limits.d/90-nproc.conf** file as follows (See MOS Note ID 1487773.1):

```
# Change this *
soft    nproc    1024
# To this *
- nproc 16384
```

4. Set secure Linux to permissive by editing the **/etc/selinux/config** file, making sure the `SELINUX` flag is set as follows:

```
SELINUX=permissive
```

5. When you made all required modifications, restart the server or run the following command: `setenforce Permissive`

6. If you have the Linux firewall enabled, you must disable or configure it as follows:

```
service iptables stop
chkconfig iptables off
```

7. Create the directories in which the Oracle software is to be installed:

```
mkdir -p /u01/app/oracle/product/12.1.0.2/db_1
chown -R oracle:oinstall /u01
chmod -R 775 /u01
```

8. Add the following lines at the end of the **/home/oracle/.bash_profile** file.

```
# Oracle Settings
TMP=/tmp; export TMP
TMPDIR=$TMP; export TMPDIR
ORACLE_HOSTNAME= serverdb.localdomain; export ORACLE_HOSTNAME
ORACLE_UNQNAME=DBBCM; export ORACLE_UNQNAME
ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/12.1.0.2/db_1; export ORACLE_HOME
ORACLE_SID= DBBCM; export ORACLE_SID
PATH=/usr/sbin:$PATH; export PATH
PATH=$ORACLE_HOME/bin:$PATH; export PATH
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/jlib; export CLASSPATH
```

9. Log on as root and run the following command:

```
xhost +
```

Installing the Oracle database

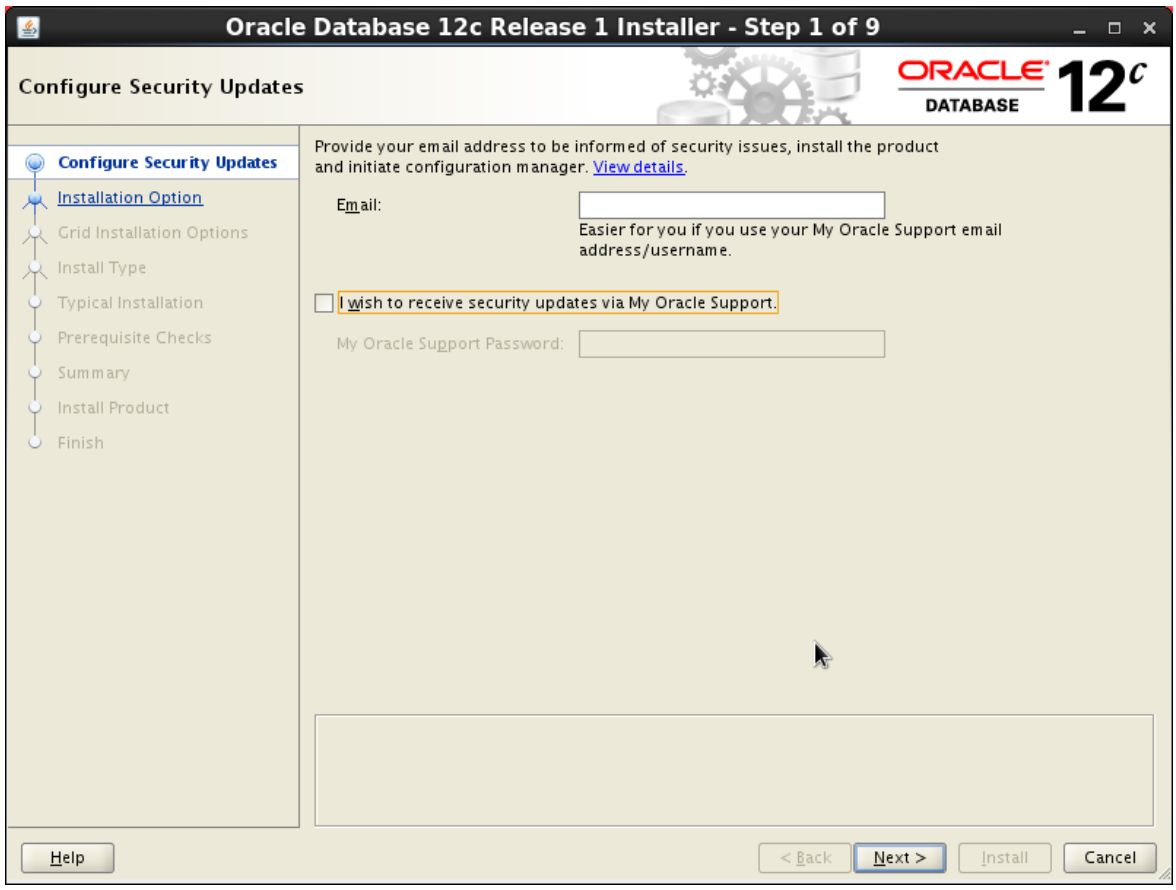
1. Log on as the **oracle** user.

```
su - oracle
```

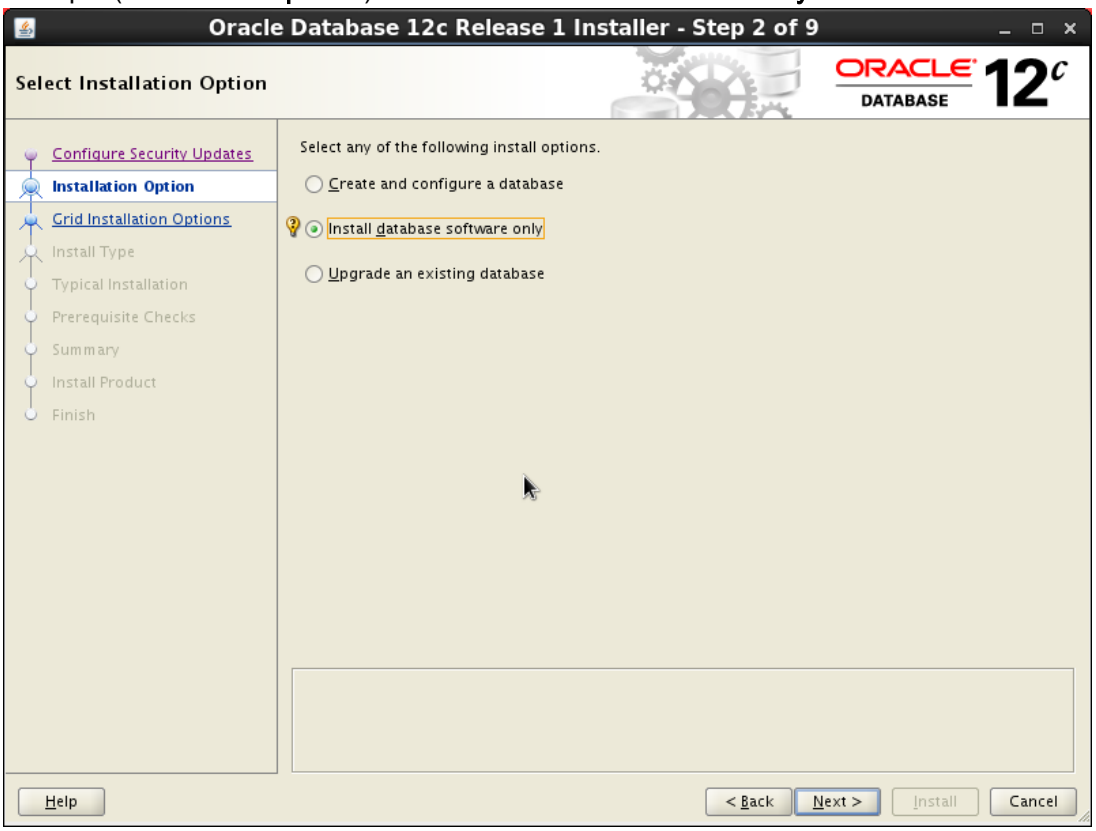
2. Run the following command in the database directory to start the **Oracle Universal Installer (OUI)** (OUI),

```
./runInstaller
```

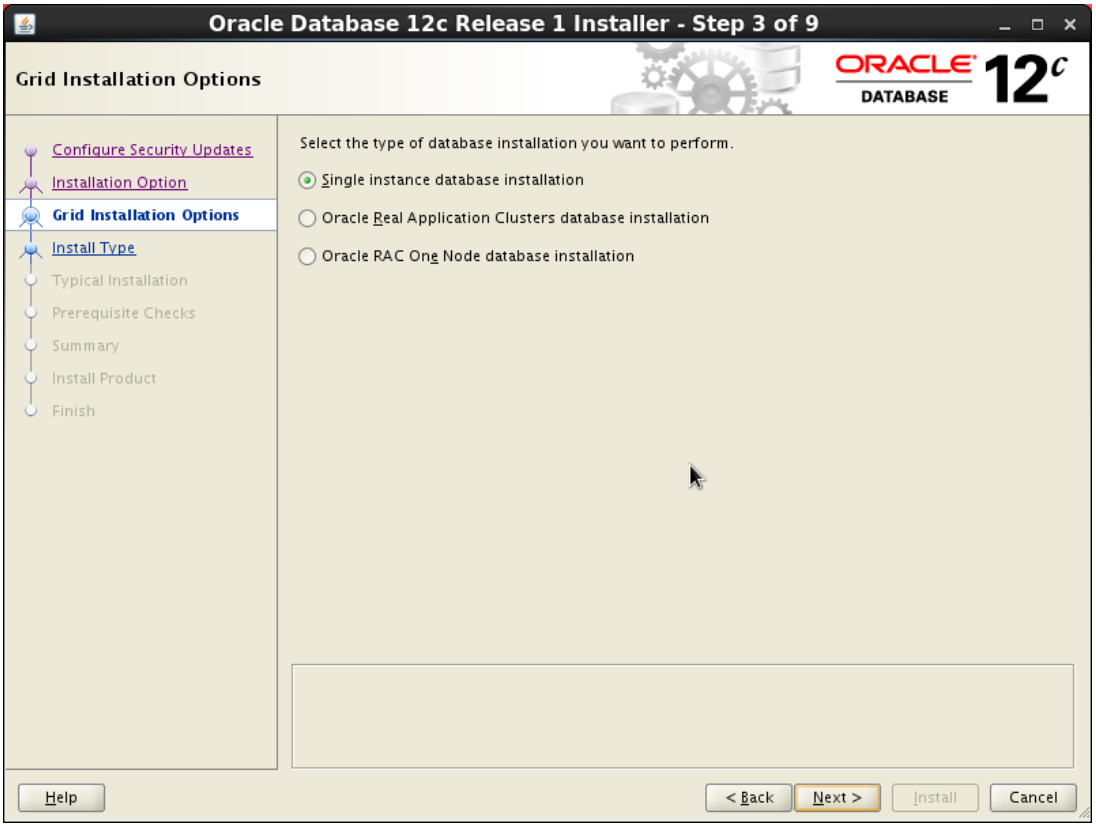
3. *(Optional)* In step 1 (**Configure Security Updates**) make your selections and click **Next** .



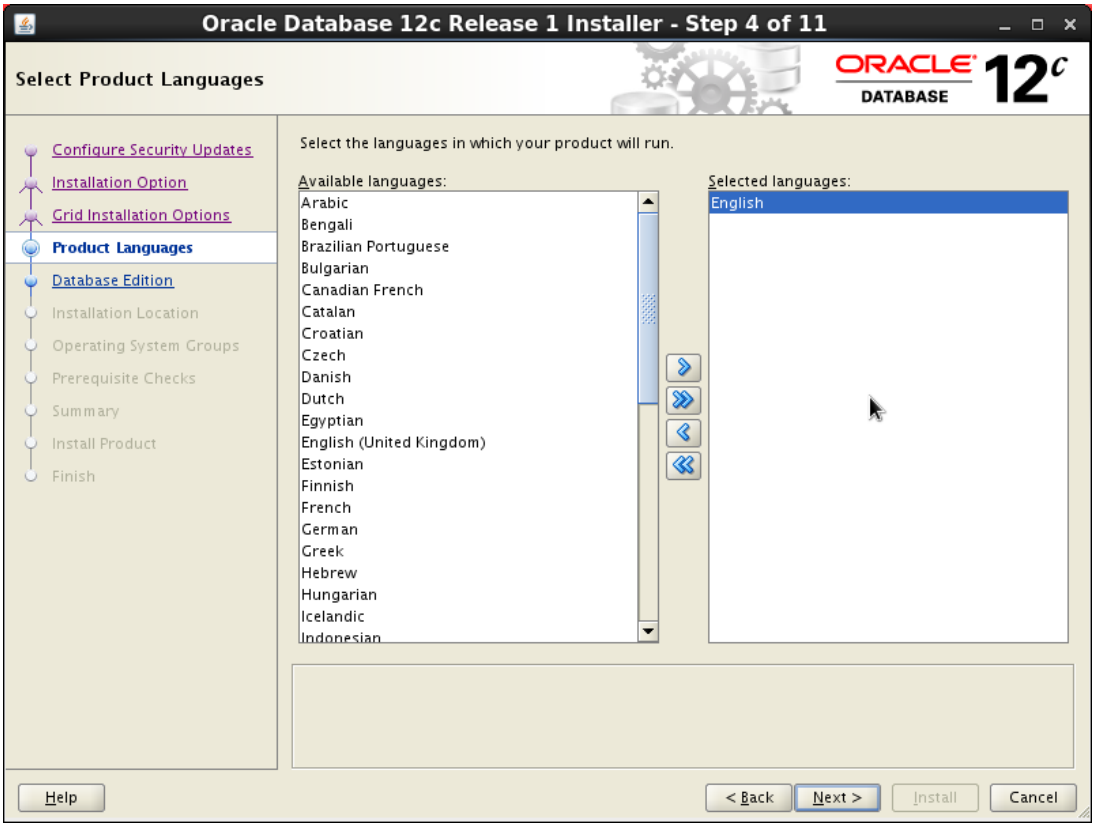
1. In step 2 (**Installation Options**) select **Install database software only** and click **Next** .



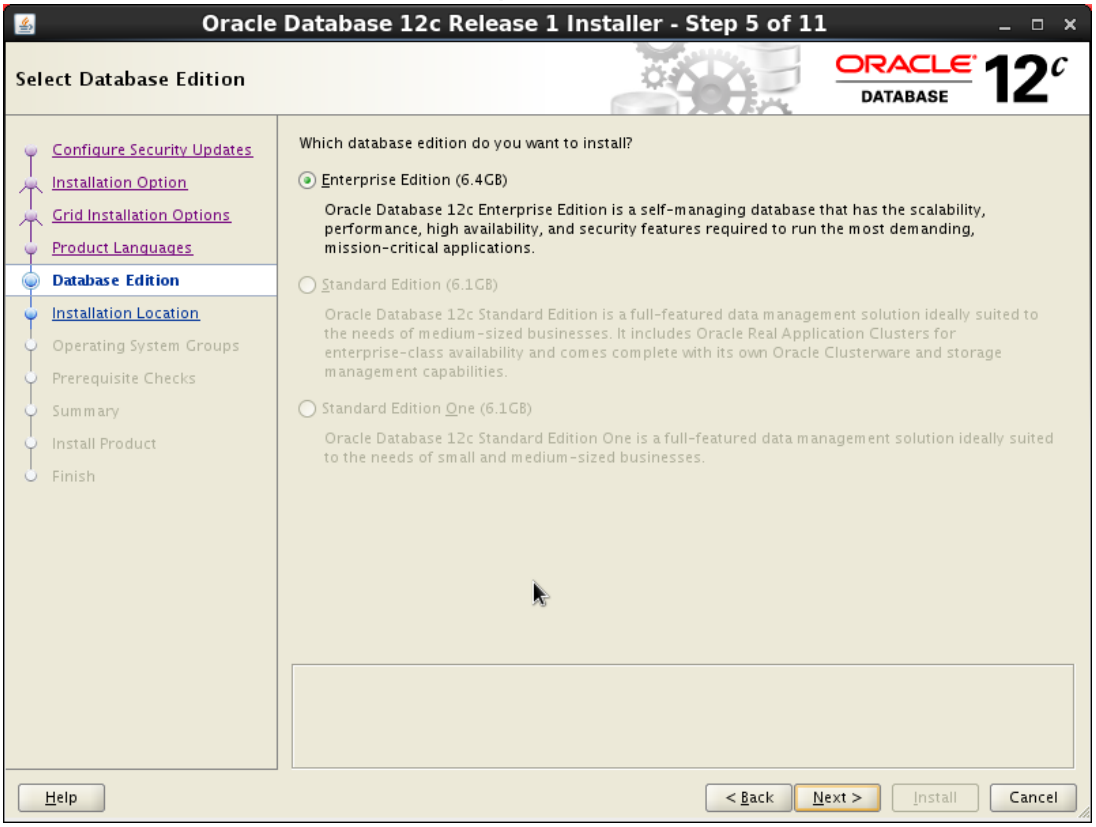
2. In step 3 (**Grid Installation Options**) select **Single instance database installation** and click **Next** .



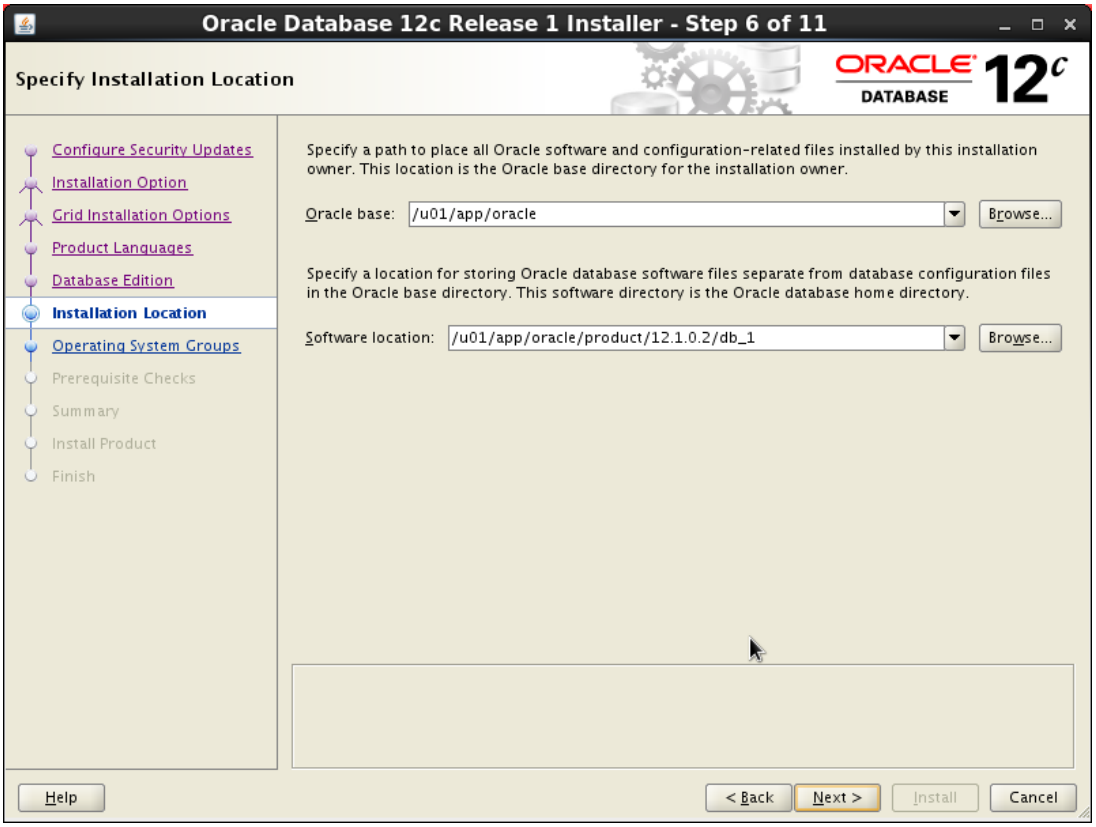
3. In step 4 (**Product Languages**), from the **Available languages** list, select the languages for the database and click the right arrow to add the languages to the **Selected languages** list. Then click **Next** .



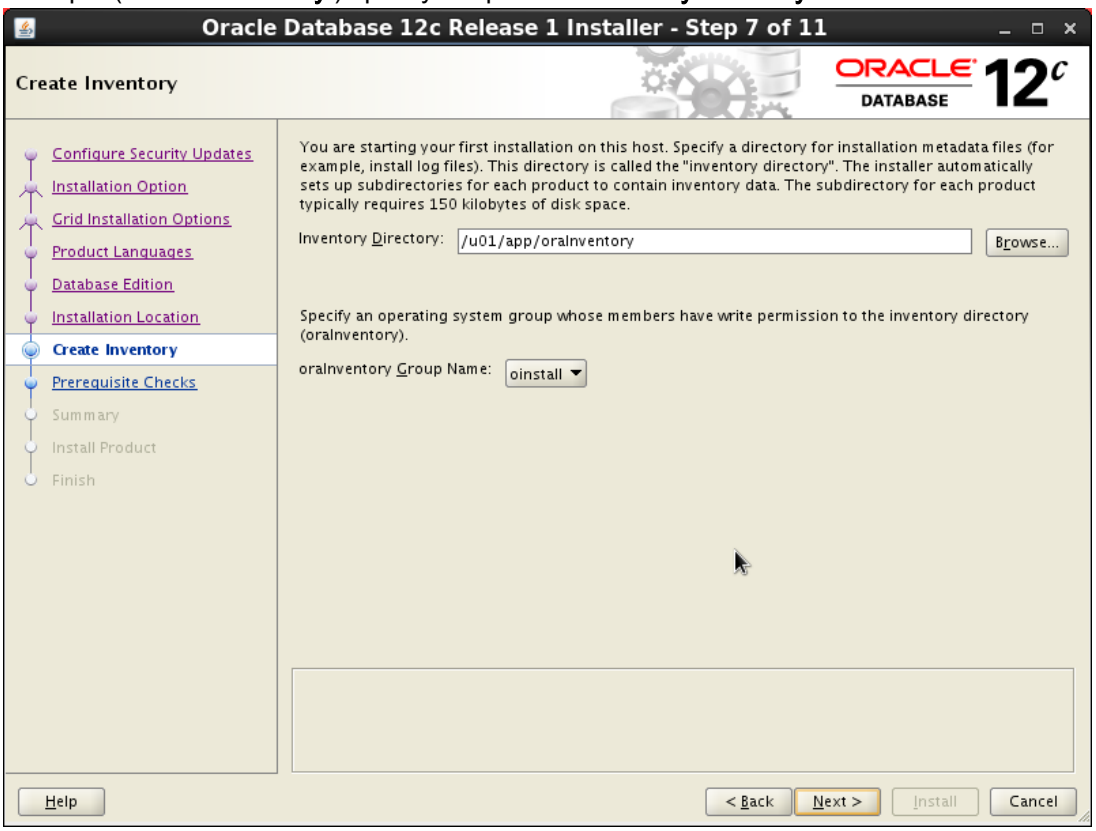
4. In step 5 (**Database Edition**) select **Enterprise Edition** and click **Next** .



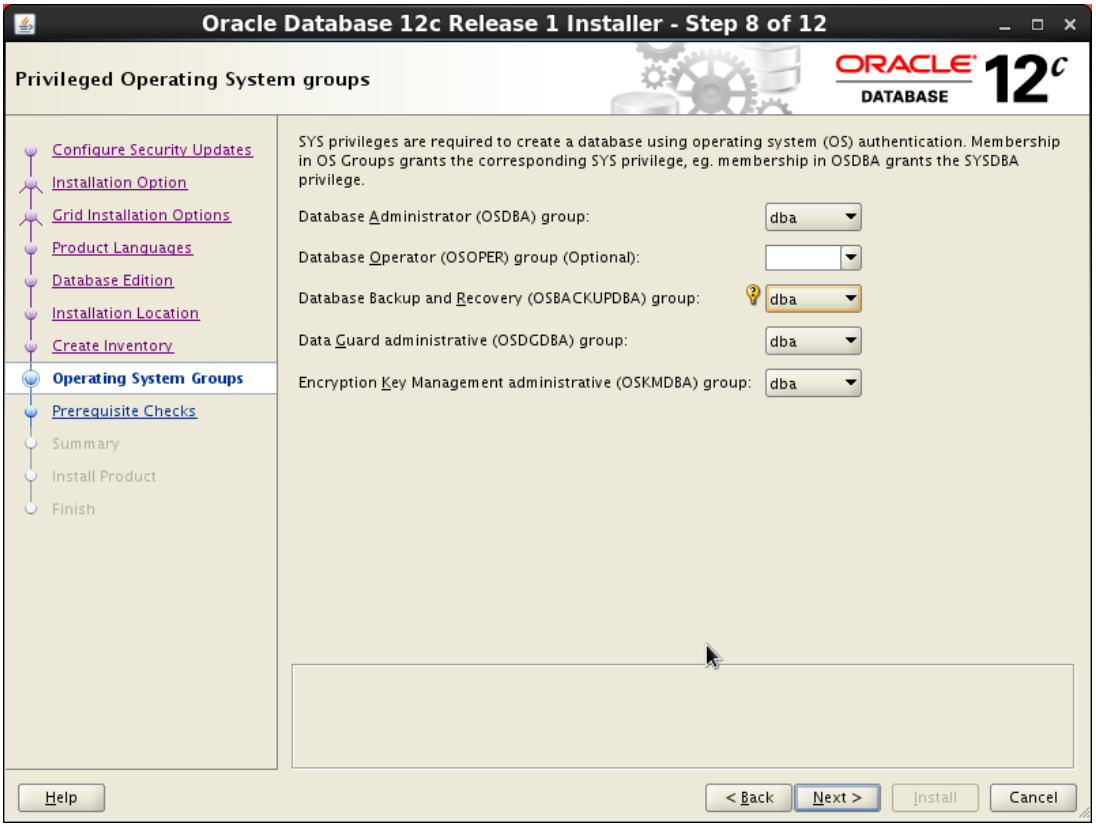
5. In step 6 (**Installation Location**) enter the paths for **Oracle Base** and **Software Location** . Click **Next** .



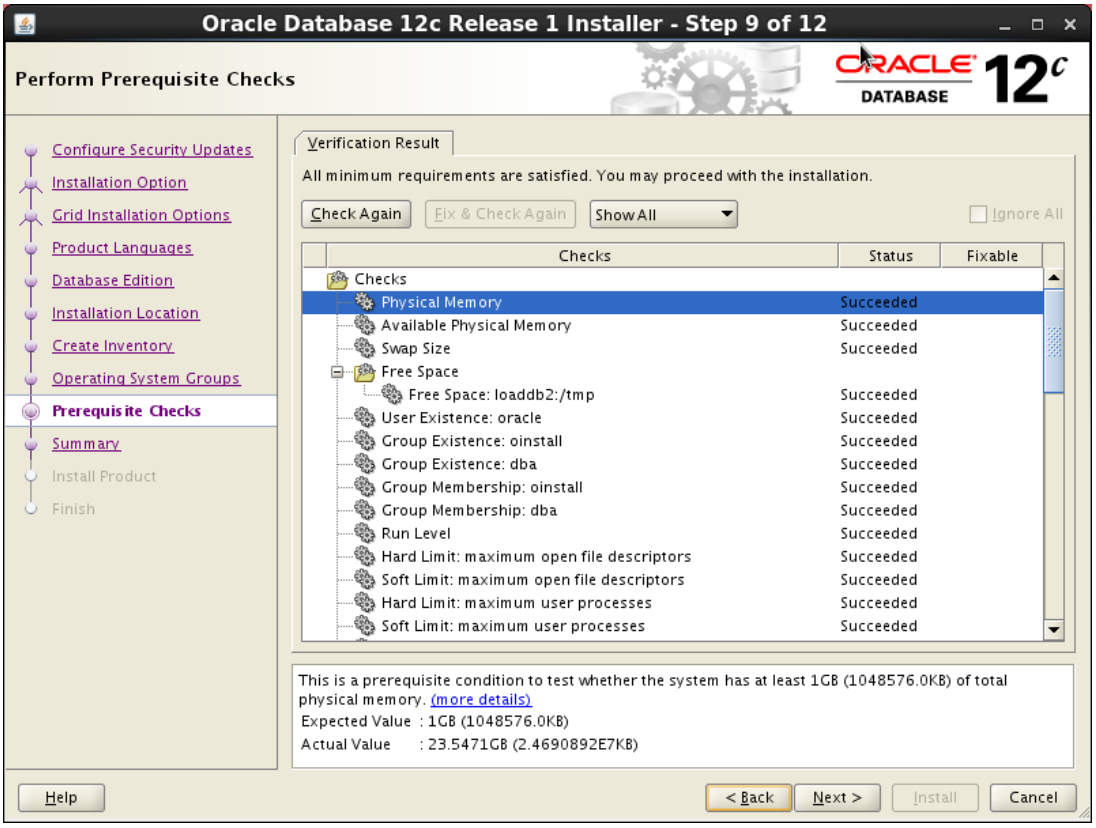
6. In step 7 (**Create Inventory**) specify the path for **Inventory Directory** and click **Next** .



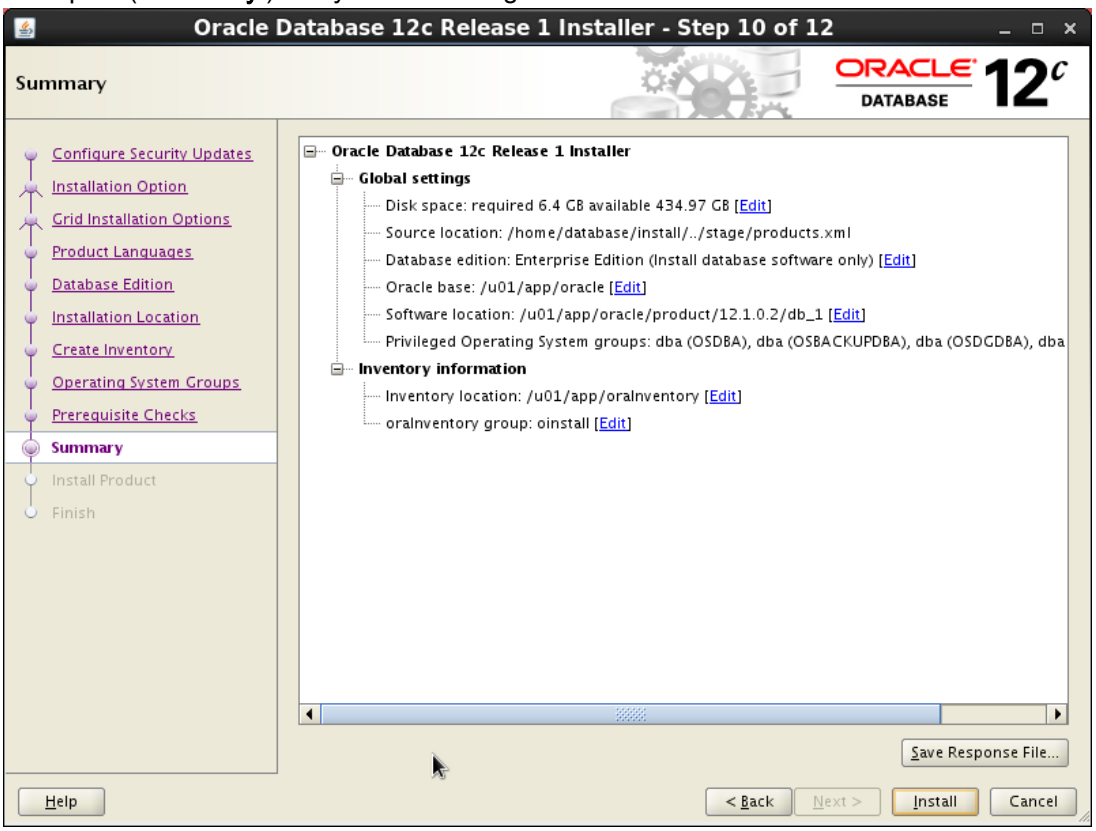
7. In step 8 (**Operating System Groups**) verify if the preentered values are correct and modify if necessary. Then click **Next** .



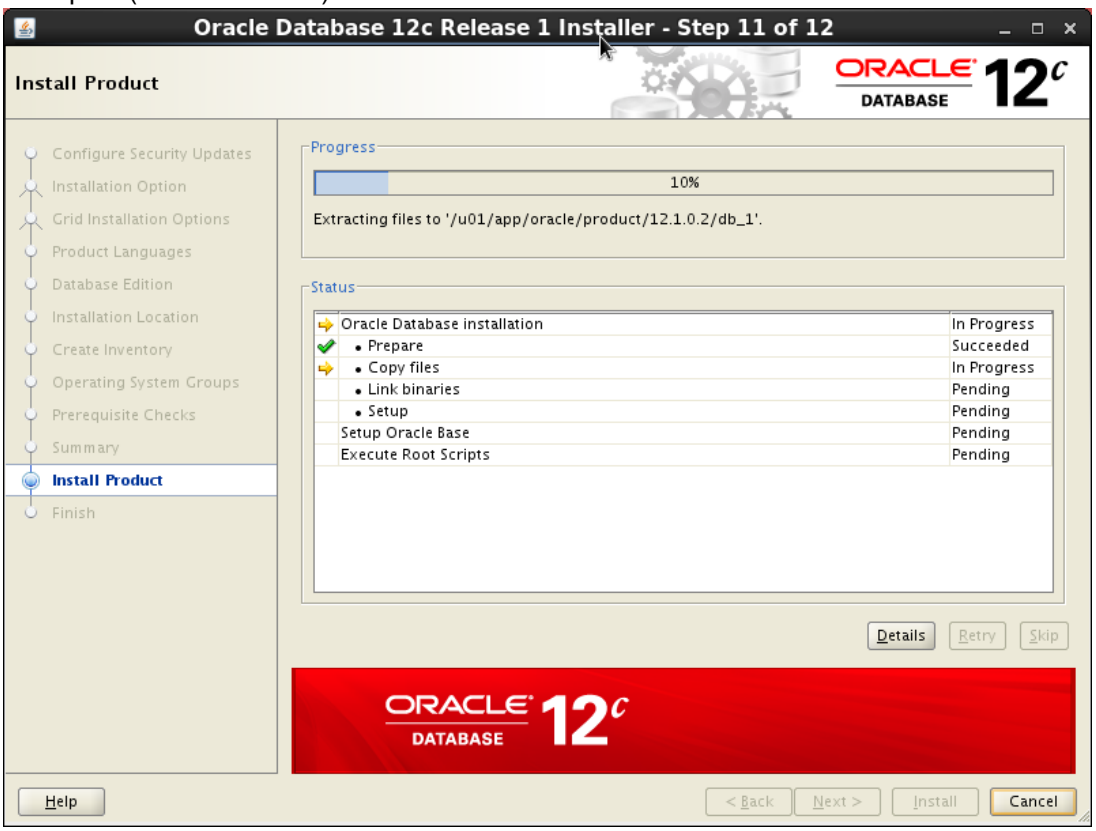
8. In step 9 (**Prerequisite Checks**) the installer runs prerequisite checks and verifies for the minimum requirements. If all tests are successful click **Install** .



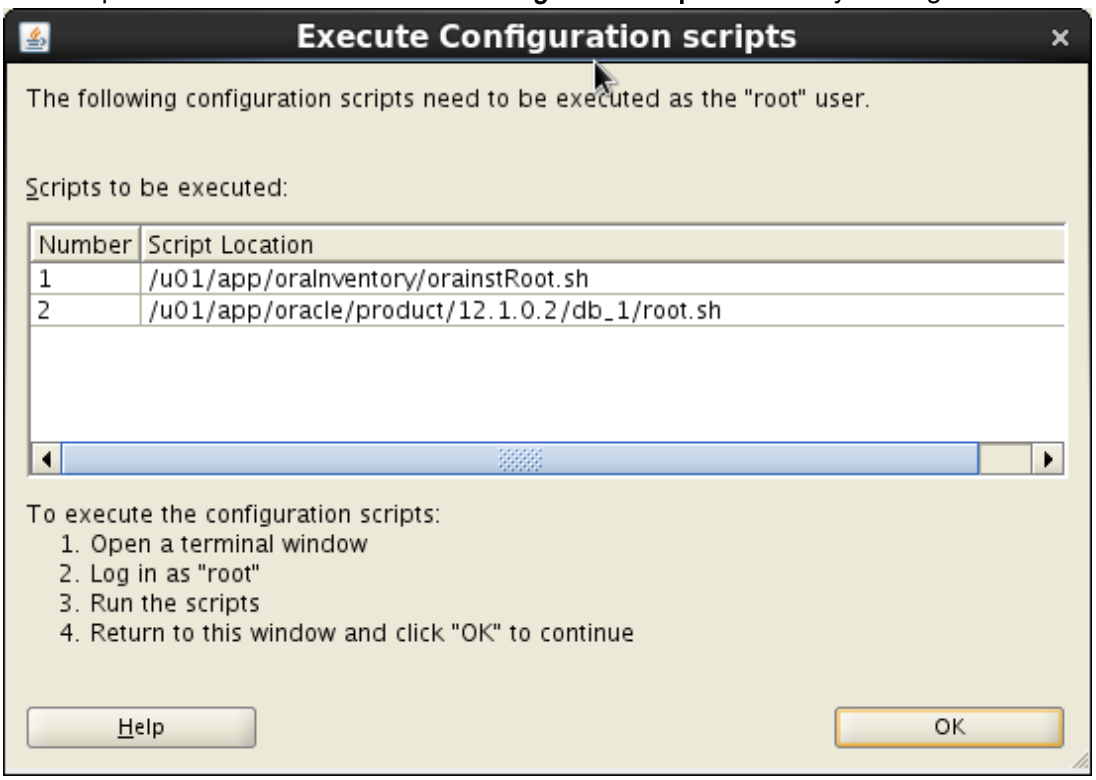
9. In step 10 (**Summary**) verify that all settings are correct and click **Install** .



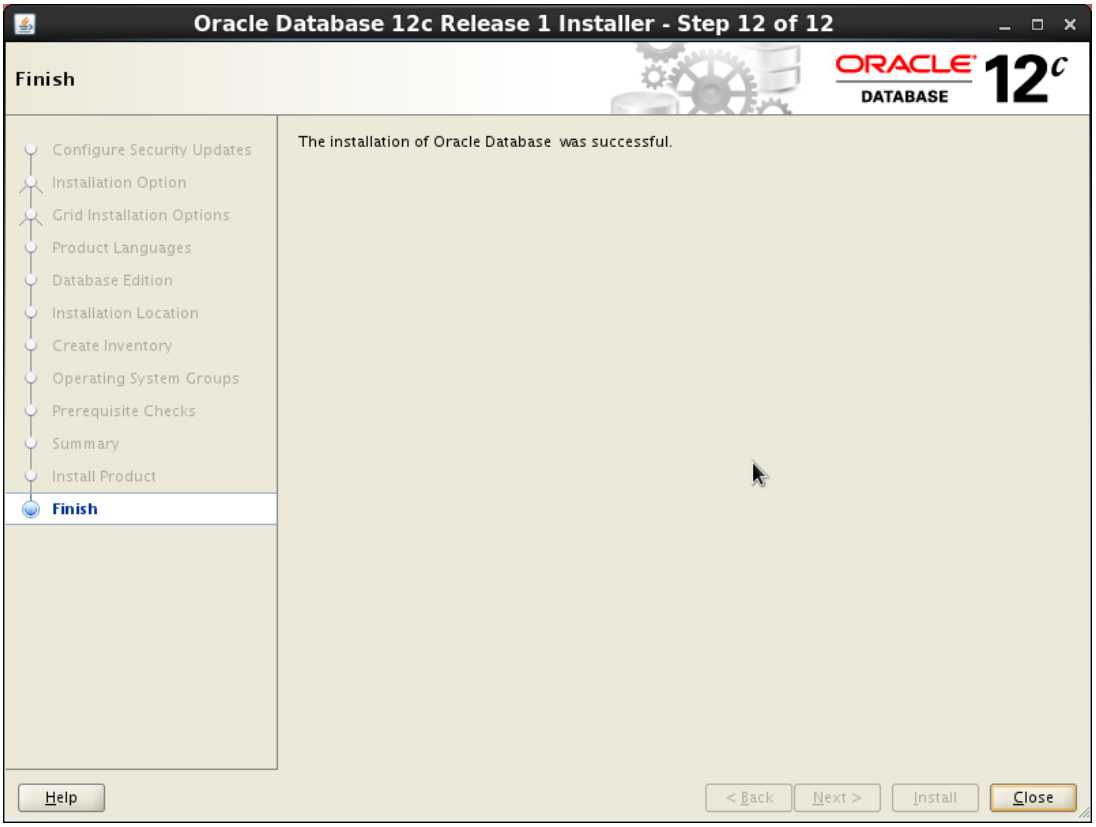
10. In step 11 (**Install Product**) click **Next** .



11. Run scripts as indicated in the **Execute Configuration scripts** window by clicking **OK** .



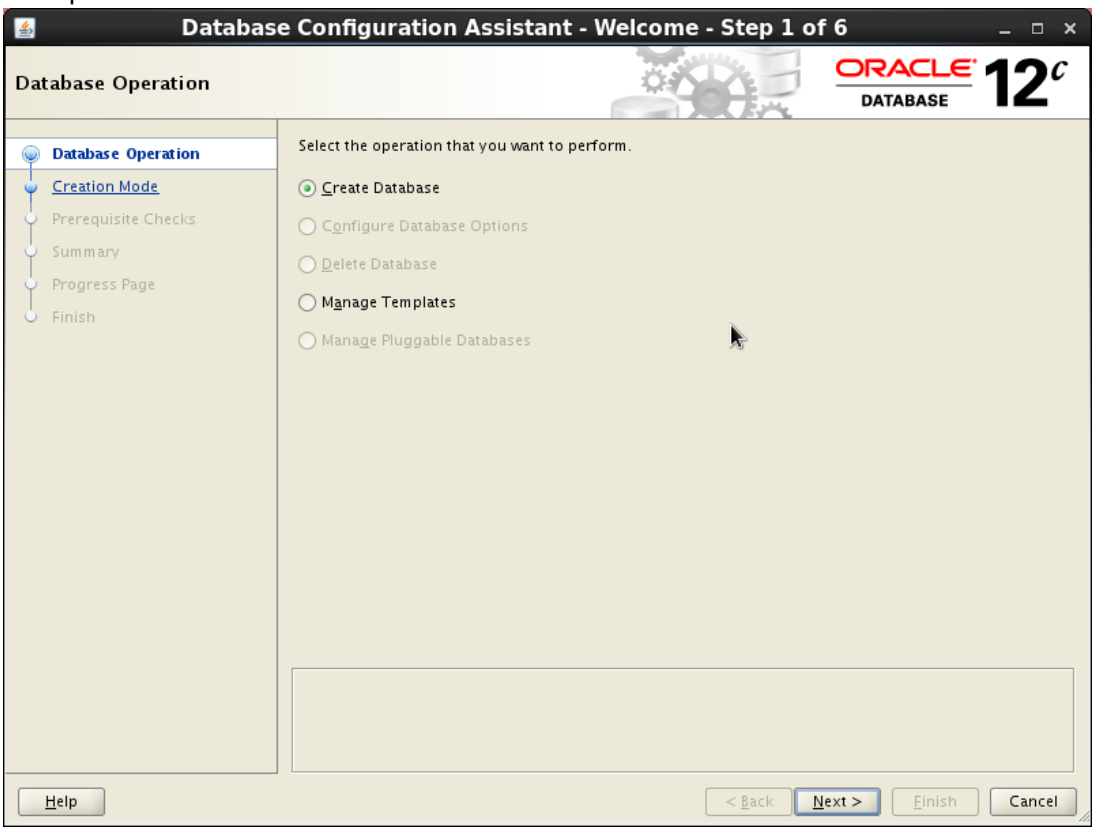
12. Click **Close** in step 12 (**Finish**) to terminate the installation.



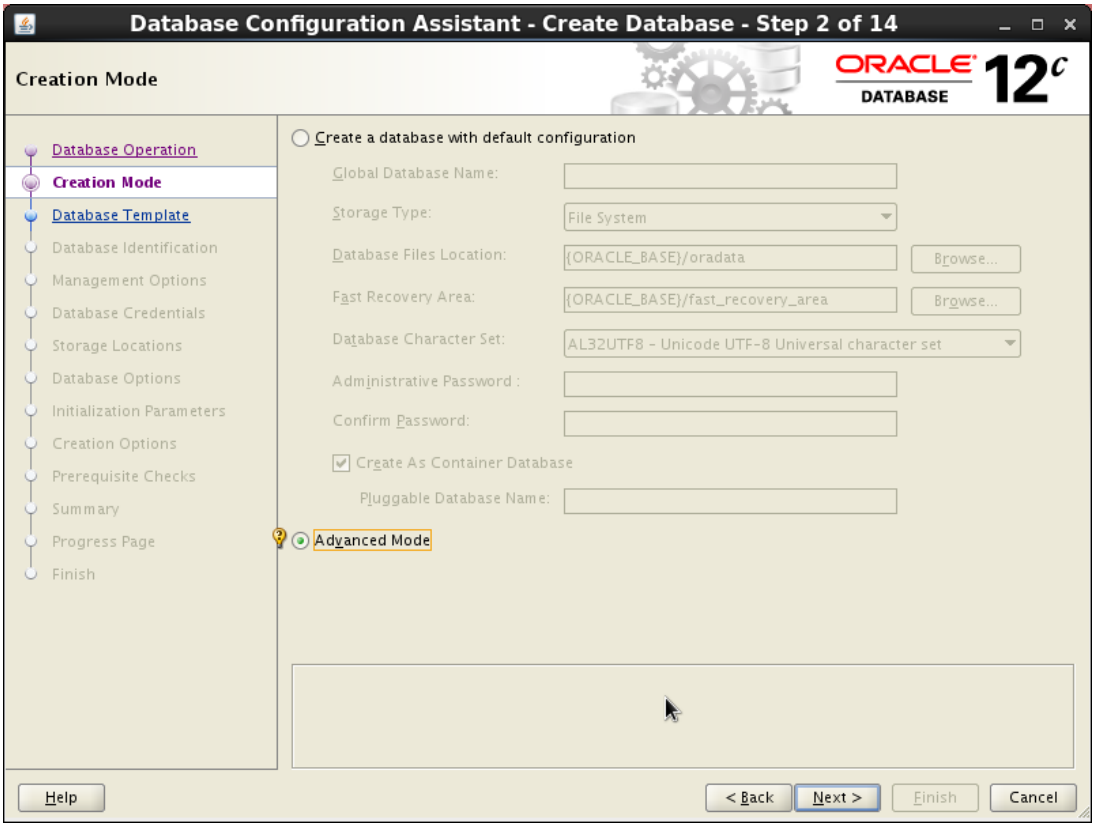
Configuring the Oracle database

After the database engine is installed, a database instance must be created and configured as follows:

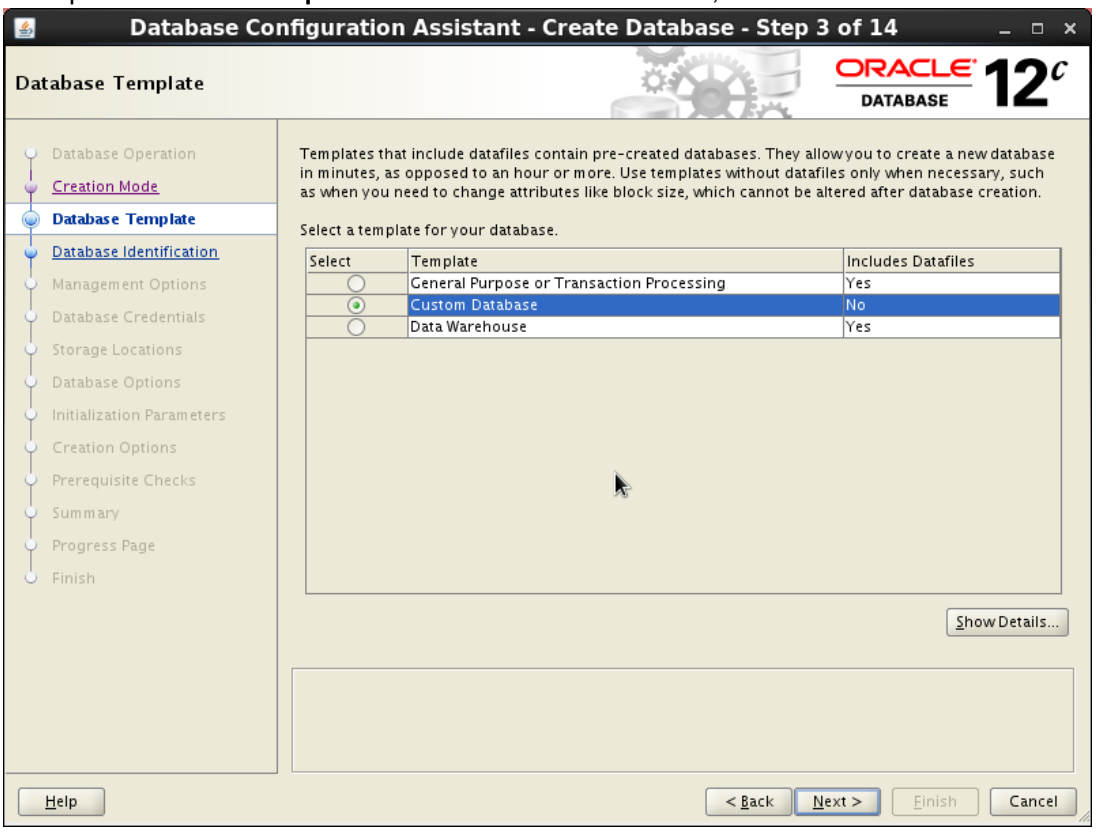
1. Enter the `dbca` command to start the **Database Configuration Assistant** from `$ORACLE_HOME/bin`
2. In step 1 - **Welcome** select **Create a Database** and click **Next** .



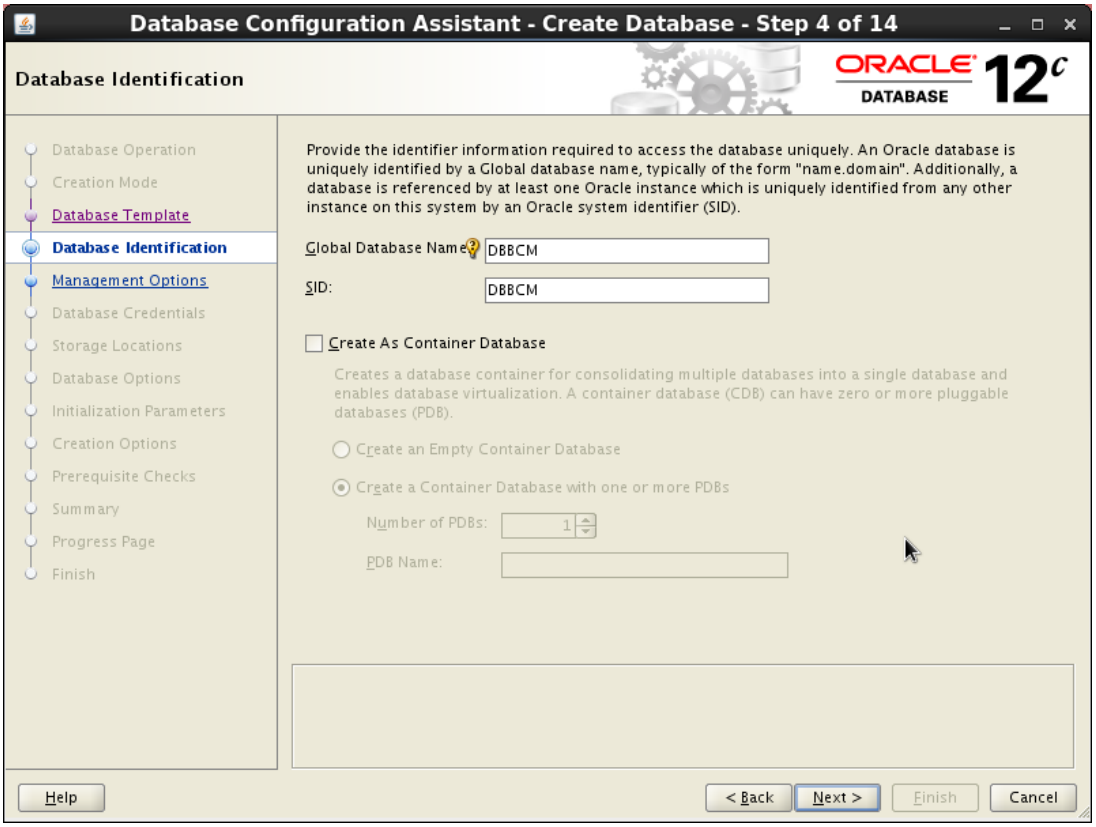
3. In step 2 - **Create Database** select **Advanced Mode** and click **Next** .



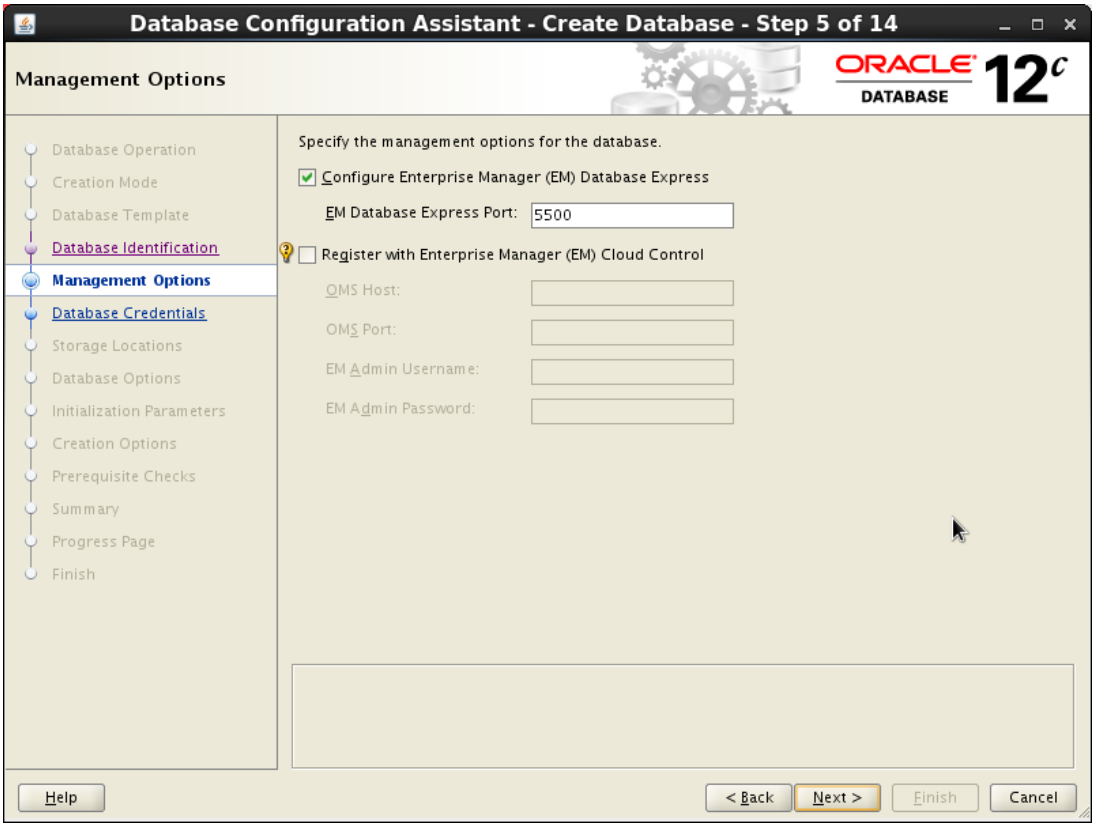
4. In step 3 - **Database Template** select **Custom Database** box, and then click **Next** .



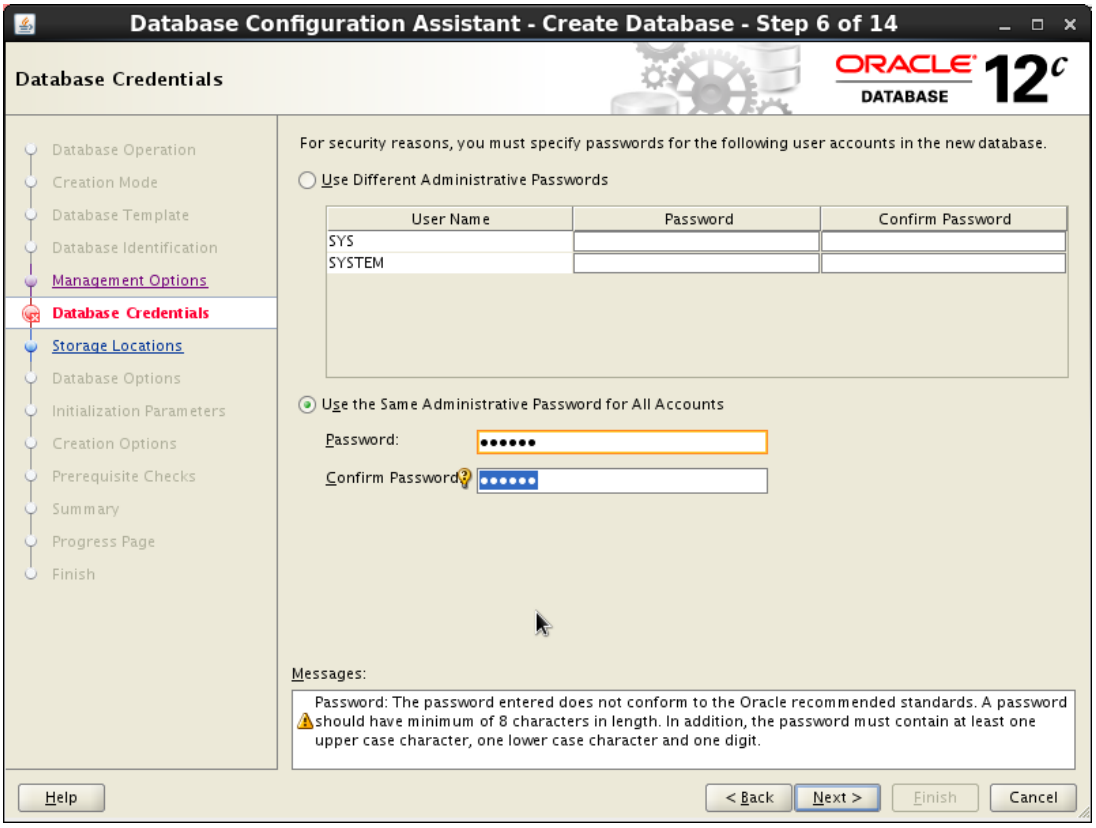
5. In step 4 - **Database Identification** enter a name for the new database in the **Global Database Name** box, if you do not want to use the default name, and then click **Next** .



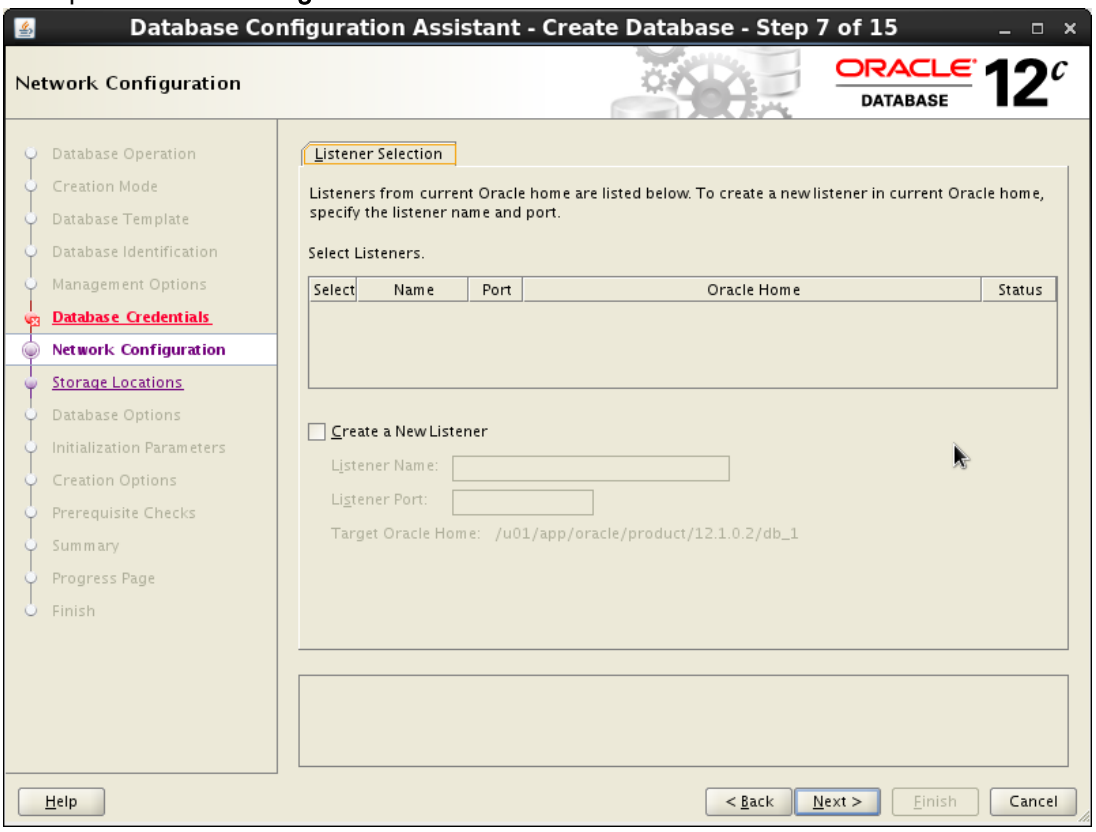
6. In step 5 - **Management Options** configure the **Enterprise Manager** and consult your DBA as needed. Then click **Next** .



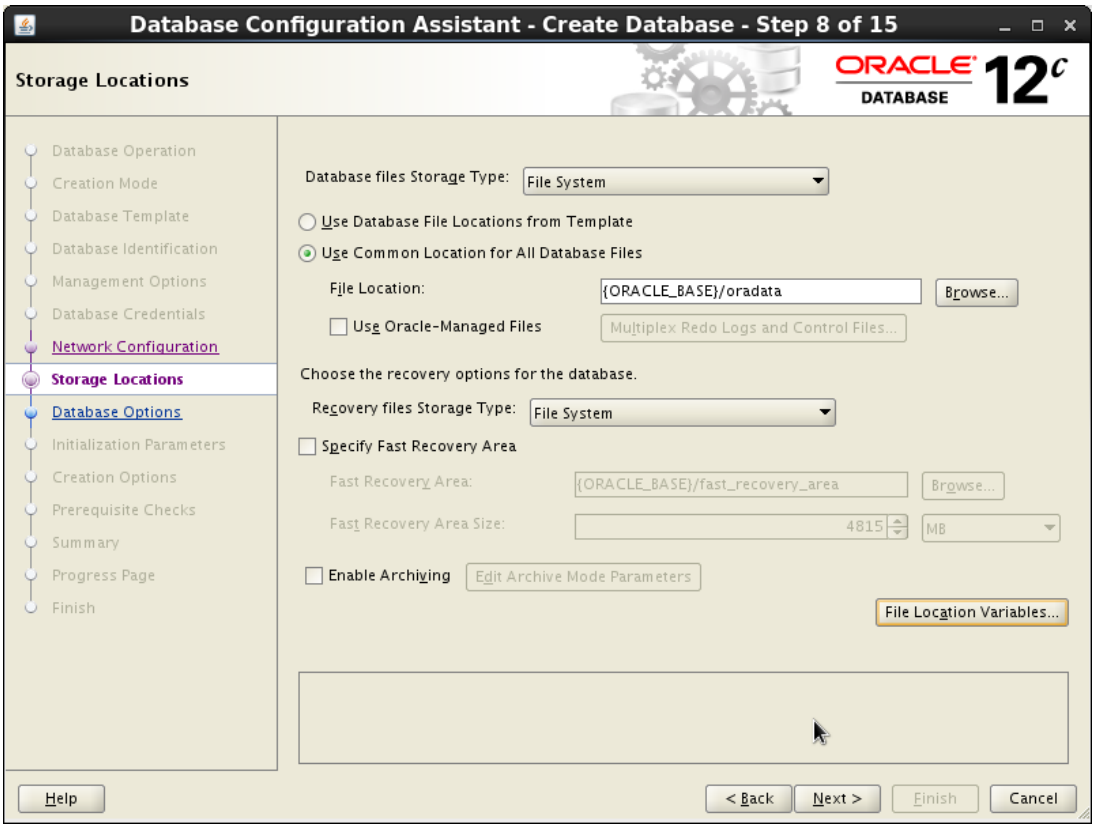
7. In step 6 - **Database Credentials** configure the passwords and click **Next** .



8. In step 7 - **Network Configuration** click **Next** .

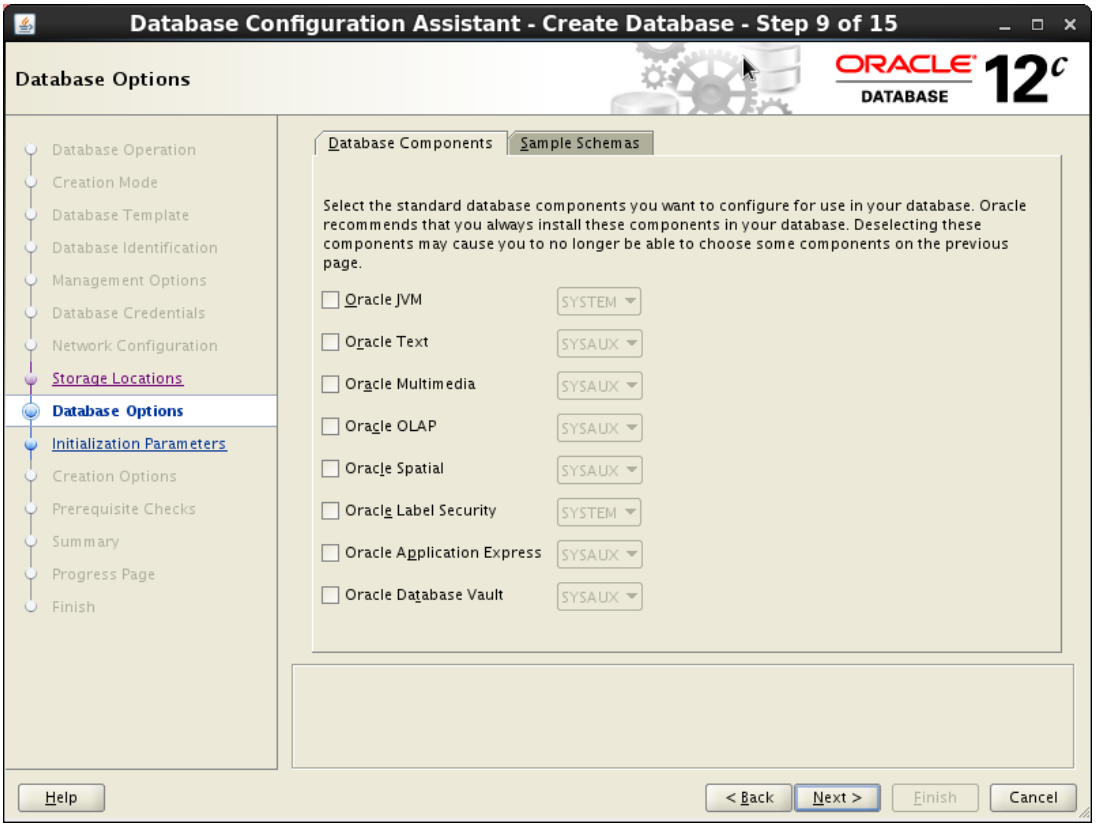


9. In step 8 - **Storage Locations** select the **Database files Storage Type** from the dropdown list and the **Use Common location for All Database Files** option. Click **Next** .



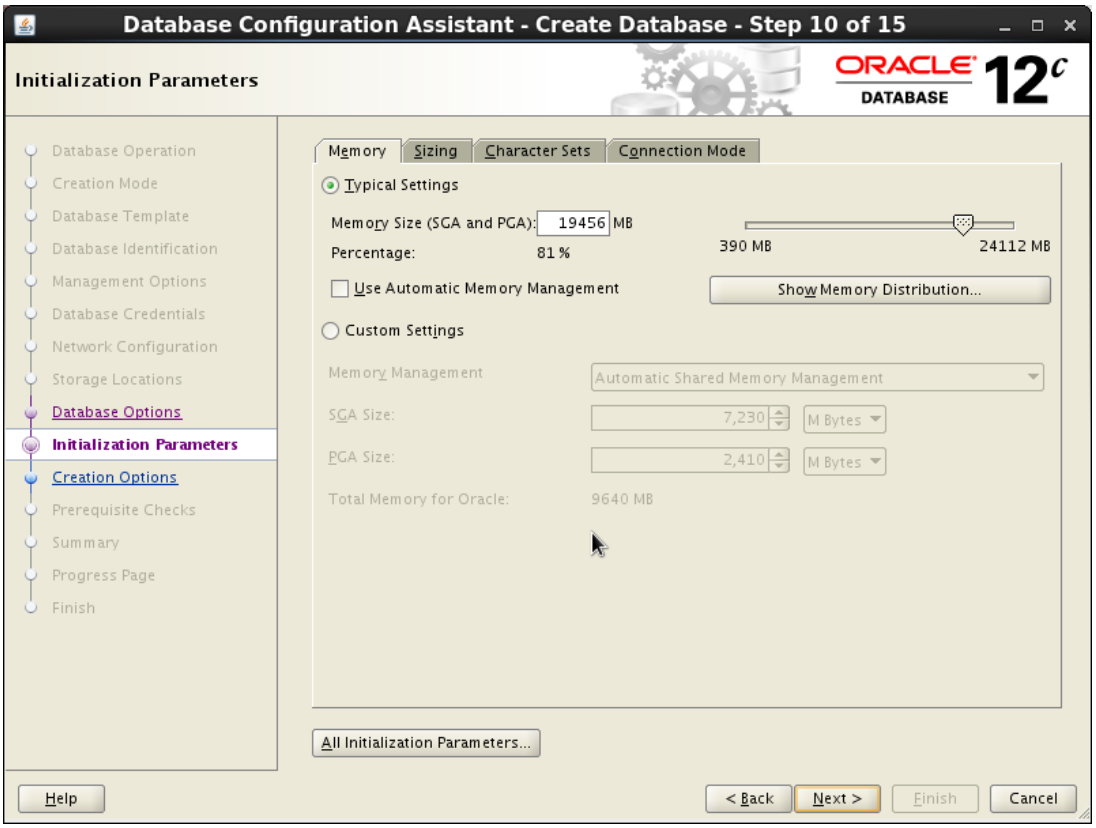
- Consult the Disk Layout topic for the recommended disk layout.
- Consult your DBA for any additional required information.

10. In step 9 - **Database Options** clear all unnecessary components and consult your DBA as needed. Click **Next** .

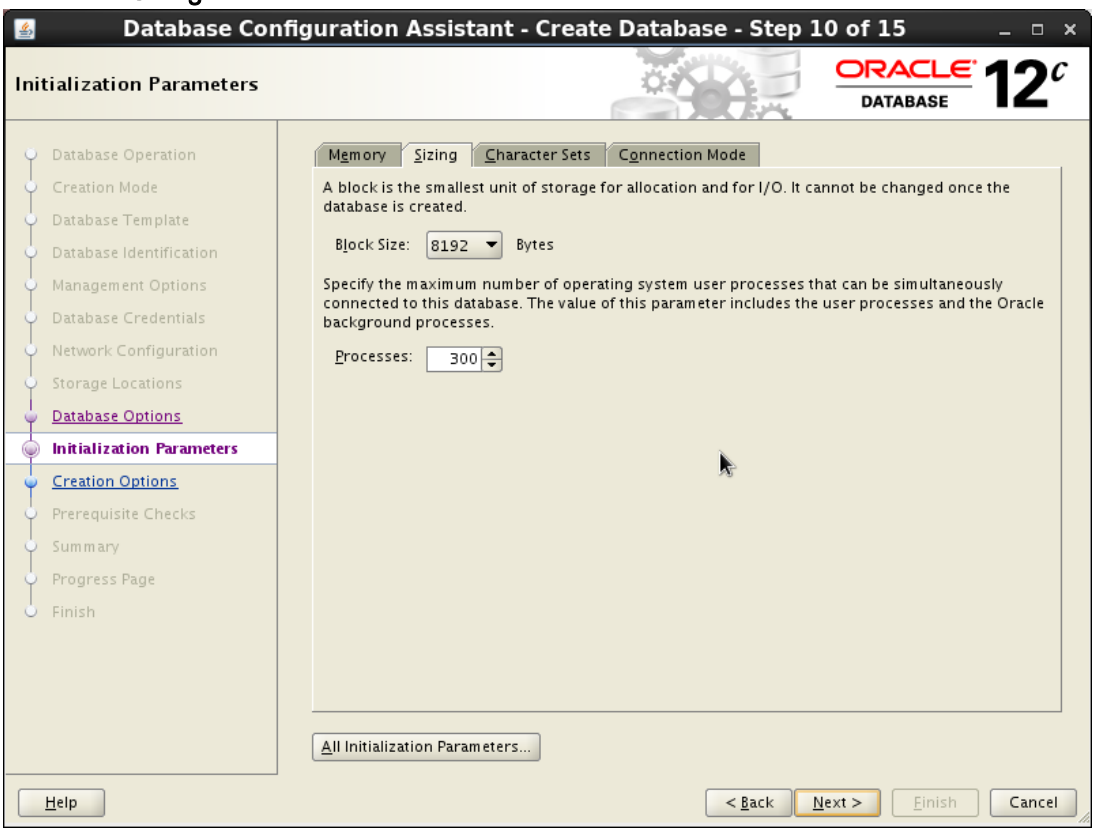


11. In step 10 - **Initialization Parameters** select **Typical** and allocate the memory.

> Consult the Oracle Memory Management topic for the recommended memory size.



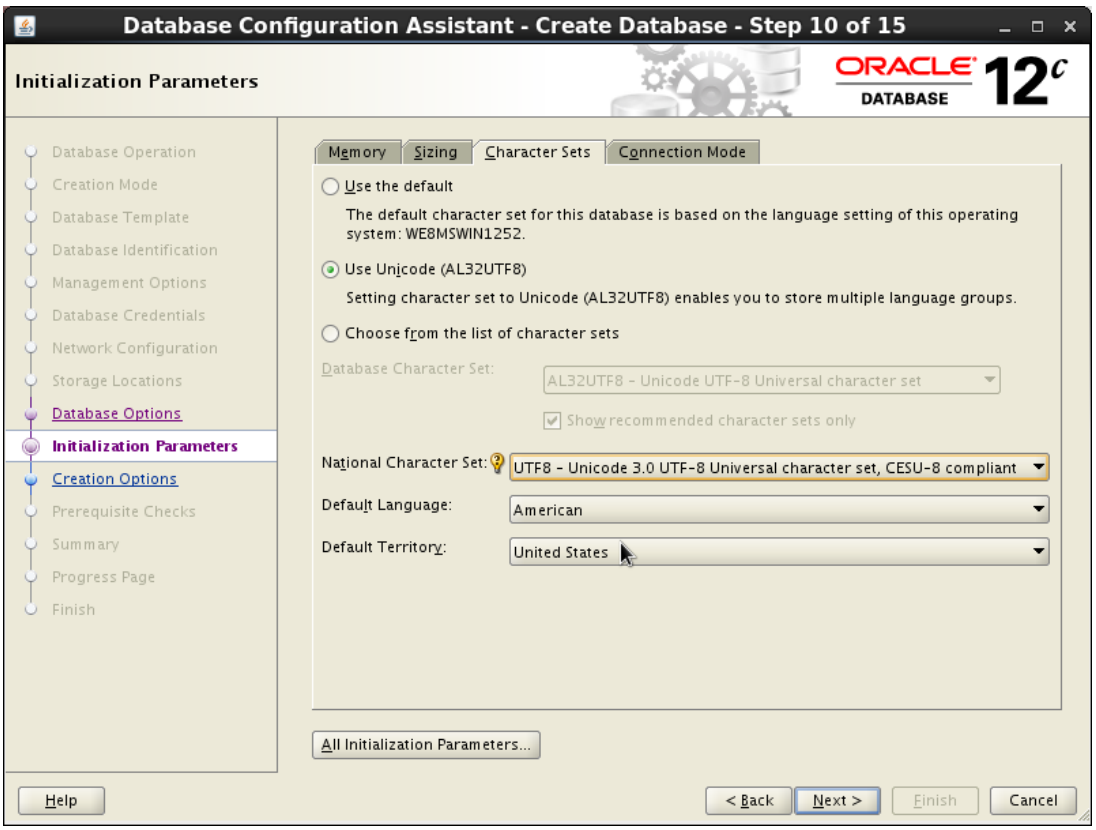
12. Select the **Sizing** tab.



13. Configure the block size and number of background processes.

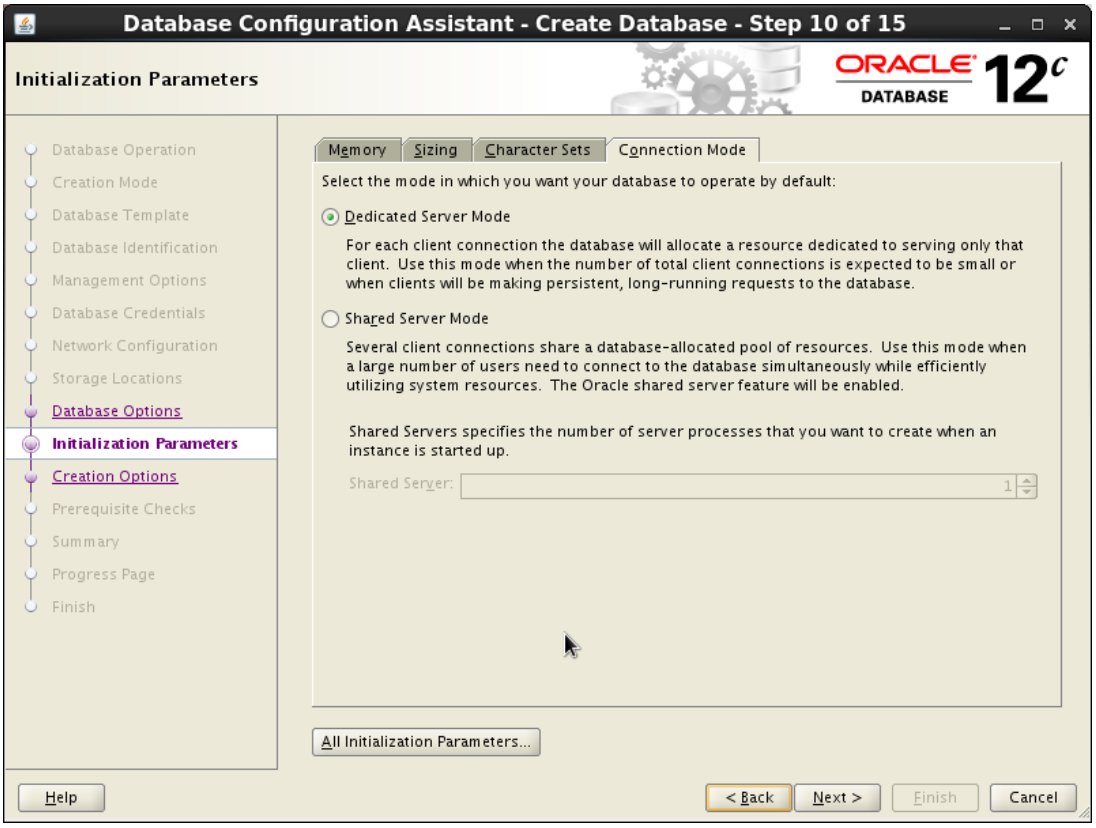
Consult your DBA as needed.

14. Select the **Character Sets** tab.



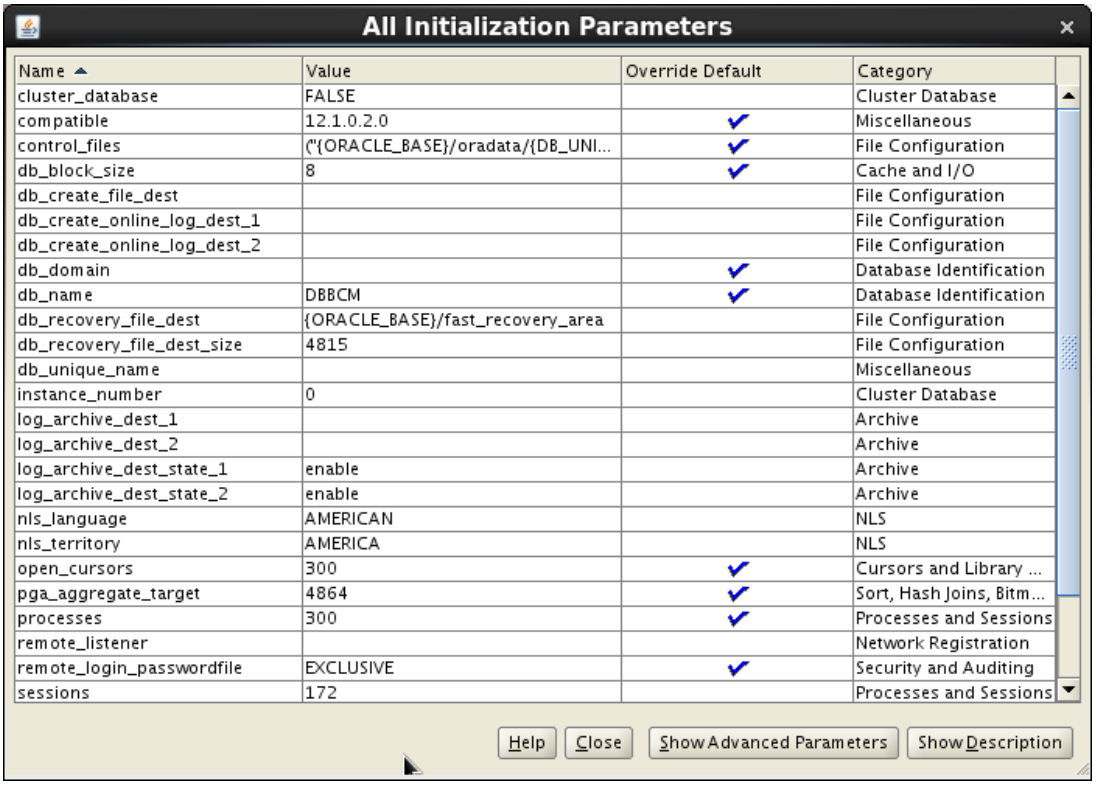
15. Select **Use Unicode (AL32UTF8)** .
16. In the **National Character Set** box select **UTF8 - Unicode 3.0 UTF-8** .
17. *(Optional)* Modify the **Default Language** and **Default Territory** if necessary.

18. Select the **Connection Mode** tab.



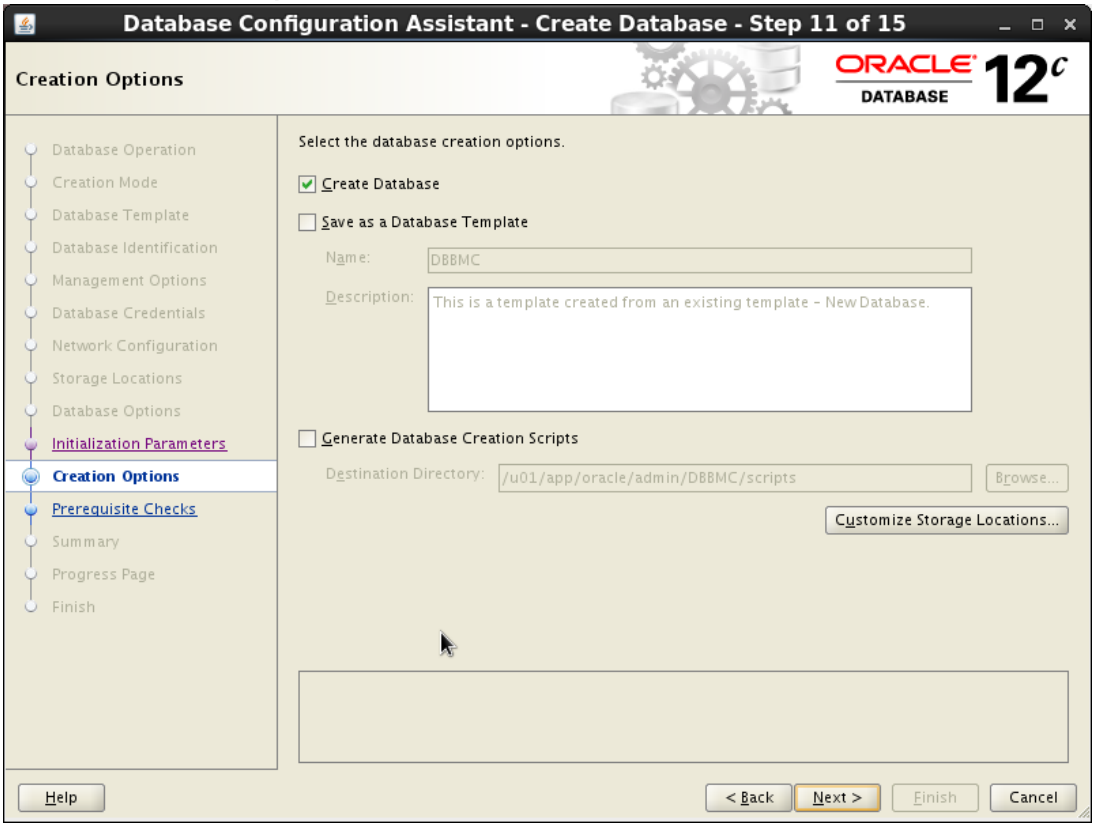
19. Select **Dedicated Server Mode** .

20. Click **All Initialization Parameters** .A table with all initialization parameters and their properties displays in a new window.

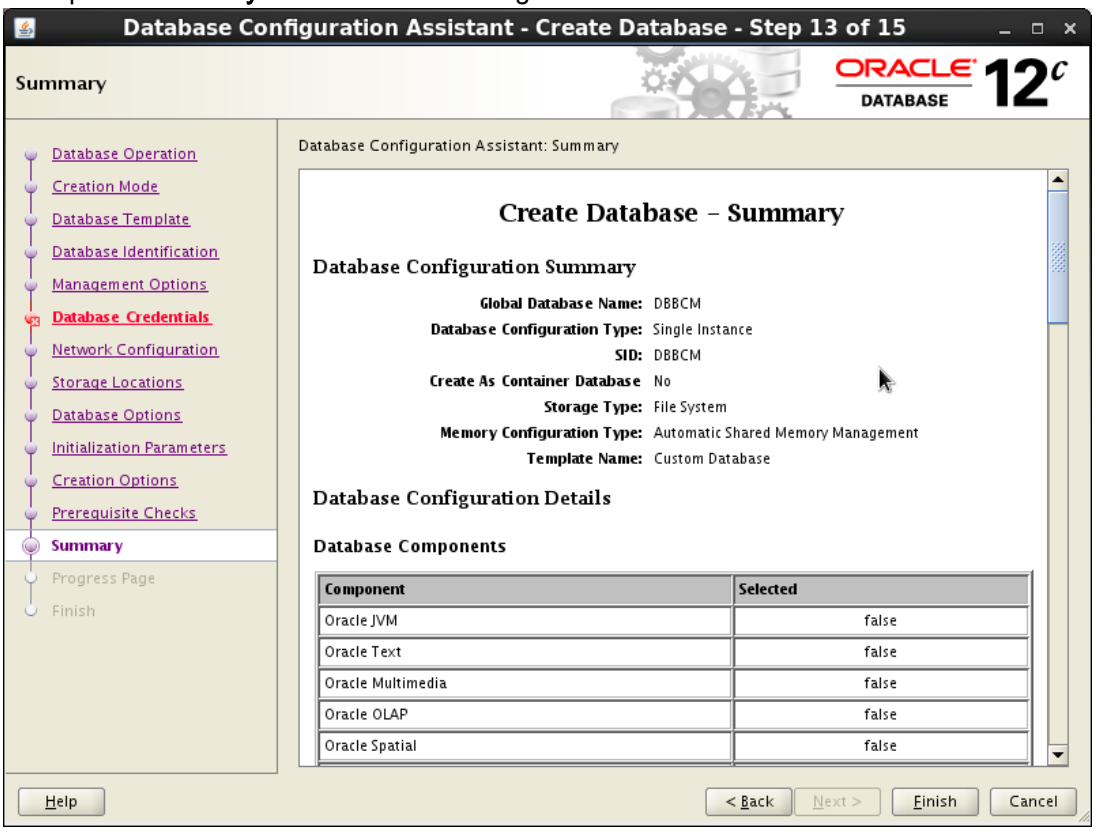


21. Click **Advanced Parameters** to display the complete list.
22. Modify the values of the parameters as explained in Oracle database initialization parameters .
23. Click **Close** and **Next** .

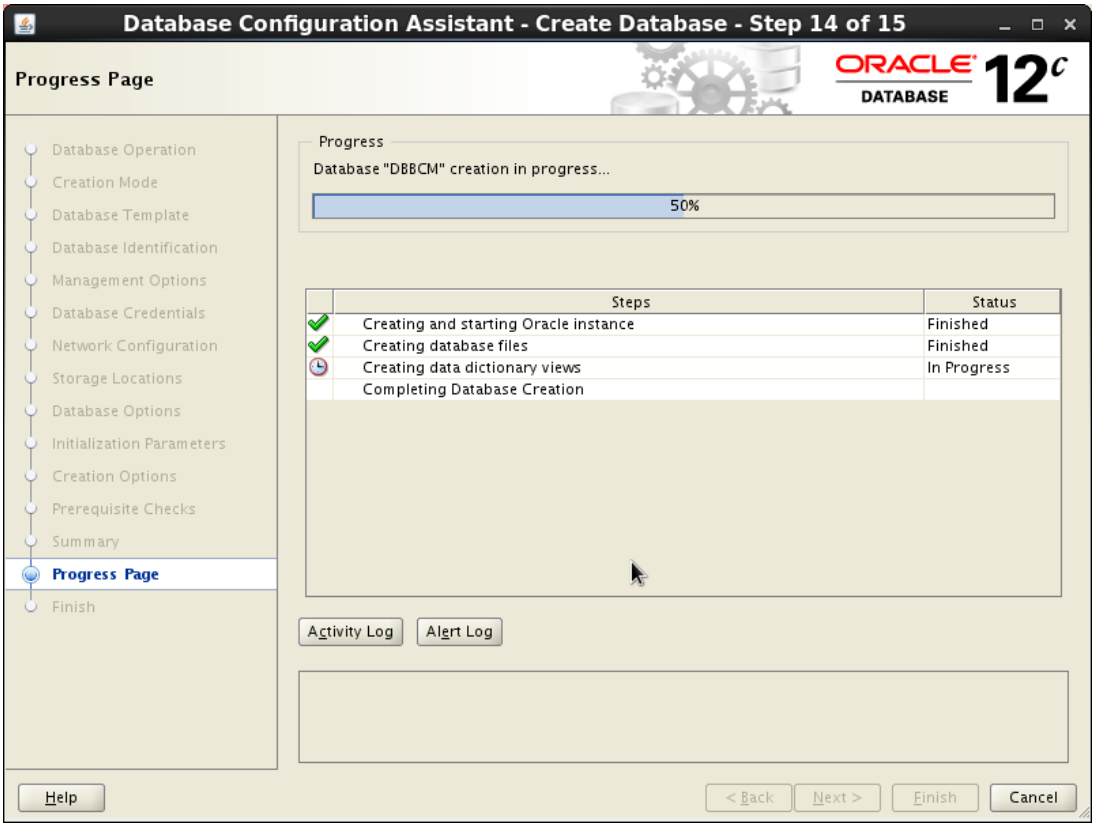
24. In step 11 - **Creation Options** click **Finish** .



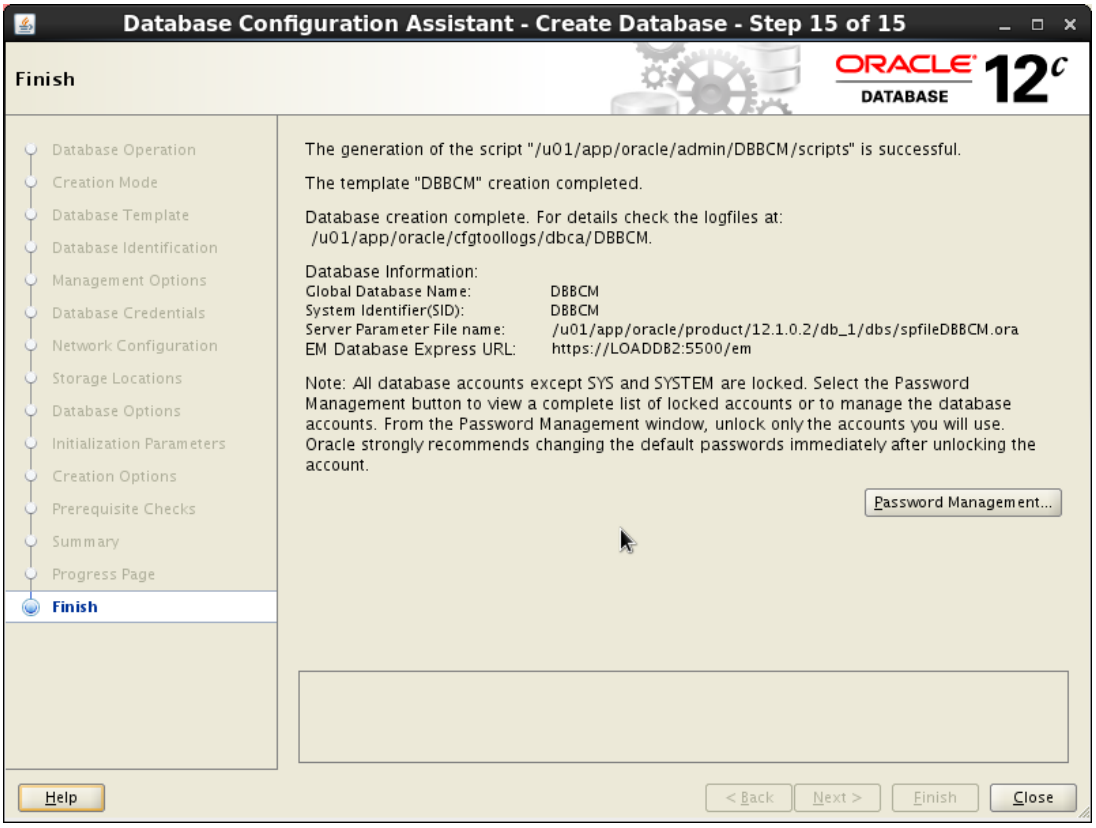
25. In step 13 - **Summary** click **Finish** if all configuration values are correct.



26. Wait for the database creation process to finish, then click **Finish** .



27. Click **Close** .



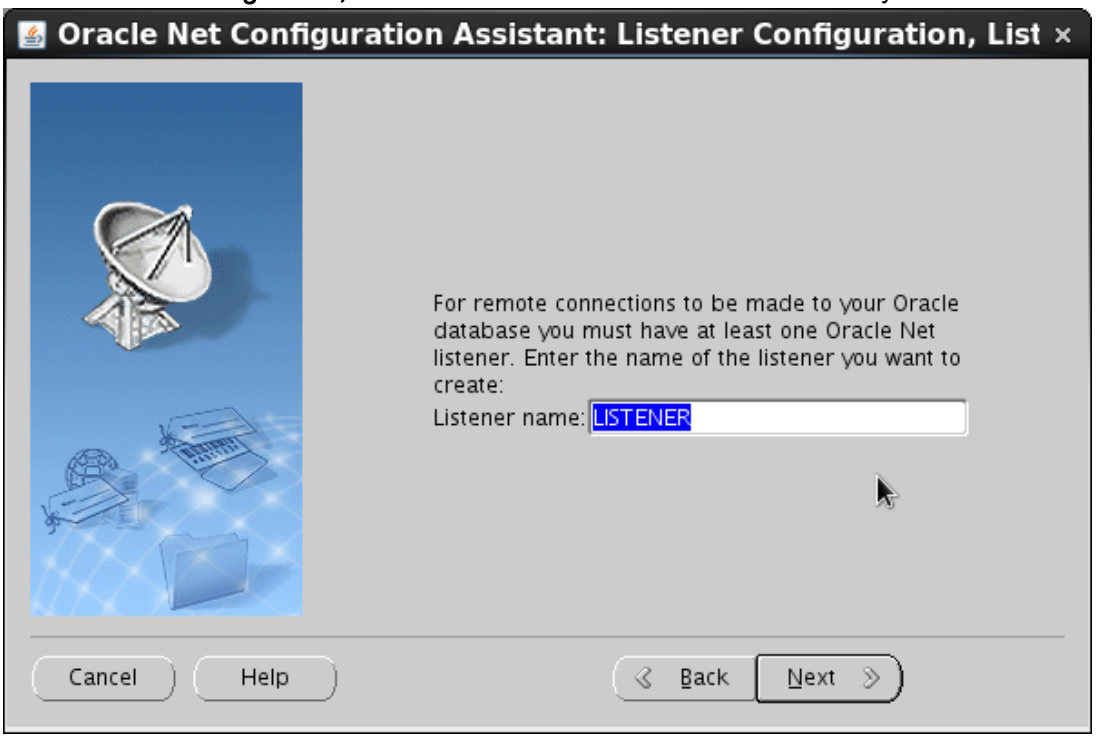
Configuring a LISTEN processe

As the last step of the database configuration, a listen process must be configured via the **Oracle Net Configuration Assistant** :

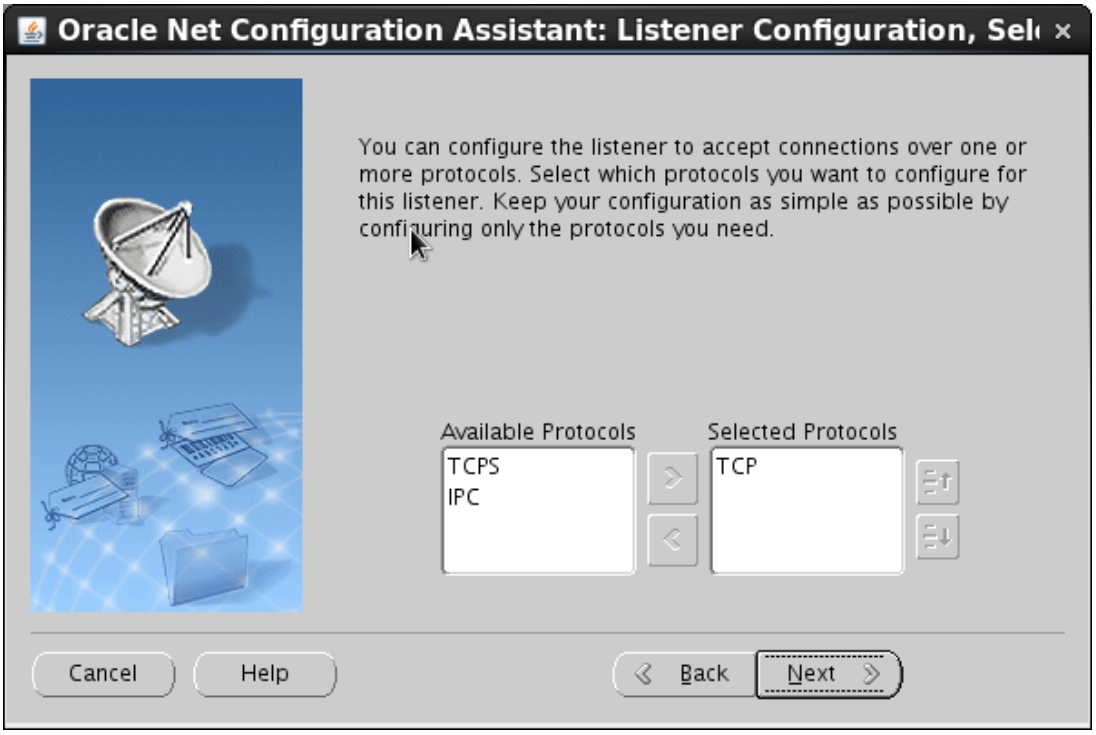
1. Start the **Oracle Net Configuration Assistant** with the `netca` command.The **Oracle Net Configuration Assistant** appears with its **Welcome** window.

2. Select **Listener Configuration** and click **Next** .The **Listener Configuration, Listener** window appears.

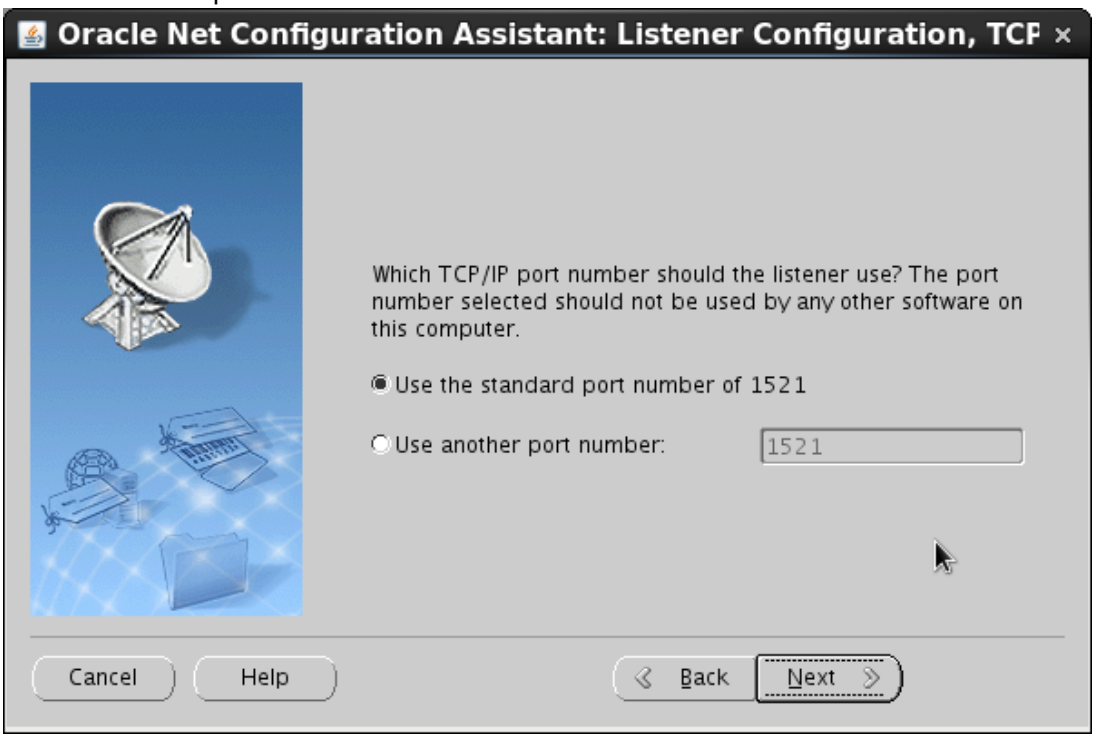
3. Ensure that the **Add** option is selected and click **Next** .
4. In the **Listener Configuration, Listener Name** window Click **Next** without any modifications.



5. In the **Listener Configuration, Select Protocol** window select the **TCP** protocol in the **Available Protocols** list box and move it to the right to the **Selected Protocols** box.

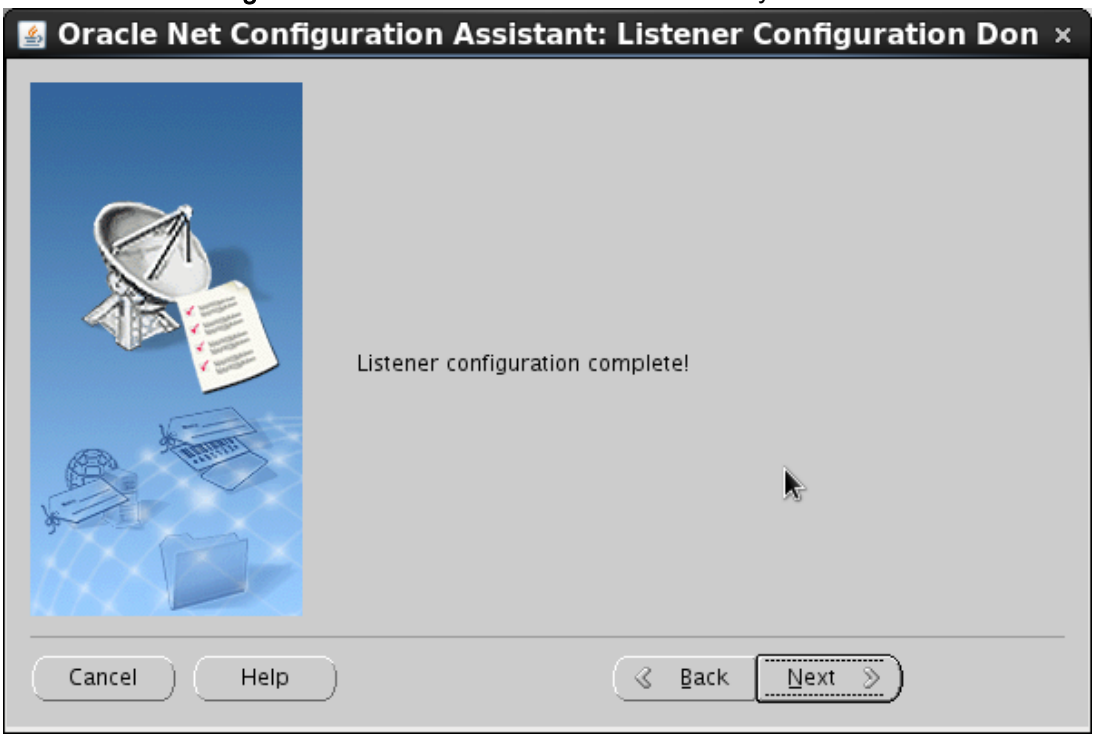


6. Click **Next** .
7. In the **Listener Configuration, TCP/IP Protocol** window ensure that the **Use the standard port number of 1521** option is selected and click **Next** .



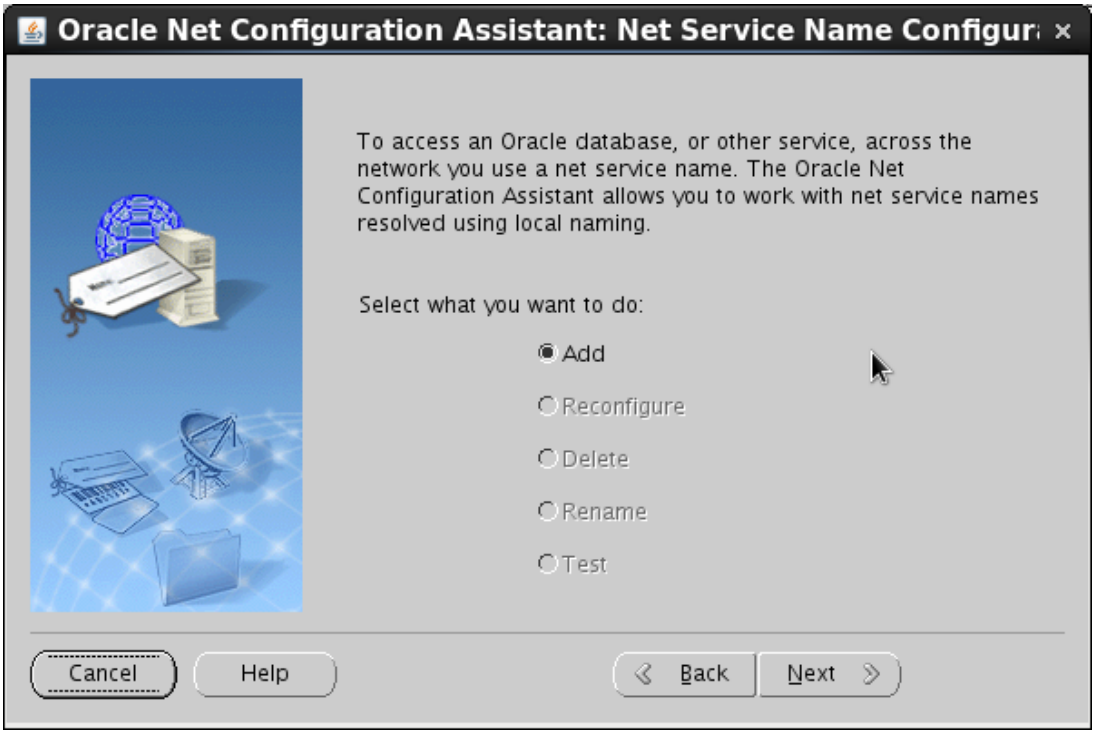
8. In the **Listener Configuration, More Listeners?** window click **Next** without any modifications.

9. In the **Listener Configuration Done** window click **Next** without any modifications.

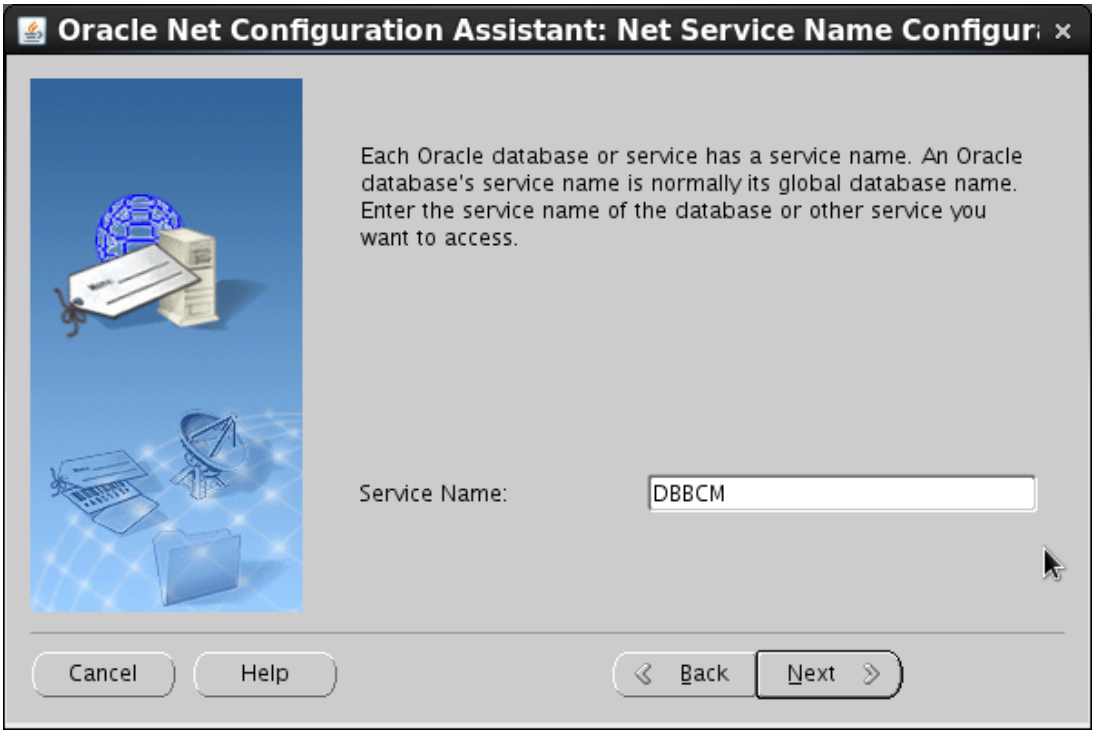


10. In the reappearing **Welcome** window select this time the **Local Net Service Name Configuration** option and click **Next** .

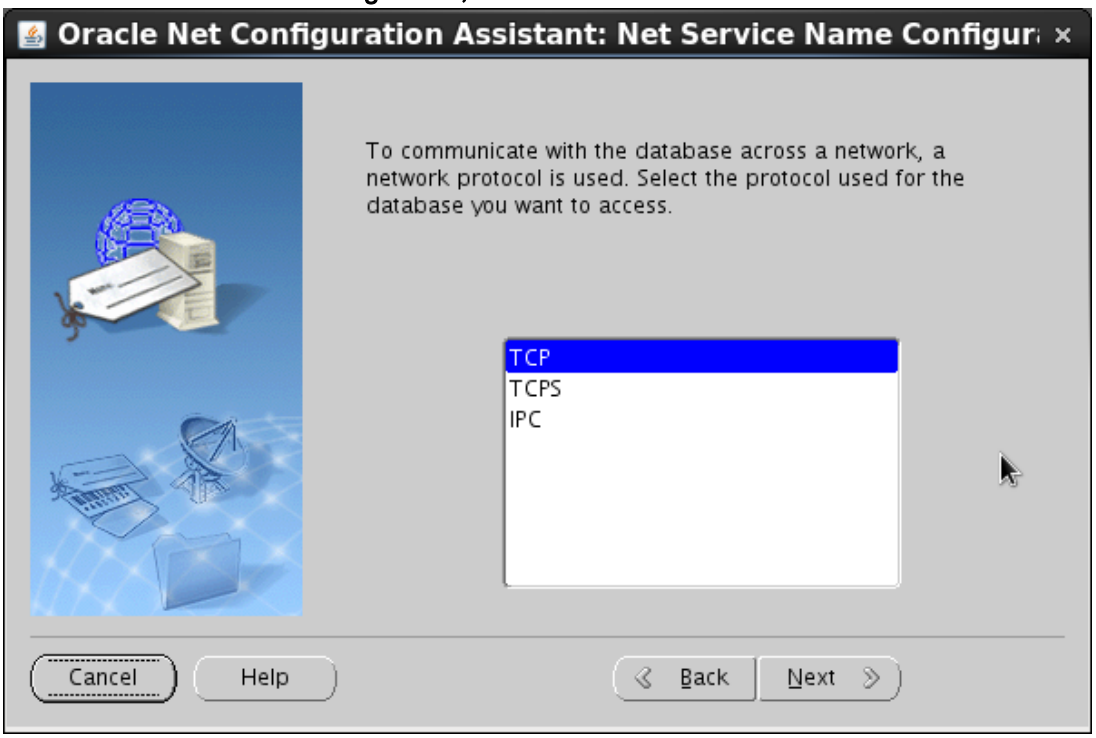
11. In the **Net Service Name Configuration** window ensure that the **Add** option is selected and click **Next** .



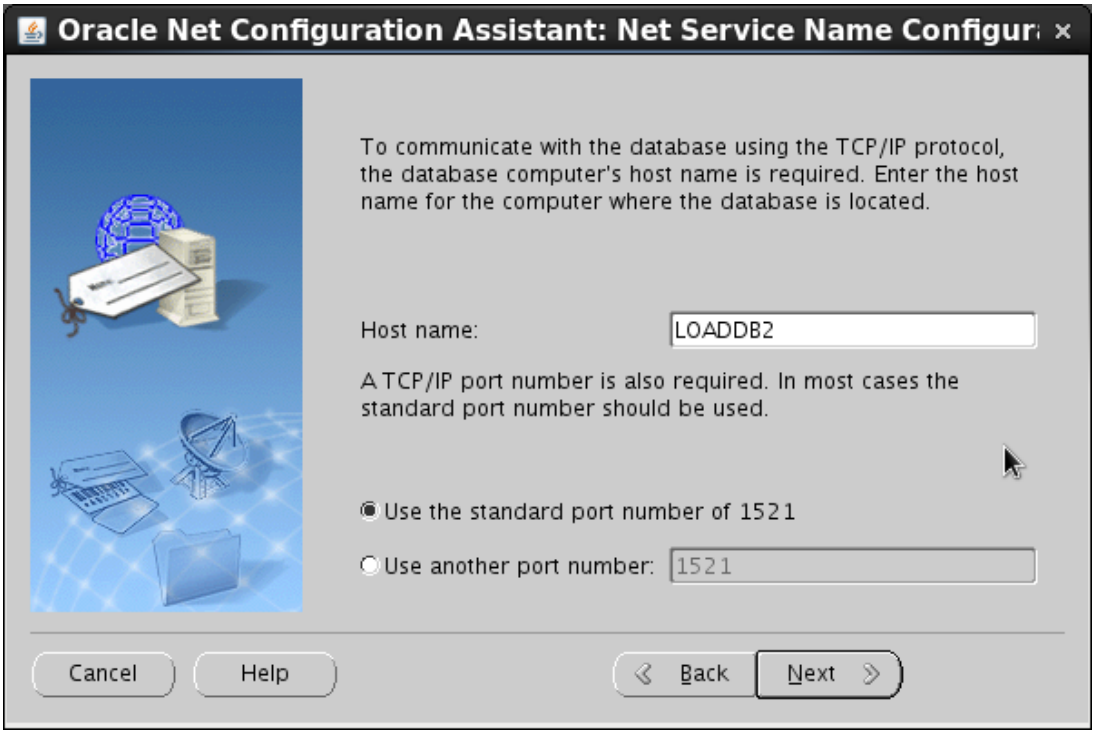
12. In the **Net Service Name Configuration, Service Name** window enter the name for the service into the **Service Name** box, for example *DBBCM* and click **Next** .



13. In the **Net Service Name Configuration, Select Protocols** window select **TCP** and click **Next** .

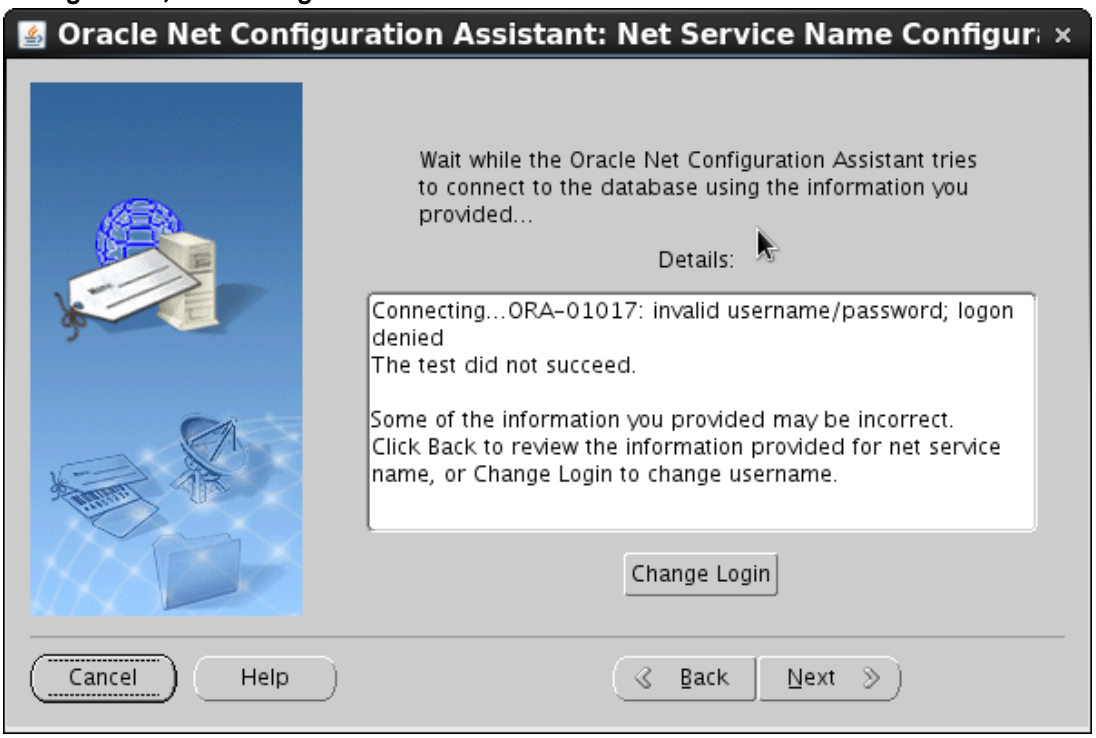


14. In the **Net Service Name Configuration, TCP/IP Protocol** window enter the name of the computer on which the database is located, either as its short or long network name or its IP address.

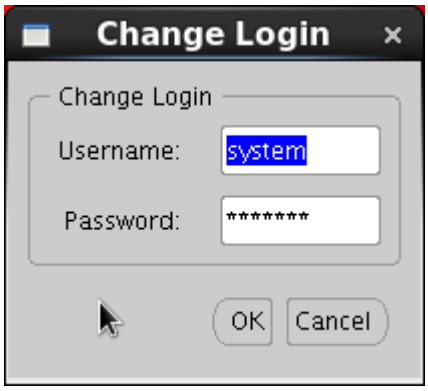


15. Ensure that the **Use the standard port number of 1521** is selected and click **Next** .
16. In the **Net Service Name Configuration, Test** window select **Yes, perform a test** and click **Next** .

17. If the test failed due to wrong credentials click **Change Login** in the **Net Service Name Configuration, Connecting** window.

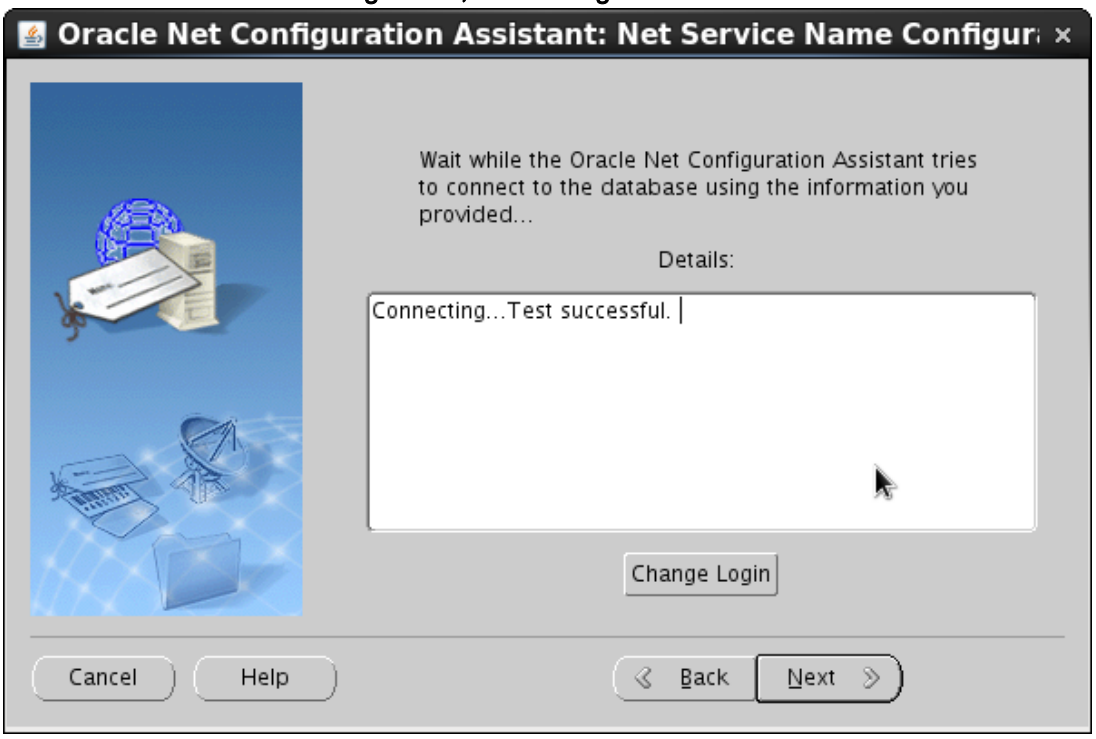


18. In the **Change Login** window enter a valid login and password, one of those that are defined in the **Database Credentials** step of the database procedure. By default the SYSTEM account and password are used.



19. Click **OK** to close the window.

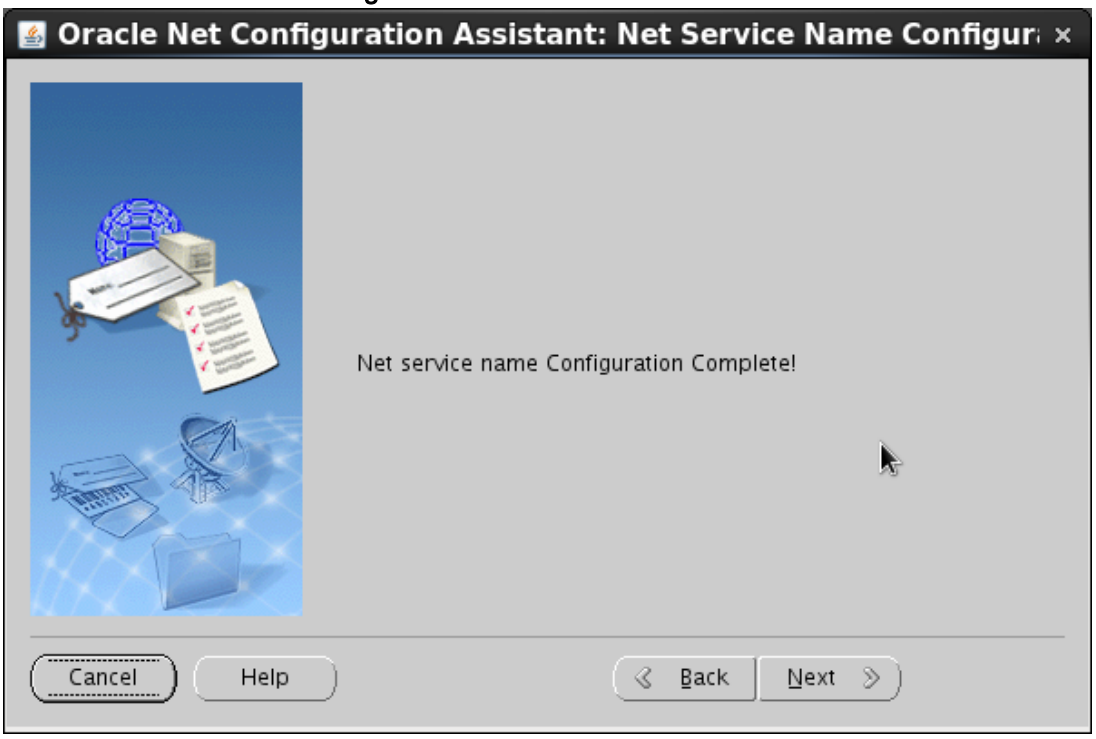
20. In the **Net Service Name Configuration, Connecting** window click **Next** .



21. In the **Net Service Name Configuration, Net Service Name** window enter a name for the net service, for example **bcmdb** , and click **Next** .

22. In the **Net Service Name Configuration, Another Net Service Name?** window leave **No** selected and click **Next** .

23. In the **Net Service Name Configuration Done** window click **Next** .



24. In the reappearing **Welcome** window click **Finish** to terminate the wizard.

The database is now set up and configured for use with the BMC Client Management agent. However, before you can install the CM master on this computer, you need to ensure that the prerequisites that are listed in topic Creating a database on Oracle versions 10g, 11g or 12c for Windows or Oracle versions 10g, 11g or 12c prerequisites for Linux are fulfilled.

You can find more installation related information under http://oracle-base.com/articles/12c/oracle-db-12cr1-installation-on-oracle-linux-6.php .

Step Reference

The CM software comes with a number of predefined operational rules and steps which are divided according their functionalities into groups.

This section provides reference information for all predefined steps including their parameters, default values, and descriptions. They are divided according to their functionalities(for example, Agent Configuration, Inventory Management, Patch Management, etc.).

The following topics are provided:

- The step properties window
- Related topics

The step properties window

To initially select a step for an operational rule or modify it later on, the **Properties** window appears. It has three tabs:

- **Parameters**
  In this tab all step parameters are listed and need to be defined. You can also modify parameters here. Any parameter with an asterisks (*) next to its label is a mandatory parameter.
  The topics following this section provide detailed information about all parameters of the individual steps.
- **Workflow**
  In this tab the verfication and stop conditions of the step within the operational rule are defined. To specify if verification and stop conditions are to be applied for this step, reply to the questions by selecting the respective answer from the list boxes.
  This tab replaces the **Verification Condition** and **Stop Condition** parameters of former BMC Client Management (formerly *BMC FootPrints Asset Core*) versions, that were the first parameters of all steps.
- **Information**
  This tab shows additional general information about the step, none of these values can be modified apart from the **Notes** box, in which you can enter any additional pertinent information regarding this step or its use.

Related topics

- Agent Configuration steps
- Custom Inventory steps
- Directory and File Handling steps
- Event Log Manager steps
- Hardware Inventory steps
- Inventory Management steps
- Master Steps steps
- Monitoring steps
- Package Factory steps
- Patch Management steps
- Power Management steps
- Process Management
- Security Settings Inventory steps
- Software Distribution steps
- Tools steps
- User Message Box steps
- Virtual Infrastructure Management steps

- Windows steps
- Windows Device Management steps
- Windows XP and 2003 Firewall steps

Agent Configuration steps

/*<![CDATA[*/ div.rbtoc1501563594761 {padding: 0px;} div.rbtoc1501563594761 ul {list-style: disc;margin-left: 0px;} div.rbtoc1501563594761 li {margin-left: 0px; padding-left: 0px;} /*]]>*/

- Agent Interface Access Configuration
- Agent Parameter Setup
- Application Monitoring Module Setup
- Application Synchronization
- Asset Discovery Module Setup
- Asynchronous Actions Module Setup
- AutoDiscovery Module Setup
- Cisco NAC Module Setup
- Custom Inventory Module Setup
- Custom Package Module Setup
- Event Log Manager Module Setup
- Event Manager Module Setup
- File Store Module Setup
- Hardware Filter Synchronisation
- Hardware Inventory Module Setup
- Identity Module Setup
- Load/Unload Module
- Logging Configuration
- MSI Package Module Setup
- Manual File Upload
- Master Information Configuration
- Non-intrusive Reboot Mode Configuration
- Operational Rule Module Setup
- Package Synchronization
- Patch Management Module Setup
- Patch Synchronization
- Power Management Module Setup
- Reboot Window Synchronization
- RPM Package Module Setup
- Relay Module Setup
- Remote Control Module Setup
- Restart Agent
- Rollout Module Setup

- Rule Synchronization
- Security Configuration
- SCAP Compliance Module Setup
- Security Settings Inventory Module Setup
- Security Products Management Module Setup
- Selfhealing Module Setup
- Snapshot Package Module Setup
- Software Filter Synchronisation
- Software Inventory Module Setup
- Timer Module Setup
- Transfer Window Synchronization
- Upload Operational Rule Status
- User Access Module Setup
- Virtual Infrastructure Manager Module Setup
- WakeOnLan Module Setup
- Web Services Module Setup
- Windows Device Management Module Setup

Agent Interface Access Configuration

This step defines which tabs of the agent browser interface are accessible and which authentication information is required. For options which are not activated in this step, the predefined default values will be used.

Parameter	Description
Access to "Inventories"	Check this box if the access to the **Inventories** pages is to specifically defined: • **All** : Allows all users to connect to the tab, that is, the locally logged user as well as any users on remote devices. • **Local Only** : Only allows the locally logged user to connect to the page. • **None** : Prohibits the access to the tab for all users.
Access to "MyApps"	Check this box if the access to **MyApps** is to be specifically defined: • **Local Only** : Only allows the locally logged user to connect to the page. The user must log on to the page with an administrator login to the local device. • **None** : Prohibits the access to the tab for all local users.
Access to "Maintenance"	Check this box if the access to the **Maintenance pages** is to specifically defined:

Parameter	Description
	• **All** : Allows all users to connect to the tab, that is, the locally logged user as well as any users on remote devices. Any user must log on to the page with an administrator login to the local device. • **Local Only** : Only allows the locally logged user to connect to the page. The user must log on to the page with an administrator login to the local device. • **None** : Prohibits the access to the tab for all users.
Access to "Privacy"	Check this box if the access to the **Privacy** pages is to specifically defined: • **All** : Allows all users to connect to the tab, that is, the locally logged user as well as any users on remote devices. Any user must log on to the page with an administrator login to the local device. • **Local Only** : Only allows the locally logged user to connect to the page. The user must log on to the page with an administrator login to the local device. • **None** : Prohibits the access to the tab for all users.
Access to "Helpdesk Ticket"	Check this box if the access to the **Helpdesk Ticket** pages is to specifically defined: • **All** : Allows all users to connect to the tab, that is, the locally logged user as well as any users on remote devices. Any user must log on to the page with an administrator login to the local device. • **Local Only** : Only allows the locally logged user to connect to the page. • **None** : Prohibits the access to the tab for all users.
Access to "Tools"	Check this box if the access to the **Tools** pages is to specifically defined: • **All** : Allows all users to connect to the tab, that is, the locally logged user as well as any users on remote devices. Any user must log on to the page with an administrator login to the local device. • **Local Only** : Only allows the locally logged user to connect to the page. The user must log on to the page with an administrator login to the local device. • **None** : Prohibits the access to the tab for all users.
Login for "Inventories"	Check this box if the access to the **Inventories** pages requires specific login parameters. If this option is not activated the default value (Remote Login) is used: • **Authentication** : Requires a valid user authentication to the local device for all permitted users. • **Remote Login** : Requires a login if the user tries to remotely log on to the page. Local users do not need to provide a login. • **No Login** : Neither local nor remote users need to provide a login to access the page.

Parameter	Description
Login for "Helpdesk Ticket"	Check this box if the access to the **Helpdesk Ticket** pages requires specific login parameters. If this option is not activated the default value (Authentication) is used: • **Authentication** : Requires a valid user authentication to the local device for all permitted users. • **Remote Login** : Requires a login if the user tries to remotely log on to the page. Local users do not need to provide a login. • **No Login** : Neither local nor remote users need to provide a login to access the page.

Agent Parameter Setup

This step allows you to define the parameter settings of the BCM agent.

Parameter	Description
Access Control	Defines the security when agents communicate with each other, that is, if the Precision Access Control (PAC) handshake is to be used for inter-agent communication: • **No** : as a server, allow PAC connections with client authentication as well as non PAC connections. As client, no PAC connections are required. • **Securised Send, Receive Both** : as server, allow PAC connections with client authentication as well as non PAC connections. As client, only allow PAC connections. • **Yes** : Only allow PAC connections (as server or client). • **Yes with mutual authentication** : Only allow PAC connections (as server or client) with mutual authentication.
Secure Communication	Defines if the agent communicates in secure format. The possible values are: • **No** : With this option the agent accepts both securized and non- securized communication, however it sends only non- securized communications. • **Securized Send, Receive Both** : This value indicates that the agent accepts both securized and non-securized communication, however it sends only securized communications. • **Yes** : When this option is selected the agent only communicates in secure mode, that is, it only receives and sends securized communication.Yes with mutual authentication: With this option the agents communicate in secure mode and in addition authenticate each other via SSL.
Authority Certificate	The authority certificate (CA Cert) to be used for signing the agent certificate if required. By default, the Numara CA is used unless a different CA Cert is configured. The parameter expects a certificate name (without extension) registered in the agent cert store (auth section), such as *Numara_ca* . This parameter is used on the server side and can also be used on the client side if the server is configured to authenticate the client.
Trusted Authorities	

Parameter	Description
	A comma separated list of certificates to be trusted when connecting to a secured server or client. By default, the agent trusts the default Numara CA unless a different list of certificates is configured. The parameter expects a list of certificate names (without extension) registered in the agent cert store (trusted section), for example, *Numara_ca, enterprise_ca, startfleet_ca* . This parameter is used on the client side as well as on the server, for the device to know if it can trust the answering device by comparing its certificate with the list of trusted certificates, if it does not match the authority certificate.
User Certificate	The user defined final certificate to be used for both the client and server roles. When this parameter is configured the agent ignores any other authority except the ones to be trusted. The parameter expects a certificate name (without extension) registered in the agent certificate store (user section), for example, *Numara, enterprise, starfleet* .
Block Navigation from Agent User Interface	Check this box if the agent user interface is to be run in the browser's kiosk mode (fullscreen without menus or naviation bar). The installation of an add-on may be necessary to be able to use this mode (for example, with Firefox).
Strict Agent User Interface Authentication	Indicate ifthe user can apply operational rules assigned to the device without explicit authentication. If the strict authentication mode is disabled the user is able to execute operational rules locally without authentication. Enabling this parameter forces user authentication for all cases. This parameter is ignored for rules that are assigned to users.
Icon Mode in SysTray (Windows only)	Defines the mode of the icon in the systray.
Message for New Packages (Windows only)	Indicates if a pop-up must appear if an operational rule is published while the systray is hidden.
New Advertisment Banner (Days)	Define the length of time in days that the **New** banner should be shown for operational rules that are newly advertized in MyApps. Setting this number to zero disables the new banner.
Send alert when an error occured	Check this box if an alert is to be sent to the master when an error is added to the agent log file.

Application Monitoring Module Setup

The Application Management module manages monitored and prohibited applications through the BCM agents. This step allows you to specify the default settings of application monitoring. This step does not apply to Mac OS systems.

If a reboot is scheduled, you can define the reboot parameters and message, which may also be localized. The logo of the message box may be customized as well. For this you only need to store the following customized images in their exact sizes in the *//data//core//res* directory of the BCM agent: FullSized.bmp (575 x 575 pixels), MediumSized.bmp (575 x 510 pixels), SmallSized.bmp (575 x 455 pixels), RebootAfterLogOut.bmp (575 x 275 pixels).

Parameter	Description
Verification Interval (sec)	Defines in seconds the interval at which any type of monitored application, that is, monitored and prohibited, are checked.

Parameter	Description
Stop Application if Prohibited	Check this box to prohibit applications. This means that applications which are monitored under the respective node is terminated if they are found running on the client.
Popup Window after Application Termination	Check this box to display a pop-up window on the screen to inform the user that the application he just tried to launch was automatically stopped because it is prohibited.
Event Creation Delay for Unterminated Monitored Applications (hours)	Specifies the number of hours after which an event is created, even if the launched application has not yet been terminated. In this case the end date of the generated event is the same as the start date. Once the application is terminated a new event is generated with the proper end date filled in.
Local Image File Path (bmp only)	The name and full path of the image file that is to be displayed in the pop-up window for a stopped application. The image file must be of type *.bmp* . If the image cannot be found, that is, because it is of another type, or it is too small, the default BMC image is used. If the image is too large it is cropped to fit the window. The default size of the BMC image is 460 x 310.
Popup Window Message Text	Enter the text that is to be displayed on the remote screen on which the application was stopped.

Application Synchronization

This step synchronizes applications defined for any type of application management, i.e., to be monitored, prohibited or to be protected, to which the managed devices are assigned.

When the client receives a synchronization request it sends back the list of its own managed applications linked to a checksum. The master then creates an up-to-date list of the device's managed applications and checks these with the list it received. If a managed application on the list from the device does not exist any more, the master sends an order to the device to delete it; if a more recent version of a managed application exists on the master, that is, the checksums on the master and the client are not identical, an update order will be sent to the device; and if a managed application is absent on the client but present on the master, then an assign order will be sent to the client device.

Parameter	Description
Check for Added Applications	Check this box to check for new applications that were added to be managed.
Check for Deleted Applications	Check this box to check for deleted applications in the base.
Check for Updated Applications	Check this box to check for updated applications in the base.

Asset Discovery Module Setup

This step modifies the default settings of the Asset Discovery Module, configuring the settings to execute an asset discovery scan on devices without BCM agent.

Parameter	Description
Excluded IP Address Range	Indicates the device range to be excluded from the previously defined range. The expected format is the same as for the included address range. This makes it possible to disable the scan for sensible devices even when using a short notation concerning the included device range (include: *192.168.1.0/24* and exclude: *192.168.1.255, mailserver,fileserver*).
Max. Timeout	Fine tunes the low level network packets sending, indicating the maximal time to use for scanning a single host. This allows to abort a device scan when it takes too long.
IP Address Range	Indicates the device range to be scanned. The expected format is a comma separated list of IP addresses or IP ranges. For instance, IP ranges must be supplied using different notations such as complete address range (*192.168.0.0-192.168.5.254*), a CIDR range (*192.168.1.0/24* or *2001:db8:85a3::8a2e:370:152/896*), a byte range notation (*192.168.0-5.0-254*) or single named devices (DNS, NetBIOS).nIt is strongly recommended not to specify complete subnet IPv6 address ranges, scanning these is extremely time consuming.
Hardware Inventory	Defines if a hardware inventory is to be executed on the remote device.
Software Inventory	Defines if a software inventory is to be executed on the remote device.
Max. Inventory Timeout	Indicates the global timeout for the whole session. The special value of 0 can be used to deactivate this option, that is, there is no timeout limit for the duration. Otherwise, the scan is aborted once the threshold value has been reached. The value is an integer followed by *s* for seconds or *m* for minutes or *h* for hours.
Parallel Script Count	The maximum number of scripts that can be executed simultaneously, possible values for this are **Low** - 5 simultaneous scripts, **Normal** - 10 simultaneous scripts and **High** - 20 simultaneous scripts.
Upload Policy	Indicates how and when to process the information upload. When set to **Immediate Upload** , the module uploads the inventories as soon as they are supplied by a scan. When set to **Upload at Scan End** , the inventories is uploaded when the scan is completed or aborted (except if the abort operation indicates not to upload). When set to **No Upload** , the module does not upload the inventories at all until specifically called for via the operational rule step.
Use Nmap for Port /OS Detection	Defines if BCM, if installed, is used to detect the ports and operating system of the remotely inventoried device.
Nmap Installation Path	Contains the relative installation path to the BCM software, relative to the agent installation directory, for example, *../bin* if it is located in the bin directory of the agent.
Prevent NMAP from sending IGMP paquets on the network	Check this box if some of your network devices have problems with IGMP traffic. In this case BCM is prohibited from sending IGMP paquets on the network.

Asynchronous Actions Module Setup

This step modifies the asynchronous module parameters.

Parameter	Description
Number of threads	Enter the number of threads to use for asynchronous calls
Retry Delay (Priority 0)	Enter the retry interval for calls of priority 0 in seconds (highest priority, currently not in use)
Retry Delay (Priority 1)	Enter the retry interval for calls of priority 1 in seconds (used for operational rule status and identity uploads)
Retry Delay (Priority 2)	Enter the retry interval for calls of priority 2 in seconds (used for operational rule assignments)
Retry Delay (Priority 3)	Enter the retry interval for calls of priority 3 in seconds (currently not in use)
Retry Delay (Priority 4)	Enter the retry interval for calls of priority 4 in seconds (lowest priority, currently not in use)
Prefer IP Addresses	Determines whether the identification for communication between the agents and with the master is effected via the agents' IP addresses or over their host names. This is to facilitate networking in environments that do not have DNS name resolution in place.
Time to Live (sec)	In order to prevent non-transferable data from remaining eternally in the queue, each object is assigned a specific time that it may stay in the queue and wait to be passed on its way to its destination. This Time To Live (TTL) for each object in seconds is displayed in this field.
Min Purge Delta Time (sec)	The minimum interval (in seconds) between two cleanup operations of the asynchronous actions database of all actions called since the last purge.
Maximum Action Count	The maximum number of actions that can be stored. The module refuses all incoming remote actions until the number of stored actions drops below this value.
Maximum File Count	The maximum number of files that can be stored. The module refuses all incoming remote files until the number of stored files drops below this value.

AutoDiscovery Module Setup

This step allows to modify the default settings for the parameters of the AutoDiscovery module.

Parameter	Description
Address Range	The list of addresses to be verified. The IP addresses can be listed in the following different notations: • Dotted notation, for example, 94.24.127.24 • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24, scotty.enterprise.com* .If the complete IP address range declaration is incorrect, the current subnet is scanned by default from address x.x.x.1 to x.x.x.254. If no IP address range is specified, the current subnet is scanned by default from address x.x.x.1 to x.x.x.254.
Can Learn	

Parameter	Description
	If set to true, this value specifies if the agent can get other agents' autodiscovered devices in order to establish its list.
Fast Address Verification Interval (sec)	Defines a fast search option to find the client's relay. If the list of devices is empty, the **Fast Address Verification Interval** value is used to verify devices until the **Scan Count** value is reached and all devices have been verified or a relay was found. If the client has a relay the **Address Verification Interval** value is used. If the IP address is modified, the **Fast Address Verification Interval** value is used to verify devices. The option is deactivated if the value is set to the same value as the **Address Verification Interval** value. As long as the AutoDiscovery is at the research for the device's relay, the **Parent Selection Retry Interval** to find the backup server is ignored.
HTTP Port Range	The range of ports to scan for an agent HTTP server. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 1610 and 8080 is scanned.
Maximum Device Age (sec)	The maximum age in seconds for an entry in the device list. This displays the maximum time a device can stay in the list of devices after last being verified.
Maximum Hop Count	The number of routers between the device providing the list and the device being read. The hop count is determined at discovery time using the ping. It provides an indication of the distance between the two devices and is used at the time of relay selection to sort the devices which are farther to the end of the list of relays being contacted. For example, all devices on the same LAN segment have a hop count of 0 as they can contact each other directly.
Number of Neighbors	Defines how many neighboring addresses to scan. The default value is 10, meaning 5 addresses below the device's own address and 5 addresses above it.
Only Learn Relays	Defines if the complete list of autodiscovered devices is sent to the master or if only the list of relays is uploaded.
Operating System Detection	Specifies if the operating system is discovered on the device found by AutoDiscovery.
Same Network Only	Specifies if devices found on other networks are to be accepted. The possible values are the following: • **No filter applied** : There is no filter applied to any of the discovered devices. • **Clients only** : All discovered client devices must be on the same network as the discovering device. • **Relays only** : All discovered devices, which have their relay function enabled, must be on the same network. • **All devices** : All discovered devices must be on the same network.
Scan Count	Each time scan count addresses have been verified, the module refreshes the list of addresses to verify by using the **Address Range, Number of Neighbors** and **Use Network Neighborhood** settings.
Timeout (sec)	The timeout in seconds for pings.
TCP Port Range	The range of ports to scan for a TCP connection. This is used in place of ping when raw sockets are not available. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 23, 25 and 139 is scanned. Each port range can consist of: • only one port number • one port range with the start and end port numbers separated by a dash (-), • several port ranges and/or individual port, for example: 10000-10100,20000,21000-22000 • Several port ranges must be separated by either a space, a comma (,), a semicolon (;) or a colon (:).If the whole range declaration is incorrect only default port 10000 is scanned.

Upload AutoDiscovery Objects	Defines if the objects discovered by the AutoDiscovery are uploaded.
Upload Interval (sec)	Defines the upload period for the autodiscovered list in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the autodiscovered list is uploaded to the master after being updated the first time on agent startup. It is not recommended to activate this option as, depending on the size of your network, this might be a very time and resource consuming process.
Use Network Neighborhood	Defines whether the network neighborhood should be used to get machine names and addresses.
Address Verification Interval (sec)	The gap in seconds between each address verification.

Cisco NAC Module Setup

This step allows you to modify the configuration settings of the Client Management-Cisco NAC module.

Parameter	Description
Notify Cisco agent on change of device status	Defines if the Cisco agent is informed if the 'compliancy' status of a network device changes.

Custom Inventory Module Setup

This step modifies the default settings of the parameters of the Custom Inventory module.

Parameter	Description
Data File	Specifies the location and name of the custom inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/custominventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the custom inventory may not longer work.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload on Startup	Defines if the custom inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.

Custom Package Module Setup

This step modifies the parameters of the configuration values of the custom packages.

No parameters need to be defined for this step.

Event Log Manager Module Setup

This step allows to modify the default settings for the parameters of the Event Log Manager module.

Parameter	Description
Enable Aggregation of Persistent Events	Defines whether aggregation of the events generated for the monitored models is enabled. This value is global for all the managed event log models. Aggregation computes automatic models content so disabling this option is recommended if such models should not be handled.
Minimum Upload Gap between Identical Alerts (min)	Defines the minimum interval between two same alerts that needs to pass before another alert is sent in minutes.
Enable Upload of Persistent Events	Defines whether the upload of the events generated for the monitored models is enabled. This value is global for all the managed event log models. When upload is executed for a model (automatically using model policy or manually using an operational rule), the module checks this value. If it is disabled, all events up to the current date are not be uploaded. This prevents huge amounts of events to be uploaded on activation.

Event Manager Module Setup

This step defines the configuration settings of the Event Manager module on the local clients

Parameter	Description
Upload Events	Specifies if events are uploaded from the client to the master database.

File Store Module Setup

This step modifies the default settings for the parameters of the File Store module.

Parameter	Description
Archive Type	Defines the type of archive to use for packing the files for upload.
Concatenation Mode	Defines if the file concatenation mode is active for the upload and if yes which one is used. Automatic concatenation means that all files to be uploaded are packed into one archive file and uploaded, manual concatenation indicates that all files are packed to be uploaded as in automatic with the exception of those specified in the **Excluded File Types** parameter which are uploaded separately.

Parameter	Description
Enable Dialup Downloads	Specifies if downloads are authorized via a RAS (Remote Access Service) connection (Windows devices only). If the value is set to false, then if a dialup connection is detected, the FileStore does not download any information such as inventory. It still receives information about files being available on its relay but it does not make any attempts to download them. Note that on a system which has a LAN connection AND a Dialup connection active at the same time, the module considers itself in dialup mode and behave as described above.
Enable Dialup Uploads	Specifies if uploads are authorized via a RAS (Remote Access Service) connection (Windows devices only). If the value is set to false, then, if a dialup connection is detected, the FileStore does not upload any information such as inventory. It is still receiving information about files being available on its relay but it does not make any attempts to download them. Note that on a system which has a LAN connection AND a Dialup connection active at the same time, the module considers itself in dialup mode and behave as described above.
Excluded File Types	This field is only required for manual concatenation and lists all types, separated with a comma (,), which are to be uploaded separately.
Check for Available Free Space before Downloading a Package	Check this box if the agent is to verify if there is enough disk space available before actually downloading the package. If not enough space is available an error is logged.
Frame Size (Bytes)	Defines the frame size of the network type which the device uses for communication. This parameter must only be modified for devices using non-Ethernet networks, such as token ring, frame relays or ATM networks.
Immediate Start of Notification Request Process	Defines if the thread is to be launched without its initial pause.
Max. Size for Package Conservation (MB)	Defines the maximum size that a package may have to be stored in the database in MB. If a package is larger than the indicated value it is stored until no more devices are in its target list and then it is deleted. If all packages are always to be kept and this option is to be deactivated enter 0 into this field.
Maximum Number of Files to Concatenate	Defines the maximum number of files that can be concatenated.
Multicast Transfer Address	Defines the range of multicast IP address. The server scans the address range and then uses the first available address for the multicast. The address range must be within the following range: *238.4.4.1 and 238.4.4.100* .
Multicast Block Size (Bytes)	Defines the rate used for data transfer. The value must be increased as the transfer rate increases. The default value (16384 byte) is the optimum value for a 128Kb/s transfers. The minimum value is 1024, the maximum 65535.
Multicast Differential Retry	Specifies if differential package retry is to be used. If activated only those frames that have not yet been received by the client are re-transferred. The differential retry is recommended for a smaller number of target clients (<50).
Multicast Minimum File Size (Bytes)	The minimum file size for a multicast transfer in bytes.
Multicast Minimum Requests	Specifies the minimum number of answers from target clients before launching a multicast transfer. If the number of answers is below the fixed threshold the file is sent unicast to the targets.
	Defines the multicast port.

Parameter	Description
Multicast Listen Port	
Multicast Retry Number	The number retries to transfer the file. This parameter is reinitialized at each wave of clients.
Multicast Minimum Success Rate (%)	Defines the minimum success rate in percent from which on the transfer is stopped. This parameter is reinitialized at each new wave of clients. To ensure that the retries continue throughout the network as long as possible, this value must be set very high, such as between 85 and 95% per wave of clients.
Multicast Transfer Delay (sec)	The delay in seconds before the notification is sent and before sending multicast data. This delay is based on the network resources as well as on the number of clients waiting for distribution. It allows the clients to demand the file from the relay.
Multicast TTL	The multicast Time To Live, that is, the maximum number of nodes the frames can pass before arriving on the target. Set to 1 for local networks up to 255 for worldwide network. To deploy to a national network 32 nodes should be enough.
Unicast Recovery on Multicast Failure	Defines if unicast recovery is to be done if the multicast delivery fails.
Copy from Repository to File Store	Defines if the package is copied into the FileStore. If the option is deactivated this means that the medium on which the package is stored must be available on the relay until the last target has collected and installed the package.
Package Repository Path	Defines the path to the storage location of referenced packages on the relay, for example, *D:Packages* , *D* being the local CD/DVD or USB drive. It is also possible to list more than one path, each path separated by a comma (,) from the next.
Synchronize Packages at Startup	Check this box if the packages are to be synchronized at every startup of the agent. Package synchronization allows a device to send its current list of packages it is assigned to as well as their checksum. The master compares the checksum and if it is different to its own, it sends the master list of packages to the device. In this case the local agent compares its list of packages assigned to the device with the master list and updates it accordingly by deleting the unassigned packages and adding the newly assigned ones.
Minimum gap between two automatic synchronizations (sec)	Defines the minimum interval in seconds at which the package synchronizations are to be done. This means that if a default synchronization is executed at 23:00 at night and the client is started at 6 am with agent startup synchronization defined, no synchronization is executed until at least 11 am even if the agent is started /restarted before, as the interval is fixed for 12 hours minimum.
Package TTL (days)	Defines the Time To Live in days for package files relative to the last time the respective package was asked for by a client. This option is also applicable to the rollout post install files which are kept as a .zip file on the file store.
Prefer IP Addresses	Determines whether the identification for communication between the agents and with the master is effected via the agents' IP addresses or over their host names. This is to facilitate networking in environments that do not have DNS name resolution in place.
Pull Timeout (sec)	The time to wait in seconds for the pull thread if it did not manage to contact our relay. Note that this timeout is randomised between (value - (value/2)) and (value + (value/2)) to smooth the relay load.
Push Timeout (sec)	The time to wait in seconds for the push thread if it did not manage to contact the relay. Note that this timeout is randomised between (value - (value/2)) and (value + (value/2)) to smooth the relay load.
Queue Delay (sec)	Defines the interval in seconds between each check of the queue of objects to move.

Parameter	Description
Request for Notifications Interval	Defines the interval in seconds which may elapse without communication from the relay after which the client re-activates its RequestThread to inquire for new notifications from the relay. After the first received notification, the thread is deactivated.
Timeout (sec)	The time to wait in seconds before a file transmission which has failed may be resent.
Threshold for Downloads (bit /sec)	Determines whether downstream transfers are blocked if a connection (whatever its type) is too slow. The thresholds must be indicated in bits/s such that 10000000 means 10Mbits/s.
Threshold for Uploads (bit/sec)	Determines whether upstream transfers are blocked if a connection (whatever its type) is too slow, 0 means no restriction is imposed on interface speed. The thresholds must be indicated in bits/s.
Time to Live (sec)	In order to prevent non-transferable data from remaining eternally in the queue, each object is assigned a specific time that it may stay in the queue and wait to be passed on its way to its destination. This Time To Live (TTL) for each object in seconds is displayed in this field.
Trusted Address	Defines a number of IP addresses from which the local agent is to accept communication in addition to its relay. This allow NAT and VPN communication to work within in the network and the BCM agent, as it recognizes VPN addresses also. Trusted addresses may be entered as single IP addresses or in form of address ranges: • Dotted notation, for example, *94.24.127.24* or *2001:db8:85a3::8a2e:370:7334* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24,2001:db8:85a3::8a2e:370:7334,scotty.enterprise.com* .Several ranges must be separated by a comma (,) or a semi colon (;).

Hardware Filter Synchronisation

This step sends the list hardware inventory filters to the respective devices to be synchronized with the database content.

No parameters need to be defined for this step.

Hardware Inventory Module Setup

This step modifies the default settings of the parameters of the Hardware Inventory module.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Configuration File	Defines the path of the hardware inventory configuration file. The path is relative to the agent configuration file. You may modify the entry, but be aware that if you wrongly modify the inventory may no longer work.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.

Parameter	Description
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Identity Module Setup

This step modifies the default settings for the parameters of the Identity module.

Parameter	Description
Check Identity Time (sec)	Defines the interval in seconds at which the device's identity is verified via its IP address and GUID.
Launch Script if IP Address Changes to 127.0.0.1	Defines if the script is also to be executed for the 127.0.0.1 address.
Execute Script on Changed IP	Check this box to execute a specific script when the agent is launched for the first time and every time the IP address of the agent's device is changed.
Short Identity Time (sec)	A special short timer which is setup and executed once after startup to make sure each object is registered in the database right away. This timer can be disabled by setting it to 0.
Identity Time (sec)	Defines how often a device is to send its identity up to its parent relay.
User Time To Live (h)	Defines the time to live of the user record in hours. Every detected user entry with a detection time older than this threshold is removed.
Primary User Period (h)	Indicates the period in hours to use for computing the primary user.

Load/Unload Module

This step unloads and reloads modules that are required for the correct functioning of the agent, such as Identity and File Store. You need to make sure that these modules are immediately reloaded after being unloaded, otherwise the BCM agent will stop working.

Modules in Client Management are responsible for a certain functionality in the product. This step loads and activates or unloads specific modules at agent startup. Only one module can be loaded per step.

Parameter	Description
Activate	Defines if the module is to be directly activated at agent startup.
Module Name	Select the name of the module to be loaded.
Persistent	Check this box if the module is to be loaded at every startup. If this option is not checked it is only loaded once after the execution of the step.

Logging Configuration

This step configures the default parameters for agent logging for all log files.

Parameter	Description
Output File	Defines the path to the log file relative to the installation directory: • **none** : There is no debugger output regardless of the other settings. • **stdout -sa -cw** : The debugging output is sent to the standard output. • **file** : The debugging output is written to a file whose name is to be specified in this field with a path relative to the agent installation directory, for example, *../../logs/namp.log* for a file located on the same level as the installation directory, not below.
List to Load First	Defines if the debugging is executed according to the principle of everything being disabled with some exceptions or everything being enabled with some exceptions. This system is defined through two lists, the **Disable List** and **Enable List** , which are explained following.
Enable List	A comma separated sequence of message filter names which are to be output to the log file. The special character * means all possible values, an empty string disables the list.
Disable List	A comma separated sequence of message filter names which are to be filtered from going to the log file. The special character * means all possible values. By default the disable list is applied AFTER the enable list and so has a higher precedence.
Displayed Types	A comma separated list of debug message types which are to be output to the log file. The special character * means all possible values.
Maximum Agent Log Size (Byte)	The maximum size of the log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified at all, there is no limit check on the size of the file.
Maximum Agent Log File Count	Maximum number of log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Agent Log Clean Start	Defines if the specified log file is to be backed up at each start of the agent. If enabled the log file specified in **Output File** is backed up at agent start time.
Maximum Audit Log File Size (Bytes)	Controls the maximum size of the audit log file in bytes. When the output file size reaches this limit, it is deleted and a new file of the same name created to start again. If the output file is stdout this setting has no effect. If set to 0 or not specified the limit is the value of the **Maximum Agent Log Size** entry.
Maximum Audit Log File Count	Maximum number of audit log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Audit Log Clean Start	Defines if the specified audit log file is to be backed up at each start of the agent.
Time Format	A formatting string used to format the timestamp part of the logged output. This field may however contain any string of characters the administrator deems appropriate and the variables may be ordered in any desired way. The variables this entry may contain are the following: %y for the year part of the timestamp with 4 digits, for example, 2004, %m for the month as its number, for example, 01 for January and 12 for December, %d for the day of the month, %H for the hour indication, %M for the minutes of the hour and %S for the seconds of the minute.

Parameter	Description
Column Separator	The separator character between the columns in the output. If no value is supplied, the output is padded out for readability. If a value is supplied, no text padding is done.
Send alert when an error occured	Check this box if an alert is to be sent to the master when an error is added to the agent log file.

MSI Package Module Setup

This step modifies the parameters of the configuration values of the MSI packages. This step is only applicable to Windows systems.

Parameter	Description
Maximum Number of Retries	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.

Manual File Upload

This step uploads the files awaiting transfer in the file store.

No parameters need to be defined for this step.

Master Information Configuration

This step allows the administrator to modify the master configuration on all agents if the one of the master parameters listed in this step changed, i.e., to update the IP address or the port number of the master.

Be aware that a large part of the functionalities may no longer work, if any of the below entered information is incorrect.

Parameter	Description
Master Port for Console	Enter the new port number of the master to which the console connects. It is recommended to not use the standard communication ports between the agents and the master, for example, *1610* for the console connections to avoid overloading this port.
Master GUID	Enter the new GUID of the master.
Master Name or IP Address	The master name in form of its short or long network name or its IP address in dotted notation.
Master Port	Enter the new port number of the master if it was changed.
Master Port for MyApps	Defines the port number on which the agent is to connect to the master for MyApps. It is recommended to not use the standard communication ports between the agent, master and console, for example, *1610* and *1611* , for MyApps connections to avoid overloading these ports.

Non-intrusive Reboot Mode Configuration

This step allows the administrator to define the settings for a non-intrusive reboot after an operational rule or patch installation reboot request. A non-intrusive reboot groups reboot requests to one reboot at the end instead of individually executing them when they arrive.nObjects in Client Management, such as operational rules of patch jobs or groups, can be executed in parallel or sequentially. Many of these objects require rebooting the device on which they are executed. If there are a number of them executed one after the other, users on these devices may be disrupted quite often for the required reboots. The non-intrusive reboot makes an object wait for a specified amount of time after execution in which another object requiring a reboot could arrive. If this is the case the first object cancels its reboot and waits for the second object to terminate and use that reboot. If no other object arrives during the specified timeframe, the device is rebooted.nWith this step you can define how long the object is to wait for another object to arrive as well as the total number of reboots per day. In this case, if this value is set to 2 and these two reboots have already happened and another object requiring a reboot arrives, the object is run, but its reboot has to wait until the next day.

Parameter	Description
Non-intrusive Reboot Mode	Check this box if the reboot requested by an operational rule or a patch installations is to be effected in a non-intrusive way. If activated, any rule or patch waits after its execution for a specified amount of time for another object to arrive to combine their required reboot requests into one. If no other rule or patch arrives, the device is rebooted as defined.
Reboot Interval	Defines the waiting time in seconds that the agent waits after receiving the reboot command and executing it.
Max. Number of Reboots	Specifies the maximum number of times a device can be rebooted per day. The default value is 2 reboots per day, 99 is the maximum number of times a device can be rebooted per day. 0 deactivates this option, that is, the device is not rebooted, even if a patch requests it or it is assigned a reboot window; all reboots must be launched manually.
Synchronize at Startup	Check this box if the reboot windows are to be synchronized at every startup of the agent. Reboot window synchronization allows a device to send its current list of reboot windows it is assigned to as well as their checksum. The master compares the checksum and, if it is different to its own, it sends the master list of reboot windows to the device. In this case the local agent compares its list of reboot windows assigned to the device with the master list and updates it accordingly by deleting the unassigned reboot windows and adding the newly assigned ones.
Additional Automatic Synchronization Hour	Enter here the hour at which an additional reboot window synchronization is to be effected, that is, the comparison of locally available reboot window with the reboot window master list. The format is 24-hour format, for example, *23* for *11 pm* .
Minimum Gap between Two Automatic Synchronizations (sec)	Defines the minimum interval in seconds at which the reboot window synchronizations are to be done. This means that if a default synchronization is executed at 23:00 at night and the client is started at 6 am with agent startup synchronization defined, no synchronization is executed until at least 11 am even if the agent is started/restarted before, as the interval is fixed for 12 hours minimum.

Operational Rule Module Setup

This step allows the administrator to modify the parameters of the operational rules module.

Parameter	Description
Automatic Status Upload	Defines if the current status of the operational rule is automatically updated. If the option is deactivated, no status value is updated, however status actualization may still be done via the **Update Operational Rule** step or via an operational rule synchronization.
Failed to check the chronological dependencies if the rule execution is failed	Check this box if an operational rule that depends on another rule is not executed if the rule it depends on does not have the status *Executed OK* . If this option is not activated, the depending rule is executed even if the first rule's execution failed.
Delete Package after Successful Distribution	Check this option, to delete the package on the client (to free up disk space) once the software distribution has executed successfully.
Recreate Local Database If Integrity Check Fails	Defines the actions to be executed if the database check fails at agent startup due to its corruption. If activated the local database is recreated and the master reassigns all operational rules for the concerned devices, depending on the settings defined in the system variables (Automatic reassignment of all general operational rules if the local database is corrupted and Automatic reassignment of all software distribution rules if the local database is corrupted). Otherwise the database is not recreated and the master does not perform any action. If this case occurs the module is executed in suspend mode, which means amongst others that no status values is updated anymore and no synchronizations be performed.
Activate Operational Rule Publication for Users	Defines if rules may be published to users. If activated, the module checks on the master if rules are available to be published to a user, otherwise rules are not published.
Output File	Defines the path to the log file relative to the installation directory: • **none** : There is no debugger output regardless of the other settings. • **stdout -sa -cw** : The debugging output is sent to the standard output. • **file** : The debugging output is written to a file whose name is to be specified in this field with a path relative to the agent installation directory, for example, *../../logs/bcm.log* for a file located on the same level as the installation directory, not below.
Maximum Log File Count	Maximum number of log file backups to keep. As a log file hits its maximum size it is copied to a backup file with an incrementing integer index. When the number of backups hits this limit, backup number 1 is removed and all the others are renumbered down.
Maximum Log File Size (bytes)	Defines the maximum size of the log file in bytes.
Enable Simultaneous Rule Execution	Defines if operational rules may be executed in parallel mode.
Resume Rule Execution at Startup	Defines if any not terminated operational rule is to be continued after a restart of the client.
Status Interval (sec)	The interval in seconds at which the status values of the operational rules are updated. Any file which has is not yet in transfer is requested again.

Parameter	Description
Check for Added Rules	Check this box to check for new rules in the base.
Synchronize at Startup	Check this box if the operational rules are to be synchronized at every startup of the agent. Operational rule synchronization allows a device to send its current list of operational rules it is assigned to as well as their checksum. The master compares the checksum and, if it is different to its own, it sends the master list of operational rules to the device. In this case the local agent compares its list of operational rules assigned to the device with the master list and updates it accordingly by deleting the unassigned operational rules and adding the newly assigned ones.
Check for Deleted Rules	Check this box to check for deleted rules in the base.
Minimum Gap between Two Automatic Synchronizations (sec)	Defines the minimum interval at which the synchronizations are to be done. This means that if a default synchronization is executed at 23:00 with a minimum interval of 12 hours and the client is started at 6 am with agent startup synchronization defined, no synchronization is executed until at least 11:00 am even if the agent is started/restarted before.
Only Check for Not Received Rules	Check this box if only those rules are to be synchronized, for which the assignment was sent but after 12 hours still was not received by the local agent.
Check for Operational Rules	Check this box to check only for operational rules in the database.
Check for Software Distribution Rules	Check this box to check for distribution rules only in the database.
Check for Published Rules	Check this box to check for published rules in the database.
Additional Automatic Synchronization Hour	Enter here the hour at which an additional synchronization is to be effected, that is, the comparison of locally available operational rules with the operational rules master list. The format is 24-hour format, for example, *23* for *11 pm* .
Check for Updated Rules	Check this box to check for updated rules in the base.

Package Synchronization

When the client receives a synchronization request it sends back the list of its own packages linked to a checksum. The master then creates an up-to-date list of the device's packages and checks these with the list it received. If a package on the list from the device does not exist any more, the master sends an order to the device to delete it; if a more recent version exists on the master i.e., the checksums on the master and the client are not identical, an update order will be sent to the device; and if a package is absent on the client but present on the master, then an assign order will be sent to the client device. Any packages which is 'paused' will not be taken into account.

This step synchronizes the packages on the managed devices and the master to make sure none of them got lost.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Patch Management Module Setup

This step modifies the default settings of the parameters of the Patch Management module.

Parameter	Description
Archive Type	Defines if the patch packages are to be of type zip or pkg.
Block Patch Installation	Check this box to prepare the patch installation on all targets of the group for execution, without launching the installation itself.
Knowledge Base Update Delay from Parent (sec)	Defines the interval in seconds between the automatic update of the Knowledge Base on all BCM devices apart from the master. If the value is set to 0, the automatic update functionality is deactivated. To update the local Knowledge Base at the defined interval the clients asks its direct parent if a newer version is available and, if yes, requests its download.
Knowledge Base Internet Download Delay (sec)	Defines the delay in seconds at which the Knowledge Base is automatically downloaded and updated to a Patch Manager. This value is only applicable to the Patch Manager, for all other devices this value should be set to 0 to deactivate the option. The Knowledge Base is only downloaded if it is of a newer version than the version currently available on the Patch Manager or if the **Force Parse** parameter is activated.
Update Knowledge Base at Startup	Defines if the local agent verifies with the master if its Knowledge Base is up-to-date at agent startup and, if this is not the case, downloads it.
Interval Before Patch Inventory Update (sec)	Defines the delay in seconds to wait for a possible update to arrive before any operations, such as a patch inventory or a patch installation, are executed.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Download Retry Interval (sec)	Defines the interval in seconds between each retry for the patch download.
Download Retry Count	Specifies the number of retries for a patch download.
Path for Local Patch Repository	Indicates a local path which the patch module checks if the patch to be downloaded is already available locally there before actually downloading it from the Internet.
Patch Process Interval (sec)	Manages the patch module thread execution, defining the interval in seconds at which requests on the database are executed.
Patch Time To Live (sec)	Defines the Time To Live in seconds for patch package files relative to the last time the respective package was asked for by a client. If the value is set to 0 the option is deactivated, that is, the patch packages are never deleted.
Upload New Inventory if New Version is Detected	If a new version of the Knowledge Base is detected on the Patch Manager, it automatically launches a new patch inventory scan via the respective operational rule and uploads the results.
	Defines if the device is scanned for the current patch situation at agent startup.

Parameter	Description
Scan Machine On Startup	
Archiving of Downloaded Patches after Publication	Defines if the patches are stored in the **download** directory of the Patch Manager after the patch custom package was created and successfully published to the Master. If the option **Move** is selected, you need to fill in the following field **Path for Local Patch Repository** which defines the path to the local storage location.
Synchronize at Startup	Check this box if the patches are to be synchronized at every startup of the agent. Patch synchronization allows a device to send its current list of patch groups it is assigned to as well as their checksum. The master compares the checksum and if it is different to its own, it sends the master list of patch groups to the device. In this case the local agent compares its list of patch groups assigned to the device with the master list and updates it accordingly by deleting the unassigned patch groups and adding the newly assigned ones.
Minimum Gap between Two Automatic Synchronizations (sec)	Defines the minimum interval in seconds at which the patch synchronizations are to be done. This means that if a default synchronization is executed at 23:00 at night and the client is started at 6 am with agent startup synchronization defined, no synchronization is executed until at least 11 am even if the agent is started /restarted before, as the interval is fixed for 12 hours minimum.
Additional Automatic Synchronization Hour	Enter here the hour at which an additional patch synchronization is to be effected, that is, the comparison of available patches with the patch master list. The format for this entry is 24-hour time format, for example, *23* for *11 pm* .
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload Installed Patches	Check this box to also upload the list of patches and service packs that are already installed on the device.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.
Patch Installation Timeout (sec)	The maximum time in seconds that a patch has to install on the target. If the patch has not finished its installation within the defined timeframe its installation is aborted. The patch is then added at the end of the list of all patches to install and retry installing after all others at the next patch installation process.

Patch Synchronization

Clients that are members of patch groups receive a list containing all the patches they will receive for installation. This step allows the master to verify that all clients have the most up-to-date list and if this is not the case, to update it.

No parameters need to be defined for this step.

Power Management Module Setup

This step modifies the parameters of the Power Management module.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Log Events	Specifies if the events that are generated are to be logged on the local database.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Reboot Window Synchronization

This step synchronizes the reboot windows on the managed devices and the master to make sure none of them got lost.

No parameters need to be defined for this step.

RPM Package Module Setup

This step modifies the parameters of the configuration values of the RPM packages.

Parameter	Description
Maximum Number of Retries	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Archive File Extension	Defines the type of extension for the package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.
Retry Interval (sec)	The retry interval defines the interval at which the step is to effect its retries in seconds.

Relay Module Setup

This step modifies the default settings for the parameters of the Relay module.

Parameter	Description
Is Enabled	Defines if the current device is a relay. If the relay functionality is deactivated the device is only a simple client.
Parent Name	

Parameter	Description
	The name of the direct parent to which the target device is to be connected. This is either the master or the new device's relay on the next higher level. The name may be entered as the short or long network name, that is, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, that is, *192.168.1.1* or *2001:db8:85a3::8a2e:370:7334* . You may also select the parent from the list of available devices by clicking the **Add Device** icon and selecting the desired parent from the appearing list.
Parent Port	The port number of the relay of the currently selected remote device on the next higher level.
Tunnel to Parent	Defines if the agent creates and maintains a tunnel with its parent. Be aware that **Auto Detection** has a slight impact on the performance. Use **Yes** if the network configuration is such that the relay cannot directly connect to its clients.
Tunnel Compression Level	Defines compression level to use when building a tunnel to the parent, the possible values range from 0 to 9, 0 meaning no compression and 9 the highest compression.
Child IP Address Range	The IP address range in which the children below the currently selected device may be found if it is enabled as a relay. If a client outside the IP range specified here, tries to define this device as its relay, it is rejected. The addresses may be entered as single IP addresses or in form of address ranges: • Dotted notation, for example, *94.24.127.0-94.24.127.24 - 2001:db8:85a3::8a2e:370:152-2001:db8:85a3::8a2e:370:896* , or *94.24.127.0-24 - 2001:db8:85a3::8a2e:370:152-896* or *94.24.127.0/24 - 2001:db8:85a3::8a2e:370:152/896* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24, 2001:db8:85a3::8a2e:370:152, scotty.enterprise.com* .Several ranges must be separated by a comma (,).
Rejected Relays	Defines a list of clients, which are NOT to be used as a relay for other clients, such as the master server or other specific devices. The devices may be listed with their short or long network names, such as *scotty* or *scotty.enterprise.com* or their IP address in dotted notation. The field may also contain a range of devices in the form of *192.1.1.1-192.1.1.4,2001:db8:85a3::8a2e:370:152-896,kirk,scotty* or *192.1.1.1-kirk* or *kirk-scotty* .
Auto-select Enabled	Defines if the device is set to check automatically for its parent relay.
Parent Selection Retry Interval (sec)	The number displays the interval in seconds at which the client tries to locate the parent relay it belongs to. This parameter is used in two cases: If the parameter **Auto-Select Enabled** is active and if a backup relay has been set.
Reselection Interval (sec)	Defines the interval in seconds between attempts at selecting a 'better' parent than the current one. This selection is done even if the current parent is contactable. This option is disabled if the value is set to 0 or if currently no parent is connected.
List of Backup Relays	A list of backup parents to be scanned if during the auto selection no suitable parent is found through AutoDiscovery. The format is *host1:port1,host2:port2,* etc. *Host 1* is the closest alternative to the regular relay and the last host listed is typically the master. The host name can be entered either as its long or short network name, for example, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, for example, *192.168.56.4* or *2001:db8:85a3::8a2e:370:7334* . If the port number is not listed the default port *1610* is assumed.
	Allows to execute a specific Chilli script every time when a connection is established with a backup relay. Enter here the absolute path to the Chilli script.

Parameter	Description
Execute Script at Connection to Backup Relay	
Execute Script at Disconnection from Backup Relay	Allows to execute a specific Chilli script every time when the connection with a backup relay is terminated. Enter here the absolute path to the Chilli script.
Parent Verification Retry Count	The number of times a device tries to contact the device defined as its parent, if the contact cannot be established at the first try. If after this count the contact still cannot be established the agent moves on to the selecion mechanisms defined by the **Sequence** parameter.
Interval between Verification Retries (sec)	The time interval in seconds between each try to contact the parent.
Bandwidth Check Port	Specifies the port number on which the bandwidth is calculated, which is available to the device for downloads from the relay.
Bandwidth Check Frequency (sec)	The delay in seconds between two calculation phase.
Bandwidth Check Duration (ms)	The calculation phase's duration in milli-seconds.
Client Check Frequency (sec)	Defines the interval at which the device verifies with the relay how many devices are currently downloading from the relay in seconds. If set to 0 the client check is disabled.
Share Point Path for Network Install	The path to the network installation point for custom packages. You may define the path as a UNC path with the following syntax: *UNC[IPAddress][CustomFiles]* , whereby *[IPAddress]* is the remote device and *[CustomFiles]* the remote network share. When using an UNC path the **Administrator Login** and **Password** must be specified as they is used to perform a **Run As** on the machine. If the agent is running under a *LocalSystem* account, this option does not work because this account cannot access network shares.
Share Point Name for Network Install	The path to the network installation point for custom packages. You may define the path as a UNC path with the following syntax: *UNC<IPAddress><CustomFiles>* , whereby <IPAddress> is the remote device and <CustomFiles> the remote network share. When using an UNC path the administrator login and password must be specified as they is used to perform a **Run As** on the machine. This option does not work if the agent is running under a LocalSystem account that cannot access network shares.
Share Point Path for Administrative or Network Install	The path to the administrative installation point for MSI packages. You may define the path as a UNC path with the following syntax: *UNC<IPAddress><MsiFiles>* , whereby <IPAddress> is the remote device and <MsiFiles> the remote network share. When using an UNC path the administrator login and password must be specified as they is used to perform a RunAs on the machine. This option does not work if the agent is running under a LocalSystem account that cannot access network shares. If you are using IPv6 addresses you must use the following format: *FD43-0-0-0-8C84-4BAD-D413-DD68.ipv6-literal.net* .
	The name of the administrative installation point for MSI packages.

Parameter	Description
Share Point Name for Administrative or Network Install	
Administrator Login for Administrative /Network Installation	The login name of the device's administrator who has all necessary access rights to log on to remote devices.
Administrator Password for Administrative /Network Installation	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
Short Storage Path	Defines if the short or the long storage path for the network and administrative installation is used on the relay. By default this option is set to false (0), meaning the package is stored under the location *<RelativePath> /<PackageName.msi>/checksum* , whereby <RelativePath> represents the directory structure in the Console under which the package was created. If activated, the package is stored directly under the <RelativePath> directory and a checksum subdirectory is created containing the *installpackage.zip* file.
Automatically Install Package on Network Share	Defines if the packages are installed on the relay via an administrative and/or network install. At module startup, the relay performs a check on the disk to look for packages that are to be installed on the network share: • **None** : The relay only stores the packages but not install them. • **Administrative** : The respective MSI packages is put on the share as defined in the **Share Point Name for Administrative Install** parameter and installed on their destination. • **Network** : The respective packages (MSI and custom) is put on the share as indicated in the **Share Point Path for Network Install** parameter and installed on their destination if they are MSI packages. • **All** : Both network and administrative packages is put on the shares as defined by the **Share Point Path** parameters above and installed on their destination if they are MSI packages.

Remote Control Module Setup

This step modifies the default Remote Control module parameters.

Parameter	Description
Activate Connection Logging	Defines if administrator connections are to be logged.
Hour(s)	The number of hours of inactivity after which the connection is automatically terminated. This value is mandatory if the **Automatic Disconnection** parameter is activated.
Minute(s)	The number of minutes of inactivity after which the connection is automatically terminated. This value is mandatory if the **Automatic Disconnection** parameter is activated.
Second(s)	

Parameter	Description
	The number of seconds of inactivity after which the connection is automatically terminated. This value is mandatory if the **Automatic Disconnection** parameter is activated.
Automatic Disconnection	Specifies automatic disconnection, that is, if the Remote Control is left inactive for a given period of time, the administrator is automatically disconnected.
Activate Remote Control Information in the Log	Defines if logging is enabled, If it is activated, logging is enabled in the agent log file, mtxagent.log.
Host IP Address	Specifies the listen address of the remote control server. This parameter is useful if the target device of the remote control has several network interfaces and the server should only listen on one specific address (Manual address mode). If it is set to *&&auto* (Automatic detection mode) the server listens on the address 0.0.0.0, which means it is reachable on all its active network interfaces. Be aware that the modification of this parameter requires an agent reboot to be taken into account.
Activate Detailed Logging	Defines the detail level of remote control logging. If activated, logging takes places with maximum information.
Dialog Port	The port at which the local client listens for incoming remote control calls and on which the connection is established.
Install and use the Client Management video driver	Defines if the BMC video driver is to be installed during the rollout to be available for use at remote control connections. Using this driver allows you for example to view the remote cursor and its movements on your screen. If this option is activated it is recommended to reboot the device.

Restart Agent

This step restarts the agent on a local device. It may be used, for example, to start an agent upgrade, which is launched at agent startup, at a specific date and time. The daemon atd must be running on Linux devices for this step to work.

Parameter	Description
Service Name (Windows only)	Defines the name of the service to be managed.
Stored Service Name (Windows only)	If this box checked, the agent is restarted with the name specified at the installation.

Rollout Module Setup

This step modifies the configuration parameters of the rollout module.

Parameter	Description
Max. Number of Simultaneous Devices	The number of devices a rollout can install at the same time.

Rule Synchronization

This step synchronizes the operational rules on the managed devices and the master to make sure none of them got lost.

When the client receives a synchronization request it sends back the list of its own operational rules linked to a checksum. The master then creates an up-to-date list of the device's operational rules and checks these with the received list. If an operational rule on the list from the device does not exist any more, the master sends an order to the device to delete it; if a more recent version of an operational rule exists on the master,that is, the checksums on the master and the client are not identical, an update order is sent to the device; and if a rule is absent on the client but present on the master, then an assignment order is sent to the client device. Any rule which is "paused" is not taken into account. Published operational rules that were already executed, are newly published, but not automatically executed.

Parameter	Description
Proceed with Added Rules	Check this box to check for new rules in the base.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Proceed with Deleted Rules	Check this box to check for deleted rules in the base.
Proceed with Operational Rules	Check this box to check only for operational rules in the database.
Proceed with Published Rules	Check this box to check for published rules in the database.
Proceed with Software Distribution Rules	Check this box to check only for distribution rules in the database.
Only Check for Not Received Rules	Check this box, if only rules for which the assignment has been sent but after 12 hours still have not been received by the local agent.
Check for Software Distribution Rules	Check this box to check only for distribution rules in the database.
Check for Quick Link Rules	Check this box to check only for Quick Link rules in the database.
Proceed with Updated Rules	Check this box to check for updated rules in the base.

Security Configuration

This step configures the default parameters for secure communication between the agents.

Parameter	Description
Authority Certificate	

Parameter	Description
	The authority certificate (CA Cert) to be used for signing the agent certificate if required. By default, the Numara CA is used unless a different CA Cert is configured. The parameter expects a certificate name (without extension) registered in the agent cert store (auth section), such as *Numara_ca* . This parameter is used on the server side and can also be used on the client side if the server is configured to authenticate the client.
Trusted Authorities	A comma separated list of certificates to be trusted when connecting to a secured server or client. By default, the agent trusts the default Numara CA unless a different list of certificates is configured. The parameter expects a list of certificate names (without extension) registered in the agent cert store (trusted section), for example, *Numara_ca, enterprise_ca, startfleet_ca* . This parameter is used on the client side as well as on the server, for the device to know if it can trust the answering device by comparing its certificate with the list of trusted certificates, if it does not match the authority certificate.
User Certificate	The user defined final certificate to be used for both the client and server roles. When this parameter is configured the agent ignores any other authority except the ones to be trusted. The parameter expects a certificate name (without extension) registered in the agent certificate store (user section), for example, *Numara, enterprise, starfleet* .
Access Control	Defines the security when agents communicate with each other, that is, if the Precision Access Control (PAC) handshake is to be used for inter-agent communication: • **No** : as a server, allow PAC connections with client authentication as well as non PAC connections. As client, no PAC connections are required. • **Securised Send, Receive Both** : as server, allow PAC connections with client authentication as well as non PAC connections. As client, only allow PAC connections. • **Yes** : Only allow PAC connections (as server or client). • **Yes with mutual authentication** : Only allow PAC connections (as server or client) with mutual authentication.
Secure Communication	Defines if the agent communicates in secure format. The possible values are: • **No** : With this option the agent accepts both securized and non- securized communication, however it sends only non- securized communications. • **Securized Send, Receive Both** : This value indicates that the agent accepts both securized and non-securized communication, however it sends only securized communications. • **Yes** : When this option is selected the agent only communicates in secure mode, that is, it only receives and sends securized communication.Yes with mutual authentication: With this option the agents communicate in secure mode and in addition authenticate each other via SSL.

SCAP Compliance Module Setup

This step allows to modify the default settings of the parameters of the SCAP Compliance Module.

Parameter	Description
OVAL Directives	This parameter defines the OVAL directives that must be applied to OVAL results. This has an impact on the level of detail for generated XML result files which are temporary files emitted during the scans.

Security Settings Inventory Module Setup

This step modifies the default settings of the parameters of the Security Settings Inventory module.

Parameter	Description
Data File	Specifies the location and name of the security settings inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/SecurityInventory.xml_ .
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Security Products Management Module Setup

This step modifies the default settings for the parameters of the Security Products Management module.

Parameter	Description
Data File	Specifies the location and name of the security products inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the security products inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/securityproductsinventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the security products inventory may not longer work.
Upload Interval (sec)	Defines the upload period for the autodiscovered list in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload on Startup	Defines if the custom inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Additional Anti-Virus Data	Check this box to collect advanced data on installed anti-virus software products (virus definition file date, etc.) and upload them to the Security Products Inventory.
Additional Firewall Data	Check this box to collect advanced data on installed firewall software products (firewall status) and upload them to the Security Products Inventory.
Additional Anti-Spyware Data	Check this box to collect advanced data on installed anti-spyware software products (anti-spyware definition file date, etc.) and upload them to the Security Products Inventory.
Additional Browsers Data	Check this box to collect advanced data on installed browser software products (CERT compliance, etc.) and upload them to the Security Products Inventory.

Selfhealing Module Setup

This step modifies the default settings of the parameter of the Selfhealing module. This functionality is only applicable to Windows and Linux devices.

Parameter	Description
Verification Interval (sec)	Defines the interval in seconds at which the protected applications are verified for their integrity on the local client.

Snapshot Package Module Setup

This step modifies the parameters of the configuration values of the snapshot packages.

Parameter	Description
Maximum Number of Retries	Defines the number of times the publishing process is repeated after a failure before the whole process is declared failed.
Archive File Extension	Defines the type of extension for the package to be created. Be aware that this extension is valid for all packages which are created. If you modify the extension after having created a number of packages already the packager does not recognize the packages with the old extension any more.
Retry Interval (sec)	The retry interval defines the interval at which the step is to effect its retries in seconds.

Software Filter Synchronisation

This step sends the list software inventory filters to the respective devices to be synchronized with the database content.

No parameters need to be defined for this step.

Software Inventory Module Setup

This step allows you to modify the default settings of the parameters of the Software Inventory module.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Scanned Extensions	Defines the file types by their extension, which are included in the software directory scan.
Scan Add /Remove Programs	Check or uncheck this box to define if registry entries for the Add/Remove Programs are to be scanned and added for the software inventory update. Be aware that this only checks for software installed for all users; applications installed for an individual user are not inventoried.
Excluded Directories	Enter the directories which are NOT to be scanned to create the list of installed software applications. The separator character between a list of directories is a comma (,). You can also enter the path to the directories as an environment variable enclosed in ${}.
Scan Hidden Directories	Check or uncheck this box to define if hidden directories are to be scanned for the software inventory update.
Included Directories	If you are only scanning **Scan Add/Remove Programs** but you also want to inventory the applications installed for a user, you must enter here the directory in which they are installed, for example `c:/users` for Windows 7 systems.
Scan MSI Database	Check or uncheck this box to define if the MSI Windows database is to be scanned for the software inventory update.
Configuration File	Defines the .xml format file used to post process the inventory data, which contains an extensive list of software products available for scanning. The path to the file may be entered as a local path or as a URL such as _ ftp://master/swinvcfg.xml_ .
Update Interval (sec)	Defines the update period in seconds for software inventory scans on the remote machines.
Minimum Gap Between Two Uploads (sec)	Defines the minimum time interval between inventory uploads in seconds. If the value is set to 0 this option is deactivated and there is no minimum interval.
Upload Interval (sec)	Defines the upload period for the inventory in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the inventory is uploaded to the master after being updated the first time on agent startup. It is recommended to activate this option to ensure that the inventory is updated at least at every startup of the agent. If it is deactivated a regular update and upload of the inventory must be configured through operational rules.

Timer Module Setup

This step defines the general behavior of the Timer module.

Parameter	Description
Take Logged User into Account	Defines if the connected user is to be taken into account when executing an operational rule. By default the rule is executed when the user, who activated the rule in MyApps, is connected. If another user is connected to the device it is not executed.

Transfer Window Synchronization

When the client receives a synchronization request it sends back the list of its own transfer windows linked to a checksum. The master then creates an up-to-date list of the device's transfer windows and checks these with the list it received. If a transfer window on the list from the device does not exist any more, the master sends an order to the device to delete it; if a more recent version of a transfer window exists on the master i.e., the checksums on the master and the client are not identical, an update order will be sent to the device; and if a transfer window is absent on the client but present on the master, then an assign order will be sent to the client device.

This step synchronizes the transfer windows to which the managed devices are assigned and the master to make sure none of them get lost.

Parameter	Description
Check for New Transfer Windows	Check this box to check for new transfer windows in the base.
Check for Deleted Transfer Windows	Check this box to check for deleted transfer windows in the base.
Check for Updated Transfer Windows	Check this box to check for updated transfer windows in the base.

Upload Operational Rule Status

This step uploads the status of an operational rule. This may be useful when the status has been lost.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

User Access Module Setup

This step allows you to add an entry to or remove it from the list of users of the User Access module.

Parameter	Description
Login	The login name for a specific user or group of users.
Authentication Type	The Authentication Type is related to the login and can be one of the following categories: • **Private** : Should be used if the user is to log on with a proper name, for example, *Scotty, Kirk* , etc. A user logged on in this category is required to give a password which is to be defined below.

Parameter	Description
	• **System** : If this authentication is used the login and password are verified by the system. • **Action** : If an access is defined as Action, its login and password are verified by the call of the specified action.
Password	Passwords depend on **Authentication Type** : • A **Private** user login is required to give a password, then to confirm it. • If the authentication type is defined as **Action** , the name of the action which is to be called and which authenticates the login must be entered into the **Action Name** field. The action defined in this field must exist on the agent to create a valid user login. • A **System** user login does not need any password or other further information. This login is mostly used by system processes.
Action Name	The name of the action which is responsible for processing the authentication. By default this is *V64DbAdminCheckLogin* .
Order	Specifies the order in which the user access is handled. This order is important, as the Http Protocol Handler goes through this list and accepts the first match it finds.
Operation	Select from the drop-down list the type of operation to be executed on the user access defined above, that is, if it is to be added to or removed from the list of valid user accesses.

Virtual Infrastructure Manager Module Setup

Parameter	Description
Local Inventory Check Interval	Defines the interval in seconds between each upload of the inventory of the local virtual machine and its upload to the master.

WakeOnLan Module Setup

This step allows to modify the configuration settings of the Wake on LAN module.

Parameter	Description
List of wake up devices (format: device1: port1, device2: port2)	The comma separated list of devices elected for the wake-up process. In this case, the registered devices are used as static proxies and the module respects the list order (from left to right). There is no deep check concerning the wake-up devices such as IP address and network mask.
Automatic Wake-up Mechanism	Agents have the capability to monitor the data flow and remember the list of devices for which they are the direct relay. Therefore, modules are able to look up possible devices that share a common subnet with another device to wake up. This option enables the capability to look up this dynamic knowledge base and detect the list of possible wake-up devices. This is the dynamic version of the previous option.

Parameter	Description
Fallback Wake-up Mechanism	This fallback parameter allows trying a last wake-up mechanism. It is often used when none of the previous mechanisms have succeeded, or if some of them were disabled. The aim is to proceed to the wake-up using a blind method. When set to **Unicast** the module tries a simple host directed unicast wake-up (a simple UDP packet sent to the exact destination address). When set to **Broadcast** , the module tries a subnet-directed broadcast (a simple UDP packet sent to the entire network). When set to **DirectBroadcast** , the module tries a direct broadcast considering the target network address. When set to **None** , the fallback mechanism is disabled.
Local Wake-up Mechanism	When enabled, the module checks whether the target and itself is part of a common subnet. In that case, the wakeup is performed by the module itself using the subnet broadcast address.

Web Services Module Setup

This step allows you to modify the default settings of the Web API module parameters.

Parameter	Description
Server Port	Defines the TCP port dedicated to the web services.

Windows Device Management Module Setup

This step defines the default settings for managing Windows peripheral devices trying to connect to the managed network devices.

Parameter	Description
Log Events	Specifies if the events that are generated are to be logged on the local database.

Custom Inventory steps

This group contains all steps concerned with the generation of the custom inventory, such as collecting specific data or values from registries or configuration files.

- Collect Environment Variable Value
- Collect Ini File Value
- Collect Registry Key Value
- File Analysis via Regular Expression
- Monitor Manufacturer Information
- Printer Inventory
- Verify File Existence
- Verify File Types

Collect Environment Variable Value

This step allows you to collect the value of system environment variables.

Parameter	Description
Custom Inventory Instance Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Parameter	Description
Environment Variable	Enter the name of the environment variable for which the value is to be recovered, for example, *CLASSPATH* .

Collect Ini File Value

This step collects the value of an entry in a configuration file and stores it in the custom inventory.

Parameter	Description
Custom Inventory Instance Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Entry Type (String or Integer)	Specifies if the value to be recovered is a string or an integer value.
Entry Name	The name of the entry of which the value is to be recovered. Make sure you enter it correctly, including lower and upper case letters, as the entry is case sensitive.
File Path	The complete or relative path to the configuration file. If you enter the path as a relative path it is relative to the *<InstallDir>/Master/config* directory.
Section Name	Enter the name of the section without its enclosing brackets, that is, *Security* for the *[Security]* section of the *mtxagent.ini* file.

Collect Registry Key Value

This step searches the value(s) of specific registry key(s) and integrates them into the custom inventory.

Parameter	Description
Custom Inventory Instance Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Custom Inventory Object Name	The name of the object under which it appears in the Console under the **Custom Inventory** node. If you listed a number of key names in the field above this field must contain the list of value names in the same order as the key names above, separated either by comma (,) or semi-colon (;) as well.
Registry Key	The name of the registry key for which the value is to be found. You may also enter a list of key names in this field separated either by comma (,) or semi-colon (;).
Value Name	The name of the value of this key. If you listed a number of key names in the field above this field must contain the list of value names in the same order as the key names above, separated either by comma (,) or semi-colon (;) as well.
Configuration File	Specifies the location and name of the custom inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/custominventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the custom inventory may not longer work.

File Analysis via Regular Expression

This step finds entries matching a provided regular expression and integrates the data into the custom inventory.

Parameter	Description
List of Attribute Names	Specifies the names of the attributes that are to be stored for the found expression. This is a list of names separated by a semi-colon, for example, *Date;Module;Detail* .
Match Case	Check this box if the string entered in the field above is to be case sensitive, that is, if the searched string is *error* , it finds *error, Error* and *ERROR* .
Delete previous entries of this object	Determines if any possibly existing previous entries of the object are to be erased.
Custom Inventory Object Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Generate Error If Not Found	Defines if an error is generated if no match is found for the regular expression.
Event Description	Enter the text for the event, describing it.
File Path	The complete or relative path to the file. If you enter the path as a relative path it is relative to the *<InstallDir> /Master/config directory* . The file path may use wildcard characters, such as the asterisks (*), for example, *.. /log/mtxagent** to search in all stored log files of the agent for a specific expression.
Maximum number of entries to preserve (0: unlimited)	Defines the number of entries to keep before overwriting them, that is, how may entries the object does have. If for example you are searching for errors of a specific type, and there are 15 of them, only the 10 last ones is stored here.
Regular Expression (PCRE)	Enter the regular expression to be found in the file(s).
Return Complete Line	Defines if the complete line is to be included in the custom inventory or only the part corresponding to the regular expression.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Monitor Manufacturer Information

This step allows you to collect information about the screens connected to a device. The information will be added to the Custom Inventory. It is applicable to Windows only.

Parameter	Description
Custom Inventory Instance Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Screen ID	Check this box if the screen ID is to be read and added to the custom inventory.
Manufacturing Date	Check this box if the manufacturing date of the screen is to be read and added to the custom inventory.
Model Name	Check this box if the model name of the monitor is to be read and added to the custom inventory.
Serial Number	Check this box if the serial number of the monitor is to be read and added to the custom inventory.
VB Script Path	Enter the path to the monitorserial.vbs script file of the target devices into this field.
Version	Check this box if the version number of the screen is to be read and added to the custom inventory.
VESA Manufacturer ID	Check this box if the VESA Manufacturer ID is to read and added to the custom inventory.

Printer Inventory

This step finds all printers within a specified IP address range via SNMP and provides information on them.

Parameter	Description
Address Range	Defines the IP address range in which the printer is to be located. The range may be entered as single IP addresses or in form of address ranges: • Dotted notation, for example, *94.24.127.24* or *2001:db8:85a3::8a2e:370:7334* • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24,2001:db8:85a3::8a2e:370:7334,scotty.enterprise.com* .Several ranges must be separated by a comma (,) or a semi colon ( .
SNMP Read Community	Defines the community string used when sending the SNMP request, for example, *public* .
TCP Retries	Specifies how many retries are executed before the step is declared as failed.
SNMP TCP Port	The port on which the frame is sent.
TCP Timeout (sec)	The timeout in seconds after which the search operation is regarded as failed.

Verify File Existence

This step checks if one or more files exist and returns their full file path(s) which are added to the custom inventory of the respective device(s).

Parameter	Description
Custom Inventory Instance Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Maximum File Date	The date of the file must be this or an earlier date. The date must be entered in the following format: *YYYY/MM /DD HH:MM:SS* .
Minimum File Date	The date of the file must be this value or a later date. The date must be entered in the following format: *YYYY /MM/DD HH:MM:SS* .
File Names	Enter the names of the files, for which you want to verify if they exist. The names are to be listed separated by commas (,).
Maximum File Size (KB)	The maximum size that the file can have in KB.
Minimum File Size (KB)	The size that the file must have at least in KB.
Directory List	Enter here the directories in which to search for the listed files types. The path may be defined as the relative or absolute local path. If the file is located on a network drive map the network resource to a "local" letter before entering the path. If the parameter is left empty, the path is either / or the first valid drive letter found, for example, *c:* .
Include Subdirectories	Check this box if the subdirectories of the above listed directories are to be searched as well.

Verify File Types

This step allows you to verify the presence of one or more file types and to return their number as well as the disk space used by each of them. This information is added to the custom inventory of the respective device(s).

Parameter	Description
File Extensions	Enter the list of file types for which to check, in the format of *exe,bat,ini,txt* .
Directory List	Enter here the directories in which to search for the listed files types. The path may be defined as the relative or absolute local path. If the file is located on a network drive map the network resource to a "local" letter before entering the path.
Include Subdirectories	Check this box if the subdirectories of the above listed directories are to be searched as well.

Directory and File Handling steps

This group of operational rule steps collects all steps which are concerned in any way with the handling of directories and files. It may be split into the following subgroups:

- Directory Handling
- Directory and File Handling

Directory Handling steps

This group of operational rule steps provides the necessary functions for handling the directories on the managed devices in the system. They are used amongst others for the monitoring and prohibiting of applications.

- Create Directory
- Delete Directory
- Backup Directory
- Rename Directory
- Restore Directory

Create Directory

This step creates a new directory at the indicated location.

Parameter	Description
Target Path or URL	Specify the name and relative or absolute path or URL to be created.

Delete Directory

This step deletes a directory on the managed devices.

Parameter	Description
Delete Read-only Files	Check this box to also delete all read-only files which may be located in the directory.
Target Path or URL	Specify the name and relative or absolute path or URL to be deleted.
Only Delete Directory Content	Check this box to only delete the directory content. The directory is not deleted.

Backup Directory

This step creates a backup of an existing directory and all its content including all subdirectories in another directory. It may also be used to copy/duplicate a directory and all its contents at another location.

Parameter	Description
Backup Name	Enter a name for the backup to be able to identify the backup. If the directory is simply to be copied enter the target name of the copy, which may be the same as the original.
Backup Path	Specify the path to the directory in which the backup/copy is to be created. If the directory does not yet exist, it is created.
Data Compression	Check this box if the backup is to compress the selected data in the backup file. Do not check this box for directory copying.
Append PC Name to Backup Name	Check this box, if the name of the client is to be added to the backup name. Do not check this box for directory copying.
Append Date to Backup Name	Check this box, if the date and time of the backup is to be added to the backup name. Do not check this box for directory copying.

Parameter	Description
Backup on Relay	Check this box if the contents of the directory are to be backed up on the device?s relay instead of locally on the device itself.
Enable Full Path	Check this box if the contents of the directory are to be backed up with the whole directory structure.
Append Registry Key Name to Backup Name	Check this box, if the registry key name is to be added to the backup name. Do not check this box for directory copying.
Append Registry Key Value Name to Backup Name	Check this box, if the registry key vale name is to be added to the backup name. Do not check this box for directory copying.
Source Path or URL	The name and relative or absolute path or URL of the directory to be backed up or copied.

Rename Directory

The following step renames an existing directory. At the same time you may move the directory to another location.

Parameter	Description
Source Path or URL	Specify the name and relative or absolute path or URL of the source directory.
Target Path or URL	Specify the new name and relative or absolute path or URL of the directory.

Restore Directory

This step restores the contents of a directory, files and subdirectories, that was backed up via the "Backup Directory" step.

Parameter	Description
Appended Device Name	Check this box if the name of the device was added to the backup name.
Appended Backup Date	If the backup of a specific date is to be restored, enter the desired date into this field in the form of YYYYMMDD. Make sure the Last Backup Date box above is not checked in this case.
Target Data Location	Specify the path to which the directory is to be restored. If the directory does not yet exist, it is created.
Backup Name	The name of the backup to be restored.
Appended Registry Key Name	Enter the name of the registry key into this field if it was appended to the backup name.
Appended Registry Value Name	Enter the name of the registry value into this field if it was appended to the backup name.
Backup Path	The name and relative or absolute path or URL to the backed up directory to be restored.
Backup on Relay	Check this box if the contents of the directory to be restored are located on the device?s relay instead of locally on the device itself.
Last Backup Date	Check this box if the latest available backup of this directory is to be restored. If this box is checked the entry in the next field Appended Backup Date is ignored.

File Handling

This group of operational rule steps collects all steps which are concerned in any way with the handling of directories and files. It may be split into the following subgroups:

The steps about file handling are divided into the following subgroups:

- File Handling
- Text File Editing
- INI File Editing

For more information on file manipulation, see File Manipulation.

File Manipulation

File manipulation through steps can be executed on files located on the same and on different disk systems. Depending on the files' location two different ways of accessing these files are provided by the respective functions:

- If the files are located on the same disk system they can be accessed by specifying their full or relative path.
- If the files are non-local files and thus need to be accessed through the network, they must be specified via URLs. The supported protocols for this mode of access are *file, http, ftp* and *smb* (Microsoft LAN Manager).

Syntax for accessing files through URL

URLs (Uniform Resource Locator) are used to find resources (files) on a network, typically the Internet, by providing an abstract identification of the resource location.

In general, URLs are written as follows: <scheme>:<scheme-specific-part>

A URL contains the name of the scheme being used (`<scheme>`), such as *ftp* or *http* , followed by a colon and then a string (the `<scheme-specific-part>`) whose interpretation depends on the scheme. For more information about the general rules of forming URLs, refer to the respective RFC documents, such as RFC 1738, 1034, 1123, and so on. The following topics are the summary compiled from these RFCs:

- File Specific Scheme
- FTP Specific Scheme
- HTTP Specific Scheme
- SMB Specific Scheme

File Specific Scheme

In this case the term *local file* is employed to specify files which are located on the same system. The syntax when specifying a local file is either the full or relative path of the respective file.

Syntax

```
file://<driveletter>/<dir1>/<dir2>/.../<dirN>/<filename>
```

Driveletter	is the letter of the local or mapped drive on which the file is located. This parameter is optional if the path is a relative path.
Dir1 - DirN	list the directory hierarchy to the file. These parameters are optional.
File name	specifies the name of the file to be accessed with its extension.

FTP Specific Scheme

The FTP URL scheme is used to designate files and directories on Internet hosts accessible using the FTP protocol.

Syntax

```
ftp://<user>:<password>@<host>:<port>/<dir1>/<dir2>/.../<dirN>/<filename>;type=<typecode>
```

User	specifies an optional user name.
Password	specifies an optional password to the user name. If present, it follows the user name separated from it by a colon. Be sure to escape the `@` of the email address when accessing an outside server with the anonymous logon, for example: Unsafe characters, such as `&, @` or `:` , should generally be escaped through the general escape scheme: `% digit digit` , for example, `@` is escaped to `%40` , `:` is escaped to `%09` , and so on Also note that an empty user name or password is different than no user name or password; there is no way to specify a password without specifying a user name.
Port	defines the port number to connect to. The default port is 21.
Dir1 - DirN	list the directory hierarchy on the server to the file. These parameters are optional.
File name	specifies the name of the file to be accessed with its extension.
Typecode	defines the mode of transfer for the file depending on the data content type of the file. Valid values are the characters `a, i` or `d` . This parameter (`;type=<typecode>`) is optional.

Example 1

Example for a password login.

```
ftp://myname:hello@lenny/lucky.png
```

Example for an anonymous login with email address as password.

```
ftp://anonymous:myname%40spyinternation.com@lenny/lucky.png/
```

Example 2

The following table shows examples about the use of no or empty user names and password:

ftp://@host.com/	has an empty user name and no password
ftp://host.com/	has no user name
ftp://foo:@host.com/	has a user name of `foo` and an empty password.

Example 3

The following table shows different examples for the use of the Directory and file name parameters.

ftp://myname@host.dom/%2Fetc/motd	is interpreted by FTP-ing to `host.dom` , logging in as myname (prompting for a password if it is asked for), and then executing `CWD /etc` and then `RETR motd` .
ftp://myname@host.dom/etc/motd	would `CWD etc` and then `RETR motd` ; the initial `CWD` might be executed relative to the default directory for `myname` .
ftp://myname@host.dom//etc/motd	would `CWD` with a null argument, then `CWD etc` , and then `RETR motd` .

HTTP Specific Scheme

The HTTP URL scheme is used to designate Internet resources accessible using HTTP (HyperText Transfer Protocol).

Syntax

```
http://<host>:<port>/<path>?<searchpart>
```

Host	specifies the fully qualified domain name of a network host, or its IP address as a set of four decimal digit groups separated by full stop (.).
Port	specifies the port number to connect to. Another port number can optionally be supplied, in decimal, separated from the host by a colon. If the port is not specified, the port defaults to 80.
Path	specifies the path to the file on the host computer. This part is optional. If it is not present, the `/` may also be omitted.
Searchpart	defines the query information. It is a string composed of parameter=value pairs separated by ampersand (`&`) symbols. This part is optional. If it is not present, its preceding ? ? and `/<path>` may also be omitted.

SMB Specific Scheme

Windows clients exchange messages with a server to access resources on that server. These messages are called Server Message Blocks (smb).

Syntax

```
smb://<user>:<password>@<host>:/<share>/<dir1>/<dir2>/.../<dirN>/<filename>
```

User	specifies an optional user name.
Password	specifies an optional password to the user name. If present, it follows the user name separated from it by a colon.
Host	specifies the fully qualified domain name of a network host, or its IP address as the dotted set of four decimal digit groups.
Share	defines the name of the share on the remote server.
Dir1 - DirN	list the directory hierarchy on the server to the file. These parameters are optional.
File name	specifies the name of the file to be accessed with its extension.

Example

```
smb://Administrator:vmCM@192.168.1.228:/Share/Folder/File.txt
```

File Handling steps

File manipulation through steps can be executed on files located on the same as well as on different disk systems. Depending on the files' location, two different ways of accessing these files are provided by the respective functions.

- Copy Files
- Check for File
- Delete File Occurrences
- Move Files
- Check for String in File

Copy Files

This step copies one or more files (via * or ? wildcard characters) into a second file.

Parameter	Description
Source Path or URL	The relative or absolute path, the URL or an environment variable of the existing file to be copied. The name may contain wildcard characters, that is, *and *?* , but in this case the target directory must exist; all files corresponding to the source pattern is copied with their original names to this directory.
Source Access User	Check this box if you need to define a specific login to access the source share with the required access rights. The fields below then become available and you can enter your credentials.
Login with Source Share Read Access	The login name with which to access the source share that has at least read access.
Corresponding Source Password	Enter the corresponding password.
Target Path or URL	Supplies the relative or absolute path, the URL or an environment variable of the file to be created. The supplied parameter may be relative or absolute paths or URLs using the http, ftp, smb or file protocols. If a network protocol URL is used, success or failure is determined by whether the server allows the operation. For non-URL paths, if the destination path exists it is overwritten. Also, for a non-URL path, if any part of the destination path does not exist, it is created. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Destination Access User	Check this box if you need to define a specific login to access the destination share with the required access rights. The fields below then become available and you can enter your credentials.
Login with Destination Share Write Access	The login name with which to access the target share and that has write access to it.
Corresponding Target Password	Enter the corresponding password.

Parameter	Description
Force File Copy	Allows to also copy protected files, that is, if the file to be copied already exists at the target location and is protected. If the option is activated the file is copied to the target, if the option is deactivated the file is not copied.
Allow Partial Execution	If this box is checked, the step executes successfully, even if one of the files matching the filter cannot be processed. In this case, an error is displayed in the Error Details column of the assigned device view. If none of the files matching the filter can be processed, the rule fails.nTo find which files were or were not successfully processed, you need to check the operational rules log (operationalrules.log), if you have activated the "Report Processing Errors" option.
Report Processing Errors	Defines if an entry is to be logged on the OperationalRules.log for files for which the required operation could not be executed.

Check for File

This step checks if a file is present or not.

Parameter	Description
File Name	Enter here the name and directory path of the file of which the existence is to be verified. The file must be defined as the absolute local path. If the file is located on a network drive map the network resource to a "local" letter before entering the path. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* .

Delete Files

This step permanently deletes one or more files (via * or ? wildcard characters).

Parameter	Description
Allow Partial Execution	If this box is checked, the step executes successfully, even if one of the files matching the filter cannot be deleted. In this case, an error is displayed in the Error Details column of the assigned device view. If none of the files matching the filter can be deleted, the rule fails.nTo find which files were or were not successfully deleted, you need to check the operational rules log (operationalrules.log), if you have activated the "Report Processing Errors" option.
File Name	Defines is the relative or absolute path, the URL or an environment variable of the existing file to be deleted. The name may contain wildcard characters, that is, *** and *?* , in this case all files corresponding to the file pattern is permanently deleted. The supplied parameter may be a relative or absolute path or a URL using the http, ftp, smb or file protocols. If a network protocol URL is used, success or failure is determined by whether the server allows the operation. If the file does not exist no error is generated. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Report Processing Errors	Defines if for files that cannot be deleted a entry is to be logged on the OperationalRules.log file.

Delete File Occurrences

This step deletes all occurrences of a file from a root directory downwards (via wildcard characters * or ?).

Parameter	Description
File Name	Enter into this field the file name or a file pattern using the asterisks (*) and question mark wildcard characters., for example, *.ini* or *Config?.log* or *log* . This field is case sensitive.
Include Subdirectories	Check this box if the file occurrences are to be searched not only in the indicated directory but also its subdirectories.
Root Directory	Enter into this field the name of the root directory from which the file is to be searched and deleted.

Move Files

This step renames or moves one or more files (via * or ? wildcard characters) to a new location

Parameter	Description
Allow Partial Execution	If this box is checked, the step executes successfully, even if one of the files matching the filter cannot be processed. In this case, an error is displayed in the Error Details column of the assigned device view. If none of the files matching the filter can be processed, the rule fails.nTo find which files were or were not successfully processed, you need to check the operational rules log (operationalrules.log), if you have activated the "Report Processing Errors" option.
Report Processing Errors	Defines if an entry is to be logged on the OperationalRules.log for files for which the required operation could not be executed.
Source Path or URL	The relative or absolute path, the URL or an environment variable of the existing file to be moved. The name may contain wildcard characters, that is, *** and *?* , but in this case the target directory must exist; all files corresponding to the source pattern is moved with their original names to this directory.
Target Path or URL	The relative or absolute path or the URL of the file to be moved to. The supplied parameter may be a relative or absolute path or a URL using the http, ftp, smb or file protocols. If a network protocol URL is used, success or failure is determined by whether the server allows the operation. In particular a move operation may succeed in creating the destination file but fail to delete the source. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous. For non-URL paths, if the destination path exists it is overwritten. Also, for a non-URL path, if any part of the destination does not exist, it is created.

Check for String in File

This step checks if the given string is in the given file.

Parameter	Description
Match Case	Check this box if the string entered in the field above is case sensitive. If the search operation is not case sensitive, the result for a searched string *enterprise* is: *enterprise, Enterprise* and *ENTERPRISE* .
Error if Found	Check this box if an error is to be raised if the string is found.
File Name	The name and directory path of the file of which the content is to be searched.
Searched String	Enter the string which is to be found in the above listed file.

Text File Editing steps

This group of steps allows you to edit simple text files.

- Insert Line
- Delete Line
- Add Line

Insert Line

This step inserts a single line of text in a text file at any specified place.

Parameter	Description
Position	Defines the number of the line (starting at 1) where the new line is to be inserted.
Line	Contains the entire text string to be added to the file.
Source Path	The relative or absolute path, the URL or an environment variable of the file to which a single line is to be added.

Delete Line

This step deletes any single line from a text file.

Parameter	Description
Position	Defines the number of the line (starting at 1) to be deleted.
Source Path	The relative or absolute path, the URL or an environment variable of the file from which a line is to be deleted.

Add Line

This step adds a single line to the end of a text file.

Parameter	Description
Line	The entire text string to be added to the file. The line is automatically added in either UNIX or DOS format and also add a CRLF at the end.
Source Path	The relative or absolute path, the URL or an environment variable of the file to which a line is to be added.

INI File Editing steps

This group of steps allows you to edit any configuration (.ini) files.

- Update INI File
- Delete Entry
- FTP Backup
- Restore

Update INI File

This step updates or adds an entry in a configuration (.ini) file.

Parameter	Description
Create if it does not exist	If the configuration file does not yet exist check this box to create it in the above defined location.

Parameter	Description
Entry Name	The name of the entry to be modified or added. If the entry does not yet exist it is added. Only the entry name must be entered, the equal sign is added automatically.
Entry Value	Define the new or modified value of the above defined entry.
File Name	Defines the name of the .ini file, which is to be modified. The file may be defined as the relative or absolute local path. If the file is located on a network drive map the network resource to a "local" letter before entering the path.
Section Name	Specifies the name of the section in which an entry is to be modified or added. If the section does not yet exist it is added. The section name corresponds to the value enclosed in brackets ([]) in the ini file, for example, *[SqlUpgrade]* . However, the value must be entered in this field without the brackets.

Delete Entry

This step deletes an entry from a configuration file.

Parameter	Description
Entry Name	The name of the entry to be deleted.
File Name	Defines the name of the .ini file, in which an entry is to be deleted. The file may be defined as the relative or absolute local path. If the file is located on a network drive map the network resource to a "local" letter before entering the path.
Section Name	Specifies the name of the section in which the entry to be deleted is located.

FTP Backup

This step backs up data of a specific directory on the local client and store the backup on another machine.

Parameter	Description
Backup Name	Enter a name for the backup to be able to identify the backup.
Data Compression	Check this box if the backup is to compress the selected data in the backup file.
Append PC Name to Backup Name	Check this box, if the name of the client is to be added to the backup name.
Append Date to Backup Name	Check this box, if the date and time of the backup is to be added to the backup name.
Remote Target Directory	Enter the complete path to the target directory on the remote backup machine, where the backup is to be stored.
FTP Port	Enter the port number on the FTP server which is to be used.
FTP Server Name	Enter the name of the FTP server which is to carry out the data backup. The name may be entered as its short or long network name, that is, *scotty* or *scotty.enterprise.com* or in form of its IP address in dotted notation, for example, *168.192.1.1* or *2001:db8:85a3::8a2e:370:7334* .
FTP Server Login	Enter a valid login to the FTP server that is to be used by the backup.

Parameter	Description
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
Append Registry Key Name to Backup Name	Enter the name of the registry key into this field, if it is to be added to the backup name.
Append Registry Key Value Name to Backup Name	Enter the value name of the registry key into this field, if it is to be added to the backup name.
Local Directory to Back up	Enter the path to the local directory which is to be backed up, such as *C:Programm FilesBMC SoftwareClient Managementmasterconfig* .

Restore

This step provides all necessary information to restore data to the local client which were backed up and stored at another location.

Parameter	Description
Appended Device Name	Check this box if the name of the client was appended to the backup name.
Appended Backup Date	Enter the date that was appended to the name of the backup into this field. It has the form YYYYMMDD.
Target Data Location	Enter the complete path to the target directory on the remote backup machine, where the backup is stored.
Backup Name	Enter the name of the backup to be restored.
Appended Registry Key Name	Enter the name of the registry key if it was appended to the backup name.
Appended Registry Value Name	Enter the name of the registry key value if it was appended to the backup name.
Backup Source Directory	Enter into this field the complete path to the directory of which the contents are to be restored by the backup.
FTP Port	Enter the port number on the FTP server which is to be used.
FTP Server Name	Enter the name of the FTP server which is to carry out the data restoration. The name may be entered as its short or long network name, that is, *scotty* or *scotty.enterprise.com* or in form of its IP address in dotted notation.
FTP Server Login	Enter a valid login to the FTP server that is to be used by the restore operation.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
Last Backup Date	Check this box if the newest backup available is to be used for restoration. In this case do not enter any value in the field below.

Event Log Manager steps

This group of steps provides you with the possibility to manage the event logs of the different event models predefined in Client Management. Thus events regarding a specific model may be activated or deactivated, deleted or uploaded to the master.

Activate Model

This step activates the event recording of a specific event log model through the local agent. All events which are generated for this model will be collected and stored on the local database.

Parameter	Description
Custom Model Name	To activate a custom defined event log model enter its name exactly into this field. The field above becomes inaccessible.
Model Name	The name of the predefined event model that is to be activated.

Deactivate Model

This step deactivates the event recording of a specific event log model. This means that all events generated for this model will be immediately deleted instead of being stored in the database.

Parameter	Description
Custom Model Name	To deactivate a custom defined event log model enter its name exactly into this field. The field above becomes inaccessible.
Model Name	The name of the predefined event model that is to be deactivated.

Delete Events

This step deletes all events stored in the local SQLite database of the agent for a specified event model immediately instead of following the default values defined at event model setup time.

Parameter	Description
Custom Model Name	To delete all events stored for a custom defined event log model enter its name exactly into this field. The field above becomes inaccessible.
Model Name	The name of the predefined event model for which the events are to be deleted.

Upload Events

This step defines an event model where the logged events are to be uploaded to the event log database of the master immediately instead of following the upload time and intervals defined at event model setup time.

Parameter	Description
Custom Model Name	To upload all events stored for a custom defined event log model to the master database enter its name exactly into this field. The field above becomes inaccessible.
Model Name	The name of the predefined event model for which the events are to be immediately uploaded to the master database.

Hardware Inventory steps

This step class contains any type of steps manipulating the contents of the hardware inventory.

- Add WMI Class

Add WMI Class

This step adds a WMI class to the hardware inventory filters and is applicable to Windows only.

Parameter	Description
Action List for Attributes	Contains the list of actions for the above specified properties in the same order, separated with a comma or a semi-colon. Possible values are **ACCEPT** - include the attribute in the inventory and **REJECT** - do not include the attribute in the inventory
List of Attribute Names	Enter here the list of names of class attributes or properties, for example, *PowerManagementSupported* . The individual attributes must be separated with a comma or a semi-colon.
List of Attribute Types	Must contain the list of types for each above listed property, separated with a comma or a semi-colon. This is the type of the attribute value as which it is entered into the database and displayed on the screen. The following values are possible: INTEGER, STRING or ALL.
Class ID	The system name or identification of the WMI class as provided by Microsoft, for example, *Win32_BaseBoard* for the above name of class name *Base Board* . There can only be a single **Class ID** within each **WMI class** .
Class Name	The name of the WMI class, for example, *Base Board* .

Inventory Management steps

This group contains all steps concerned with inventory management, such as the upload or update of any type of inventory.

- Clean Custom Inventory
- Clean Security Settings Inventory
- Update Custom Inventory
- Update CustomInventory.xml File
- Update Hardware Inventory
- Update Security Settings Inventory
- Update Security Products Inventory
- Update Software Inventory
- Update and Upload the Local Virtual Infrastructure Inventory

- Upload Agent Identity
- Upload Asset Discovery Results
- Upload AutoDiscovery List
- Upload Custom Inventory
- Upload Hardware Inventory
- Upload Security Settings Inventory
- Upload Security Products Inventory
- Upload Software Inventory

Clean Custom Inventory

This step allows you to delete entries in the custom inventory. Be aware that you need access to the CustomInventory.xml on the device to be cleaned as the values to be entered into the fields of the step are those of the .xml file.

Parameter	Description
Object Type	The value <OBJECT type="<value>"> of the entry/entries to be deleted from the .xml file. As there may be several objects of the same type with different names all entries of this type will be deleted if you do not specify the respective name in the field below. It is possible to use the wildcard characters *?* for a single letter and * for several letters.
Object Name	The value <OBJECT name="<value>"> of the entry/entries to be deleted from the .xml file. As there may be several objects with the same name of different types all entries of this name will be deleted if you do not specify the respective type in the field above. It is possible to use the wildcard characters *?* for a single letter and * for several letters.
Delete All	Check this box if all entries of a specific name or type in the inventory are to be deleted.

Clean Security Settings Inventory

This step deletes entries in the inventory for security settings. Be aware that you need access to the SecurityInventory.xml on the device to be cleaned as the values to be entered into the fields of the step are those of the .xml file.

Parameter	Description
Object Type	The value <OBJECT type=”<value>”> of the entry/entries to be deleted from the .xml file. As there may be several objects of the same type with different names all entries of this type will be deleted if you do not specify the respective name in the field below. It is possible to use the wildcard characters *?* for a single letter and * for several letters.
Object Name	The value <OBJECT name=”<value>”> of the entry/entries to be deleted from the .xml file. As there may be several objects with the same name of different types all entries of this name will be deleted if you do not specify the respective type in the field above. It is possible to use the wildcard characters *?* for a single letter and * for several letters.
Delete All	Check this box if all entries of a specific name or type in the security settings inventory are to be deleted.

Update Custom Inventory

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Configuration File	Specifies the location and name of the custom inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/custominventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the custom inventory may not longer work.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Update CustomInventory.xml File

This step either updates an existing XML object/attribute pair in the CustomInventory.xml file or adds it as a new set of XML tags.

Parameter	Description
Object Name	Defines the name of the object to be modified or added. In the **Custom Inventory Attribute** view this corresponds to the **Instance Name** value, i.e., *Monitor1* for the **Screen Information** attribute. In the .xml file this value corresponds to tag element **<OBJECT type="<object type name>" name="<object name>">** .
Object Type	Specifies the name of the object type. In the .xml file this corresponds to the tag **<OBJECT type="<object type name>"** , for example, *<OBJECT type="Monitor"* . The type name in this example will be translated if a translation exists, for example, for this example in the **Custom Inventory** view the type name **Monitor** corresponds to the **Name** value of the **Attributes** tab: **Screen Information** .
Attribute Name	Defines the name of the attribute to be modified or added. In the .xml file this corresponds to the tag **<ATTRIBUTE name="<Attribute Name>"** , for example, *<ATTRIBUTE name="SerialNumber"* . This value is also translated if a translation exists and corresponds to the column header of the table in the **Attributes** tab.
Attribute Value	The new value of the attribute to modify to or to be added. In the .xml file this corresponds to the tag **<ATTRIBUTE name="<Attribute Name>"**, e.g., **<ATTRIBUTE name="SerialNumber"**. This value is also translated if a translation exists and corresponds to the column header of the table in the **Attributes** tab.

Update Hardware Inventory

This step launches an update the hardware inventory of the device.

Parameter	Description
Configuration File	Defines the path of the hardware inventory configuration file. The path is relative to the agent configuration file. You may modify the entry, but be aware that if you wrongly modify the inventory may no longer work.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.

Parameter	Description
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Update Security Settings Inventory

This step launches an update of the security settings inventory of the device.

Parameter	Description
Configuration File	Defines the path of the security settings inventory configuration file for example, *../data/SecurityInventory /SecurityInventory.xml* . The path is relative to the agent configuration file. You may modify the entry, but be aware that if you wrongly modify the security settings inventory may no longer work.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Update Security Products Inventory

The step allows you to update the security products inventory of the device.

Parameter	Description
Configuration File	Specifies the location and name of the security products inventory .xml file. This file defines all attributes and values which is recovered from the remote clients to set up the custom inventory. The path to the file may be entered as a local path or as a URL such as _ftp://master/securityproductsinventory.xml_ . The path is relative to the agent configuration file. You may modify the entry, but be aware, that if you wrongly modify, the security products inventory may not longer work.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Additional Anti-Virus Data	Check this box to collect advanced data on installed anti-virus software products (virus definition file date, etc.) and upload them to the Security Products Inventory.
Additional Firewall Data	Check this box to collect advanced data on installed firewall software products (firewall status) and upload them to the Security Products Inventory.
Additional Anti-Spyware Data	Check this box to collect advanced data on installed anti-spyware software products (anti-spyware definition file date, etc.) and upload them to the Security Products Inventory.
Additional Browsers Data	Check this box to collect advanced data on installed browser software products (CERT compliance, etc.) and upload them to the Security Products Inventory.

Update Software Inventory

This step launches an update of the security settings inventory of the device.

Parameter	Description
Configuration File	Defines the path of the software inventory configuration file. The path is relative to the agent configuration file, for example, *../data/SoftwareInventory/swinvcfg.xml* . You may modify the entry, but be aware that if you wrongly modify the software inventory may no longer work.
File Extensions to Scan	Enter into this field the file extensions which are to be scanned to create the list of installed software applications, examples are *com,exe,bat* ,...
Included Directories	If you are only scanning **Scan Add/Remove Programs** but you also want to inventory the applications installed for a user, you must enter here the directory in which they are installed, for example `c:/users` for Windows 7 systems.
Excluded Directories	Enter the directories which are NOT to be scanned to create the list of installed software applications. The separator character between a list of directories is a comma (,). You can also enter the path to the directories as an environment variable enclosed in ${}.
Scan Hidden Directories	Check or uncheck this box to define if hidden directories are to be scanned for the software inventory update.
Scan Hidden Files	Check this box to scan hidden files for the software inventory update.
Scan Add /Remove Programs	Check or uncheck this box to define if registry entries for the Add/Remove Programs are to be scanned and added for the software inventory update.
Scan MSI Database	Check or uncheck this box to define if the MSI Windows database is to be scanned for the software inventory update.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.
Force Upload	

Parameter	Description
	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Update and Upload the Local Virtual Infrastructure Inventory

This step allows to update and upload the virtual infrastructure inventory of all virtual machines that are hosted on the device.

Parameter	Description
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed.

Upload Agent Identity

This step forces an upload of the identity of the agent to the master. The agent regularly uploads its identity according to the parameters defined in the identity configuration file. In special circumstances, however, it might be necessary to force an upload of the agent identity, for example, when agents were rolled out or changed location and there has been a data loss in the network, such as a broken down relay.

No parameters need to be defined for this step.

Upload Asset Discovery Results

This step uploads the inventory of a remote agentless device to the master.

No parameters need to be defined for this step.

Upload AutoDiscovery List

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Upload AutoDiscovery Objects	Defines if the objects discovered by the AutoDiscovery are uploaded.

Upload Custom Inventory

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.

Upload Hardware Inventory

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.

Upload Security Settings Inventory

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.

Upload Security Products Inventory

The step allows you to upload the security products inventory of the device to the master.

Parameter	Description
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.

Parameter	Description
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.

Upload Software Inventory

This step uploads the list of devices discovered by the local agent to the master and other devices.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.

Master Steps steps

This following group of steps is executed on the master, but they can be launched from any other device.

- Autodiscovered Device Verification
- CSV File Import
- Device Clean-up
- Centralized Wake On LAN
- Assignment Management via XML File
  - Example 1
  - Example 2
- Operational Rule Assignment via XML File
  - Example
- Package Assignment via XML File
  - Example

Autodiscovered Device Verification

This step sends an email with the list of newly autodiscovered devices since the last verification. The email contains the complete list of devices with other information pertinent to the individual devices, such as the operating system, discovered date and agent version, that have been added since the last verification.nThis step is only applicable on the master.

Parameter	Description
From	Enter the email address of the sender. This does not have to be a personal email, this may be any address which exists in your systems, such as *support@starfleet.com* . Also the email address does not have to be defined for an administrator account within the Console.
Message Text	Specify the introductory text of the mail body.
Port Number	Enter into this field the port number of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** .
Server Name	Enter into this field the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** . The name may either be entered as the full or short network name such as *mail* or *mail.enterprise.starfleet.com* or as its IP address in dotted notation, for example, *213.2.146.1* or *2001:db8:85a3::8a2e:370:7334* .
Subject	Contains the subject line of the mail.
To	Enter the email address of the recipient. This does not have to be a personal email, this may be any address which exists in your systems, such as *support@starfleet.com* . Also the email address does not have to be defined for an administrator account within the Console. You may specify more than one target address by separating them with a comma (,).

CSV File Import

This step imports data into the custom inventory data from a CSV file. The values in the CSV file may be separated either by a comma (,) or a semi-colon (;).

Parameter	Description
Administrator Name	The name of the administrator which is to execute this step. Make sure this administrator has the required capabilities and access rights, otherwise the step execution fails. Click the **Select** button next to the field and select the desired administrator from the list.
CSV File Path	The complete or relative path to the csv file. If you enter the path as a relative path it is relative to the master installation directory, *<InstallDir>/Master/* .
Custom Inventory Object Name	Enter the prefix for the instance name for the custom inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.
Erase CSV File after Import	Defines if the csv file is stored or deleted after the data import.

The format of the csv file must be as follows:

- The first line is the header and contains the names of the attributes equalling the columns of the final table; the first attribute (column) must be `Device Name` , the following are the remaining attributes
- The lines 2 to n are the data lines, containing the values of the devices, whereby the first value must be the device name followed by the other attributes matching their column title defined in the header line.
- The separator can be either a comma (,) or a semi-colon (;).

Example:

```
DeviceName;Name;IPAddress
DEVICE1;Samuel;10.5.157.55
DEVICE2;John;10.5.157.56
```

Device Clean-up

This step allows you to delete direct and indirect members from selected device groups. Optionally, if the deprecate device option is selected, the devices are deprecated instead of deleted.

Parameter	Description
Device Group	Enter the name of the device group, of which you want to delete or deprecate all its members. To select the group click the **Add** button and select the group or groups in the appearing window.
Delete Subgroup Members	Check this box to also delete or deprecate all members of all subgroups of the selected group.
Deprecate Devices	Check this box to deprecate all member devices of this group instead of deleting them.
Delete Assigned Devices	Check this box to delete the devices even if they are assigned to objects.
Allow Partial Execution	If this box is checked, the step executes successfully, even if some of the devices cannot be deleted or deprecated. In this case, an error is displayed in the "Error Details" column of the assigned device view. If none of the devices can be deleted or deprecated, the rule fails.nTo find which devices were not successfully deleted or deprecated, you need to check the operational rules log (operationalrules.log).
Administrator Name	The name of the administrator which is to execute this step. Make sure this administrator has the required capabilities and access rights, otherwise the step execution fails. Click the **Select** button next to the field and select the desired administrator from the list.

Centralized Wake On LAN

This step allows you to wake up specific devices via a number of other devices. Depending on the agent configuration, wakener devices should try to wake up the target devices using one of the available mechanisms: local, remote via configured wakeners, remote via notified topology or fallback (Unicast or Subnet-Directed Broadcast).

Parameter	Description
Number of Retries	Defines the number of retries the step is to execute before abandoning if it fails.
Which devices or groups should be woken?	Add into this list field the devices or device groups which are to be woken up. To add select the **Add** button and select the desired objects from the **Select Objects** window.
Retry Interval (sec)	Defines the interval at which the step is to effect its retries in seconds.

Parameter	Description
Who should wake up the devices?	Allows the master to call the wake up action on another device for which it has the following possibilities: To **Use Specific Wakener** , that is, a wakener device can be defined to execute the wake up actions if all targets are located in one subnet, or the waking up actions can be executed by the targets' parent device, **Wakeup via Target Parent** . In this case the list of direct parents of the devices to wake up is retrieved from the database and the waking up is delegated to the parents of the respective devices to wake up.
Which device should wake up the targets?	Enter into this list the device to wake up the devices listed above. You may only specify one device in this field. If you are not sure that all targets are on the defined device's subnet select the option **Wakeup via Target Parent** above to make sure all targets are woken up.

Assignment Management via XML File

This step allows you to assign/unassign objects (operational rules, packages, patch groups and application lists) via an XML file to/from their targets (devices and device groups).

Parameter	Description
File Path	Enter the complete path to the storage location of the XML file. The path may contain wildcard characters, for example, *c:tempbmcac**.xml_ .
Administrator Name	The name of the administrator which is to execute this step. Make sure this administrator has the required capabilities and access rights, otherwise the step execution fails. Click the **Select** button next to the field and select the desired administrator from the list.
File destination path if successful	Enter into this field the full destination path into which the XML file is copied if it has been treated with success, that is, all assignments listed on the listed objects could be effected in the BCM database, for example, *c:tempok* . This path must point to a different directory than that of the source path, it can however be the same as for failed assignments.
File destination path if failed	Enter into this field the full destination path into which the XML file is copied if an error occurred during its treatment, that is, at least one of the assignments could not be effected in the BCM database, for example, *c:tempnok* . This path must point to a different directory than that of the source path, it can however be the same as for successful assignments.
Activate Created Assignment	Check this box, if the assignments provided by the XML file are to become active right away. If the box is left unchecked, the assignments are all recorded in the database, however the assigments are not sent and the object is thus not executed.
Reassign if Assignment Already Exists	Check this box if in case of an existing assignment it is to be reactivated. If the box is not checked the modifications supplied by the XML file are made to the assignments, however they do not become active.

Example 1

The following example assigns and a patch group to an individual device and a device group on March 9, 2011 at 4pm and advertises an operational rule to the device and group as well. The assignment is done by the administrator admin.

```
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTASSOCIATIONS>
  <!-- This section must contain the list of objects to assign -->
  <OBJECTS>
    <!-- type can be OperationalRule, Package, PatchGroup or ApplicationList -->
    <!-- the object can be referenced with its database ID with attribute "id" -->
    <!-- or through its name with attribute "name" -->
    <OBJECT type="OperationalRule" id="1001"/>
    <OBJECT type="PatchGroup" name="PG Test Rule"/>
  </OBJECTS>
  <DEVICES>
    <!-- This section contains the list of devices to which the objects are to be assigned -->
    <!-- Devices can be referenced with database ID (attribute "id") -->
    <!-- or name (attribute "name") -->
    <DEVICE id="1000"/>
    <DEVICE name="Device X"/>
  </DEVICES>
  <DEVICEGROUPS>
    <!-- This section contains the list of device groups to which the objects are to be assigned --
>
    <!-- Groups can be referenced with database ID (attribute "id") -->
    <!-- or name (attribute "name") -->
    <DEVICEGROUP id="1000"/>
    <DEVICEGROUP name="My Group"/>
  </DEVICEGROUPS>
  <OPTIONS>
    <!-- Which administrator profile will be used for the assignment -->
    <ADMINISTRATOR name="admin"/>
      <!-- When will the object assignment be sent to devices (number of hours, minutes, etc and 0 for
immediate) -->
      <!-- This only applies to OperationalRule, Package, PatchGroup object types -->
      <SCHEDULE hour="16" minute="0" day="9" month="3" year="2011"/>
        <!-- Add if type is OperationalRule and only advertizemnt is needed -->
      <ADVERTIZE/>
  </OPTIONS>
</OBJECTASSOCIATIONS>
```

Example 2

This example unassigns an operational rule and a patch group from an individual device and a device group with the default schedule, that is, immediately.

```
<?xml version="1.0" encoding="UTF-8"?>
<OBJECTUNASSIGN>
  <!-- This section must contain the list of objects to unassign -->
  <OBJECTS>
    <!-- type can be OperationalRule, Package, PatchGroup or ApplicationList -->
    <!-- the object can be referenced with its database ID with attribute "id" -->
    <!-- or through its name with attribute "name" -->
    <OBJECT type="OperationalRule" id="1001"/>
    <OBJECT type="PatchGroup" name="PG Test Rule"/>
  </OBJECTS>
  <DEVICES>
    <!-- This section contains the list of devices from which the objects are to be unassigned --
>
    <!-- Devices can be referenced with database ID (attribute "id") -->
    <!-- or name (attribute "name") -->
    <DEVICE id="1000"/>
    <DEVICE name="Device X"/>
  </DEVICES>
  <DEVICEGROUPS>
    <!-- This section contains the list of device groups from which the objects are to be unassigned --
>
    <!-- Groups can be referenced with database ID (attribute "id") -->
    <!-- or name (attribute "name") -->
    <DEVICEGROUP id="1000"/>
    <DEVICEGROUP name="My Group"/>
  </DEVICEGROUPS>
</OBJECTUNASSIGN>
```

Operational Rule Assignment via XML File

This step is designed to automate the assignment process of operational rules. The assignment itself is defined in the XML file. The schedule is defined via the administrator with which the assignment is created. It is therefore recommended to create an administrator group with a number of administrator members for each of which a specific schedule is to be defined. When listing an administrator in the respective field, its activation/execution schedule combination is used as the schedule for the operational rule/device assignment.

This step allows you to assign operational rules via an XML file to their target devices with a predefined schedule.

Parameter	Description
Administrator Name	The name of the administrator which is to execute this step. Make sure this administrator has the required capabilities and access rights, otherwise the step execution fails. Click the **Select** button next to the field and select the desired administrator from the list.
XML File Path	Enter the complete path to the storage location of the XML file.

Example

The following example assigns an operational rule to an individual device on March 9, 2011 at 4 pm as the administrator admin.

```
<?xml version="1.0" encoding="UTF-8"?>
<RULEASSOCIATIONS>
    <!-- This section must contain the list of operational rules to assign -->
    <RULES>
        <RULE id="1001"/>         // The Rule ID/Name must be the exact value that the rule is
        <RULE name="Test Rule"/>      known in Precision Database.
    </RULES>

    <DEVICES>
    <!-- This section must contain the list of devices to which the rules are to be assigned -->
        <DEVICE id="1000"/>        // The Device ID/name must be the exact value that the device is
        <DEVICE name="Device X"/>     known in Precision Database.
    </DEVICES>

    <OPTIONS>
        <!-- When will the rule be activated (number of hours, minutes, etc and 0 for immediate) -->
        <ADMINISTRATOR name="admin"/>
        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2006"/>
        <!-- What type of installation should be used: "normal", "administrative" or "network"-->
        <NETWORKINSTALL mode="normal" />
    </OPTIONS>

</RULEASSOCIATIONS>
```

Package Assignment via XML File

This step is designed to automate the assignment process of packages. The assignment itself is defined in the XML file. The activation schedule may also be defined in this XML file. If a bad date is specified the assignment will be planned for the current day.

This step allows to assign packages via an XML file to their target devices with a predefined schedule.

Parameter	Description
Administrator Name	The name of the administrator which is to execute this step. Make sure this administrator has the required capabilities and access rights, otherwise the step execution fails. Click the **Select** button next to the field and select the desired administrator from the list.
XML File Path	Enter the complete path to the storage location of the XML file.

Example

The following example assigns a package to two devices on March 9, 2011 at 4 pm as the administrator admin.

```
<?xml version="1.0" encoding="UTF-8"?>
<PACKAGEASSOCIATIONS>
    <!-- This section must contain the list of packages to assign -->
    <PACKAGES>
        <PACKAGE id="1001"/>  // The Package ID must be the value that the package is
                                 known in Precision Database.
    </PACKAGES>

    <DEVICES>
    <!-- This section must contain the list of devices to which the packages are
         assigned to-->
        <DEVICE id="1000"/>  // The Device ID must be the value that the device is
        <DEVICE id="1002"/>      known in Precision Database.
    </DEVICES>

    <OPTIONS>
        <!-- This section contains the optional parameters, such as the administrator
              under which the packages are assigned and the schedule. -->
        <ADMINISTRATOR name="admin"/>
        <SCHEDULE hour="16" minute="0" day="9" month="10" year="2006"/>
    </OPTIONS>
</PACKAGEASSOCIATIONS>
```

Monitoring steps

The following steps are used for monitoring the state and operating systems of the managed devices. If any of the conditions specified for monitoring passes its threshold an event is raised.

- Advanced Installed Software Check
- Check Disk Space
- Check File Date
- Check Installed RAM
- Check Installed Software
- Check Operating System Version
- Check Service Execution
- Check URL Availability
- Check Windows Events
- IP Address Verification
- Low Disk Space
- New Event Monitoring
- Total Memory Changed

Advanced Installed Software Check

This step allows you to verify if a specific software is installed on a device, and if not, to assign it directly to a device group via which the respective software will be installed. The existence of the software may be verified via the execution status of an operational rule, the existence of the software in the software inventory and via the existence of an executable file.

Parameter	Description
Check for File	Check this box, if the agent is also to search for the software via its executable file. If checked you also need to fill in the following parameter.
Check in Software Inventory	Defines if the agent is to check for the software in the generated software inventory.
Check for Operational Rule	Check this box, if it is possible that the software in question has been installed via an operational rule. In this case you must also fill in the following field. The software is regarded as existing, if the operational rule specified below was assigned to the device and has the final status *Executed* .
File Path	The complete or relative path to the file. If you enter the path as a relative path it is relative to the *<InstallDir> /Master/config directory* . The file path may use wildcard characters, such as the asterisks (*), for example, *../log /mtxagent** to search in all stored log files of the agent for a specific expression.
Full Name Match	Check this option if the operation is only to be run if the software application and version number provide a complete match to the above listed parameters.
Device Group to Assign	If the software could not be found on the target device via either of the above defined methods, the device may be directly assigned to a device group which is assigned to the operational rule installing the software. For this you need to enter the respective device group in the field below by clicking the **Add** button. Find the device group assigned to the operational rule and click the **OK** button.
Operational Rule	If you checked the box above, enter the operational rule, that installs the software in question. To enter the rule, click the **Add** button. Find the operational rule that installs the software application in the window and click the **OK** button.
Software Name	Enter into this field the name of the software for which the target device is to be checked, for example, *Microsoft Word 2003* .
Version	Enter the version number of the application if it is relevant. This parameter is optional.
Check Version	Defines the operator to be used with the above listed version number: • **Version higher than** : if the installed version is higher than the one specified in the **Version** field above. • **Version lower than** : if the installed version is lower than the one specified in the **Version** field above. • **Version equal to** : if the installed version is equal to the specified version. • **No Version Check** : if the any version of the software application is to be searched for. • **Version not equal to** : if the installed version is to be any version but the specified version. • **Version higher than or equal to** : if the installed version is higher than or equal to the specified version. • **Version lower than or equal to** : if the installed version is lower than or equal to the specified version.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check Disk Space

This step raises an event if the free disk space is less than the given threshold.

Parameter	Description
Free Space (MB)	Defines the amount of disk space that is to remain free and available on the managed devices in MB.
Target Partition	Defines the partition which is to be checked for the disk space.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check File Date

This step checks if file creation or modification date match the given parameters. Year, month and day parameters are mandatory.

Parameter	Description
Operator	Select the verification operator for the date provided in the following fields.
Check Type	Select from this dropdown list if the creation (**Creation Date**) or the modification (**Modification Date**) date is to be verified.
Day	The day of the month.
File Name	The name and full directory path of the file.
Hour	Check the box to not only verify the date but also the hour of the file. Enter the hour value in the field that becomes available now with its 24-hour value, for example, 13 for 1 pm.
Minute	Check the box to not only verify the date but also the minutes of the file. Enter the minute value in the field that becomes available now. If no minute value is indicated with the hour value all files created between for example, 13: 00 and 13:59 are verified as OK with the equal operator.
Month	The month value in its two digit form, for example, 03 for march.
Second	Check the box to not only verify the date but also the second of the file. Enter the second value in the field that becomes available now.
Year (YYYY)	Enter the year value with its four digits, for example, *2009* .

Check Installed RAM

This step checks the size of the physical RAM on the managed devices and raises an event if the required amount if RAM is not available.

Parameter	Description
Generate Event If Failed	Check this box if an event is to be sent if the step fails.
RAM (MB)	Specifies the minimum size of the physical RAM to be installed on the managed devices in MB.

Check Installed Software

This step checks if a certain software application is installed on a target device and if yes, which version of it. It is particularly useful for software distribution, for example, for executing upgrades to a specific application. If the application is not installed an event is generated.

Parameter	Description
Full Name Match	Check this option if the operation is only to be run if the software application and version number provide a complete match to the above listed parameters.
Software Name	Enter the name of the software for which the target devices are to be checked, for example, *Microsoft Word 2003* .
Version	Enter the version number of the application if it is relevant.
Version Equal to	Check this box, if you need to know if the installed version is equal to the one specified in the **Version** field above.
Version higher than	Check this box, if you need to know if the installed version is higher than the one specified in the **Version** field above.
Version lower than	Check this box, if you need to know if the installed version is lower than the one specified in the **Version** field above.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check Operating System Version

This step checks for the operating system installed on target machines. It is particularly useful for software distribution; for example, when an application is only to be installed on a certain type of operating system. If the name of the operating system and the revision number do not match, an event is generated.

Parameter	Description
Operating System	Enter the name of the operating system for which the target devices are to be checked, for example, *Window 2000 Professional* .
System Revision	Enter the revision number of the operating system, for example, *Service Pack 3* .

Parameter	Description
Full Name Match	Check this option if the operation is only to be run if the operating system and revision number provide a complete match to the above listed parameters.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check Service Execution

This steps checks if the specified service is currently running. An event can be generated if the specified service is not running.

Parameter	Description
Service Name	Enter the name of the service as it is known by the respective system.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check URL Availability

This step checks if the specified URL is responding or not. If not, an alert can be sent and the step returns an error.

Parameter	Description
URL	Enter into this field the URL to verify in the format of http(s)://<server>/ or http(s)://<user>:<password>@<server>:<port>/<subdir>/<file>.
Send an alert if not responding	Check this box to generate an alert if the specified URL cannot be reached.
Alert Description	Enter into this field the descriptive text for the alert to be displayed.
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check Windows Events

This step checks for a specified string in the Windows event log files. If an event matching the string is found, the step returns an error and an alert can be sent. The first time this step is executed, no alert is generated.

Parameter	Description
String	Enter the string to find in the Windows event log file(s). It may be entered as a regular expression using the * and ? characters.
Match Case	Check this box if the string entered in the field above is to be case sensitive, that is, if the searched string is *error* , it finds *error, Error* and *ERROR* .
Event ID	Defines if only events of a specific ID are to be monitored. In this case you need to enter the ID exactly as it is known in Windows.
Event Log	The log file in which to check for the event. You can either search in all or in one of the event logs.
Event Severity	The event severity to verify.
Send Alert if Found	Check this box to activate the sending of an alert if an event is found since the last check that matches all the criteria defined below.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

IP Address Verification

This step verifies if the IP address of a host has changed. The first time this step is run, no comparison can be effected, as the IP address is not yet referenced. During this execution, the reference address will be entered into the respective configuration file for further verifications.

No parameters need to be defined for this step.

Low Disk Space

This step creates an event if the disk space is less than the given threshold.

Parameter	Description
Insufficient Disk Space	Check this box if events are to be included in the mail that indicate that there is insufficient disk space available on a device.
Drive	Defines the drive which is to be checked for its remaining available disk space. It is specified through its letter.
Threshold (%)	Defines the threshold as a percentage value of 100%. Once the available disk space falls below this percentage, an event is raised.
Send an alert	Check this box to send an alert.

Parameter	Description
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

New Event Monitoring

This step sends an email to specific recipients with a list of newly generated events of a specific type that were registered since the last verification.

Parameter	Description
A monitored Windows event occurred	Check this box if generated Windows events are to be included in the mail, which have been defined to be monitored by the Monitored Objects module.
From	Enter the email address of the sender. This does not have to be a personal email, this may be any address which exists in your systems, such as *support@starfleet.com* . Also the email address does not have to be defined for an administrator account within the Console.
Insufficient Disk Space	Check this box if events are to be included in the mail that indicate that there is insufficient disk space available on a device.
Message Text	Specify the introductory text of the mail body.
Port Number	Enter into this field the port number of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** .
Server Name	Enter into this field the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** . The name may either be entered as the full or short network name such as *mail* or *mail.enterprise.starfleet.com* or as its IP address in dotted notation, for example, *213.2.146.1* or *2001:db8:85a3::8a2e:370:7334* .
Subject	Contains the subject line of the mail.
A monitored performance counter passed its threshold	Check this box if events are to be included in the mail, which were generated when the threshold of a monitored performance counter was exceeded.
Memory Size	Check this box if events regarding changed memory size are to be included in the mail.
To	Enter the email address of the recipient. This does not have to be a personal email, this may be any address which exists in your systems, such as *support@starfleet.com* . Also the email address does not have to be defined for an administrator account within the Console. You may specify more than one target address by separating them with a comma (,).

Total Memory Changed

This step generates an event if the RAM of a device has changed.

Parameter	Description
	Check this box to send an alert.

Parameter	Description
Send an alert	
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Package Factory steps

This class of steps comprises all those concerned with the package factory and the creation and maintenance of the different types of packages and packagers.

- Copy Package
- Publish Package to Master

Copy Package

This step copies a package from a remote package factory to your local package factory. Be aware that it is imperative that the packager alias for the package type to be copied is already created under section HttpAliases of the HttpProtocolHandler.ini configuration file of the server, for example, PackagerCustom.

Parameter	Description
Package Type	Select the type of the package that is to be copied from the drop-down list.
Package Name	The name of the package to be copied.
Server Port	The corresponding port on the remote device.
Server Name	Enter the name of the server from which the package is to be copied. You may enter in form of the remote device's IP address, for example, *192.1.125.2* or *FD43-0-0-0-8C84-4BAD-D413-DD68.ipv6-literal.net* , or as its short or long network name.
User Name	Enter into this field a valid user login to log on to the remote device.
User Password	The password corresponding the login specified above. For security reasons the password is only displayed in the form or asterisks (*).

Publish Package to Master

This step publishes a specific package to the master at a specific time which is managed via the package's schedule. The step must be executed on the respective packager.

Parameter	Description
Package Type	Select the type of the package to be published to the master from the drop-down list.
Package Name	Enter into this field the complete name of the package, that is, including the extension, for example, *orca.msi* . If the package is located in a folder under the packager this folder must also be included in the complete name, that is, *database_pkgs/orca.msi* .

Patch Management steps

This group contains all steps regarding the management of patches.

- Analyze Patch Situation
- Purge Patch Inventory
- Uninstall Patch
- Update Knowledge Base
- Deploy Patches on MAC OS

Analyze Patch Situation

This step executes a scan for the patch manager module.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.

Purge Patch Inventory

This step purges the patch inventory for the assigned devices. In this way you may free up licenses to patch additional devices which still need patching when the patch license count has been reached.

No parameters need to be defined for this step.

Uninstall Patch

This step uninstalls any patch which is located in the Add or Remove Programs list of the Control Panel.

Parameter	Description
Force Reboot	Check this option if the step is to launch a system reboot after the successful uninstall.
Patch Name	Enter the name of the patch to uninstall as it is entered in the Add or Remove Programs list of the Control Panel.
Quiet Mode Uninstall	Defines that the patch uninstallation is to be executed without the remote user's being aware of it. If you uncheck this box the default dialog boxes concerned with patch uninstallation appears on the screen. Be aware, however, that not all patches necessarily interact with the user.
Wait for End of Execution	Check this parameter if the step is to wait for the end of the operation before declaring its execution terminated.

Update Knowledge Base

This step updates the local Patch Knowledge Base with the base provided by the master.

No parameters need to be defined for this step.

Deploy Patches on MAC OS

This step deploys patches on devices with a MAC operating system.

Parameter	Description
Deployment Type	Select from this list which type of patch you want to apply. You can install all patches that are currently available, the patches that are recommended to be installed and a specific update. In this case you need to specify the patch to apply in the following field.
Install Specific Update	If you have selected to install a specific patch only in the field above you need to enter the name and version number of the patch to install into this field. Be careful to exactly copy its name, paying attention to capital and small letters and append the version number with a dash to the name, for example, *iPhoto-9.4.2* , otherwise it is not installed.
Install from Local Repository	Check this box if the patch is to be installed from a local repository and then enter the URL to it into the field to the right, for example, _http://swscan.apple.com/content/catalogs/others/index-leopard.merged-1.sucatalog_ .
Reboot after deployment	Defines if a reboot is previewed after the installation of the last patch package of the patch group. Be aware that if you do not reboot after installation when a reboot is expected by one of the patches installed, this patch is still seen as missing even if you force a scan after install by the option below.
Allow User to Cancel Reboot	Specifies if the user may definitely cancel the reboot of his device.
Allow User to Extend Countdown Timer	Check this box if the user may extend the countdown timer before the patch installation automatically starts.
Initial Countdown Timer (min)	The waiting time in minutes between the pop-up window's first appearance and the actual initialisation of the device reboot.

Parameter	Description
Countdown Timer Increment (min)	The interval by which the countdown timer is incremented each time the user decides to extend it, if he has been allowed to do so by the option above.
Countdown Timer Maximum (min)	Defines the maximum interval the countdown timer may be extended. If for example the initial value is 2 minutes, the user may each time extend it by 2 minutes as well, and this value is set to 5 minutes, the user may extend the countdown once, 2 min initial 2*2 min extension makes 6 minutes which is higher than the defined 5 minutes.

Power Management steps

This group collects all power management steps in the Client Management. The steps are applicable to Windows only with one exception.

- Create/Modify Advanced Power Plan
- Create/Modify Global Power Policies
- Create/Modify Power Plan
- Define Power Plan
- Delete Power Plan
- Hibernate
- Suspend
- Update Power Management Inventory

Create/Modify Advanced Power Plan

This step allows you to write power plans that are compatible with the older Windows versions as well as Vista and later version schemes. Fields that are not filled in will take the current value on the device. The step contains parameters applicable to all versions, as well as those for before and after Vista versions.

Parameters existing for AC and DC options will be explained only once, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop. All parameters need to be activated first, i.e., the left checkbox must be marked before the step will activate the parameter. Only then can the desired values be entered, selected or marked.

Parameter	Description
Active Power Plan	Defines, if the newly defined power plan is to be activated right away and thus is the default plan.
Power Plan Description	A longer textual description of the new power plan, such as after how much time the components is switched off.
Power Plan Name	The name for the new power plan.

Parameter	Description
Allow Away Mode (Vista and later, AC)	Allows users to keep their system running in case they share resources or perform other tasks for which the user doesn't actually need to operate the computer. When the PC enters **Away mode** , the display is turned off, sound is disabled, and keyboard and mouse input are ignored. **Away mode** is not a real power state. Although the PC appears to be turned off, it actually still runs and consumes power as normal. The latter is why **Away mode** is not recommended unless it's really needed. Once **Away mode** is enabled, any action that would normally put the computer into **Sleep mode** now puts the computer in **Away mode** . Pressing the physical **On/Off** button on the PC exits **Away mode** . **Away mode** can be set by media sharing applications when needed.
Allow Away Mode (Vista and later, DC)	Allows users to keep their system running in case they share resources or perform other tasks for which the user doesn't actually need to operate the computer. When the PC enters **Away mode** , the display is turned off, sound is disabled, and keyboard and mouse input are ignored. **Away mode** is not a real power state. Although the PC appears to be turned off, it actually still runs and consumes power as normal. The latter is why **Away mode** is not recommended unless it's really needed. Once **Away mode** is enabled, any action that would normally put the computer into **Sleep mode** now puts the computer in **Away mode** . Pressing the physical **On/Off** button on the PC exits **Away mode** . **Away mode** can be set by media sharing applications when needed.
Allow RTC wake (Vista and later, AC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Allow RTC wake (Vista and later, DC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Allow sleep states (Vista and later, AC)	Determines whether programs can prevent a device from entering sleep mode. If this option is activated, applications and services with active processes do not prevent the device from entering sleep mode. If deactivated, they do.
Allow sleep states (Vista and later, DC)	Determines whether programs can prevent a device from entering sleep mode. If this option is activated, applications and services with active processes do not prevent the device from entering sleep mode. If deactivated, they do.
Low battery level action (Vista and later, AC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Critical battery level action.
Low battery level action (Vista and later, DC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Critical battery level action.
Critical battery level action (Vista and later, AC)	Defines which of the battery discharge policy settings is used when the battery discharges below the critical threshold.
Critical battery level action (Vista and later, DC)	Defines which of the battery discharge policy settings is used when the battery discharges below the critical threshold.

Parameter	Description
Low battery level (%, Vista and later, AC)	Defines the low level threshold of battery discharge in percentage. When the device enters a low-power state, the system notifies the user with either a text prompt alone or a text prompt and an audible alarm. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Low battery level action.
Low battery level (%, Vista and later, DC)	Defines the low level threshold of battery discharge in percentage. When the device enters a low-power state, the system notifies the user with either a text prompt alone or a text prompt and an audible alarm. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, Low battery level action.
Critical battery level (%, Vista and later, AC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Critical battery level action** .
Critical battery level (%, Vista and later, DC)	Defines the critical level threshold of battery discharge in percentage. Critical level indicates that battery failure is imminent. When the device enters a critical power state, the system notifies the user and then enters the sleep mode. In some cases it might be advisable to configure the device to go a step further and enter another power mode, as defined via the following parameter, **Critical battery level action** .
Critical power transition (Vista and later, AC)	Specifies if critical power transition is supported. Critical power transition occurs when battery voltages for the primary batteries decrease to a critically low level that prevents the target device from performing a safe shutdown. Instead of running an On-to-Suspend transition, during which power is shut down in a timely manner, the critical power transition bypasses the usual steps of turning off power to any peripherals or devices by immediately shutting down power to them and applying refresh voltage to the RAM. This preserves the file system and sets the microprocessor into the suspend power state. Recovery from a critical power transition occurs when adequate power is applied to the device. The process of a target device recovering from a critical power transition is equivalent to a warm boot transition.
Critical power transition (Vista and later, DC)	Specifies if critical power transition is supported. Critical power transition occurs when battery voltages for the primary batteries decrease to a critically low level that prevents the target device from performing a safe shutdown. Instead of running an On-to-Suspend transition, during which power is shut down in a timely manner, the critical power transition bypasses the usual steps of turning off power to any peripherals or devices by immediately shutting down power to them and applying refresh voltage to the RAM. This preserves the file system and sets the microprocessor into the suspend power state. Recovery from a critical power transition occurs when adequate power is applied to the device. The process of a target device recovering from a critical power transition is equivalent to a warm boot transition.
Hibernate after (before Vista, seconds, AC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Hibernate after (before Vista, seconds, DC)	Determines whether and when a device hibernates to conserve power. When a computer goes into hibernation a snapshot of the user workspace and the current operating environment is taken by writing the current memory to disk. When a user turns the computer back on, reading the memory from disk restores the user workspace and operating environment. In Windows Vista this setting is normally not used because the standard configuration is to sleep after a period of inactivity. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device hibernates.
Sleep after (before Vista, seconds, AC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.

Parameter	Description
Sleep after (before Vista, seconds, DC)	Determines whether and when a device enters a sleep state to conserve power. Leave the option unchecked to deactivate it. Check the option to activate it and enter a specific value in minutes to define how long the device must be inactive before the device enters a sleep mode.
Fan throttle tolerance (%, before Vista, AC)	The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event, expressed as a percentage. The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event while the system is operating on AC (utility) power, expressed as a percentage.
Fan throttle tolerance (%, before Vista, DC)	The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event, expressed as a percentage. The lower limit that the processor may be throttled down to prior to turning on system fans in response to a thermal event while the system is operating on AC (utility) power, expressed as a percentage.
Forced throttle (%, before Vista, AC)	The processor throttle level to be imposed by the system, expressed as a percentage. The processor throttle level to be imposed by the system while the computer is running on AC (utility) power, expressed as a percentage.
Forced throttle (%, before Vista, DC)	The processor throttle level to be imposed by the system, expressed as a percentage.
Allow hybrid sleep (Vista and later, AC)	Specifies whether the device uses the Windows Vista sleep mode rather than the sleep mode used in earlier versions of Windows. The Window Vista hybrid sleep mode puts the device in a low power consumption state until the user resumes using the computer. When running on battery, laptops and Tablet PCs continue to use battery power in the sleep mode, but at a very low rate. If the battery runs low on power while the computer is in sleep mode the current working environment is saved to the hard disk and then the device is shut down completely. This final state is similar to the hibernate mode used with Windows XP. Leave the option unchecked to deactivate it or check to activate it.
Allow hybrid sleep (Vista and later, DC)	Specifies whether the device uses the Windows Vista sleep mode rather than the sleep mode used in earlier versions of Windows. The Window Vista hybrid sleep mode puts the device in a low power consumption state until the user resumes using the computer. When running o battery, laptops and Tablet PCs continue to use battery power in the sleep mode, but at a very low rate. If the battery runs low on power while the computer is in sleep mode the current working environment is saved to the hard disk and then the device is shut down completely. This final state is similar to the hibernate mode used with Windows XP. Leave the option unchecked to deactivate it or check to activate it.
Hibernate after (seconds, Vista and later, AC)	Puts the device into hibernation mode after the defined number of seconds of inactivity. A value of zero indicates never hibernate.
Hibernate after (seconds, Vista and later, DC)	Puts the device into hibernation mode after the defined number of seconds of inactivity. A value of zero indicates never hibernate.
Action at idling (before Vista, AC)	Defines the system power action to initiate when the system idle timer expires.
	Defines the system power action to initiate when the system idle timer expires.

Parameter	Description
Action at idling (before Vista, DC)	
Idle at (%, before Vista, AC)	The level of system activity that defines the threshold for idle detection, expressed as a percentage.
Idle at (%, before Vista, DC)	The level of system activity that defines the threshold for idle detection, expressed as a percentage.
Idle after (seconds, AC)	The time in seconds that the level of system activity must remain below the idle detection threshold before the system idle timer expires.
Idle after (seconds, DC)	The time in seconds that the level of system activity must remain below the idle detection threshold before the system idle timer expires.
Lid close action (Vista and later, AC)	Sets the default action when the lid of a laptop is closed.
Lid close action (Vista and later, DC)	Sets the default action when the lid of a laptop is closed.
Lock console on activation (Vista and later, AC)	Determines whether a password is required when a device wakes from sleep. This option may be activated or deactivated. With domain devices this option should be activated and can only be controled via Group Policy.
Lock console on activation (Vista and later, DC)	Determines whether a password is required when a device wakes from sleep. This option may be activated or deactivated. With domain devices this option should be activated and can only be controled via Group Policy.
Maximum Sleep State (before Vista, AC)	The maximum system sleep state currently supported.
Maximum Sleep State (before Vista, DC)	The maximum system sleep state currently supported.
Minimum Sleep State (before Vista, AC)	The minimum system power state to enter on a system sleep action.
Minimum Sleep State (before Vista, DC)	The minimum system power state to enter on a system sleep action.

Parameter	Description
Minimum processor state (%, AC)	Sets a minimum performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted minimum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. For example a value of 5 % would lengthen the time required to respond to requests and process data while offering substantial power savings. A value of 50 % helps to balance responsiveness and processing performance while offering moderate power savings. A value of 100 % would maximize responsiveness and processing performance while offering no power savings at all.
Minimum processor state (%, DC)	Sets a minimum performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted minimum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. For example a value of 5 % would lengthen the time required to respond to requests and process data while offering substantial power savings. A value of 50 % helps to balance responsiveness and processing performance while offering moderate power savings. A value of 100 % would maximize responsiveness and processing performance while offering no power savings at all.
Multimedia when sharing media (Vista and later, AC)	Determines what the device does when a device or another computer plays media from the computer. If you set this option to **Allow the computer to enter Away Mode** , the computer does not enter sleep mode when sharing media with other devices or computers. If you set this option to **Allow the computer to sleep** , the computer can enter sleep mode after an appropriate period of inactivity regardless of whether media is being shared with other computers or devices. If you set this option to **Prevent idling to sleep** , the computer only enters sleep mode, when sharing media with other devices or computers, if a user puts the computer in sleep mode.
Multimedia when sharing media (Vista and later, DC)	Determines what the device does when a device or another computer plays media from the computer. If you set this option to **Allow the computer to enter Away Mode** , the computer does not enter sleep mode when sharing media with other devices or computers. If you set this option to **Allow the computer to sleep** , the computer can enter sleep mode after an appropriate period of inactivity regardless of whether media is being shared with other computers or devices. If you set this option to **Prevent idling to sleep** , the computer only enters sleep mode, when sharing media with other devices or computers, if a user puts the computer in sleep mode.
Optimized for high performance (before Vista, AC)	If this option is activated, the system turns on cooling fans and run the processor at full speed when passive cooling is specified. This causes the operating system to be biased towards using the fan and running the processor at full speed.
Optimized for high performance (before Vista, DC)	If this option is activated, the system turns on cooling fans and run the processor at full speed when passive cooling is specified. This causes the operating system to be biased towards using the fan and running the processor at full speed.
Action at over-throttling (before Vista, AC)	Defines the system power action to initiate in response to a thermal event when processor throttling is unable to adequately reduce the system temperature.
Action at over-throttling (before Vista, DC)	Defines the system power action to initiate in response to a thermal event when processor throttling is unable to adequately reduce the system temperature.
PCI Express Link State Power Management (Vista and later, AC)	Determines the power saving mode to use with **Peripheral Component Interconnect (PCI) Express** devices connected to the device. Possible values are **Off, Moderate power savings** or **Maximum power savings** .

Parameter	Description
PCI Express Link State Power Management (Vista and later, DC)	Determines the power saving mode to use with **Peripheral Component Interconnect (PCI) Express** devices connected to the device. Possible values are **Off, Moderate power savings** or **Maximum power savings** .
Power button action (Vista and later, AC)	Specifies the action to take when the device's power button is pressed.
Power button action (Vista and later, DC)	Specifies the action to take when the device's power button is pressed.
Maximum processor state (%, Vista and later, AC)	Sets a maximum or peak performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted maximum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. Although reducing the maximum processing power to 50 % or below can cause a significant in reduction in performance and responsiveness, it can also provide significant power savings.
Maximum processor state (%, Vista and later, DC)	Sets a maximum or peak performance state for the device's processor in percent. To save power and reduce energy consumption, lower the permitted maximum performance state. However, lowering the performance state has a direct cost in responsiveness and computational speed. Although reducing the maximum processing power to 50 % or below can cause a significant in reduction in performance and responsiveness, it can also provide significant power savings.
Reduced Latency Sleep State (before Vista, AC)	The system power state to enter on a system sleep action when there are outstanding latency requirements.
Reduced Latency Sleep State (before Vista, DC)	The system power state to enter on a system sleep action when there are outstanding latency requirements.
Search and indexing power saving modes (Vista and later, AC)	Allows you to balance indexing activity with power consumption.
Search and indexing power saving modes (Vista and later, DC)	Allows you to balance indexing activity with power consumption.
	Defines the system power action to initiate when the system sleep button is pressed.

Parameter	Description
Sleep button action (Vista and later, AC)	
Sleep button action (Vista and later, DC)	Defines the system power action to initiate when the system sleep button is pressed.
Sleep mode after idling at (%, Vista and later, AC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Sleep mode after idling at (%, Vista and later, DC)	Determines whether a computer can wake up from the specified sleep state by using the Real Time Clock (RTC).
Turn off hard disk after (seconds, AC)	Determines whether and when a device's hard disk is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the hard disk is turned off.
Turn off hard disk after (seconds, DC)	Determines whether and when a device's hard disk is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the hard disk is turned off.
Sleep after (seconds, Vista and later, AC)	Put the device into sleep mode after the defined number of seconds of inactivity. A value of zero indicates never sleep.
Sleep after (seconds, Vista and later, DC)	Put the device into sleep mode after the defined number of seconds of inactivity. A value of zero indicates never sleep.
Throttle Policy (AC)	The processor dynamic throttling policy to use. The following values are possible: • **None** : No processor performance control is applied. This policy always runs the processor at its highest possible performance level. This policy does not engage processor clock throttling, except in response to thermal events. • **Degrade** : Does not allow the processor to use any high voltage performance states. This policy engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events. • **Constant** : Does not allow the processor to use any high voltage performance states. This policy does not engage processor clock throttling, except in response to thermal events.

Parameter	Description
	• **Adaptive** : Attempts to match the performance of the processor to the current demand. This policy uses both high and low voltage and frequency states. This policy lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage. This policy engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events.
Throttle Policy (DC)	The processor dynamic throttling policy to use. The following values are possible: • **None** : No processor performance control is applied. This policy always runs the processor at its highest possible performance level. This policy does not engage processor clock throttling, except in response to thermal events. • **Degrade** : Does not allow the processor to use any high voltage performance states. This policy engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events. • **Constant** : Does not allow the processor to use any high voltage performance states. This policy does not engage processor clock throttling, except in response to thermal events. • **Adaptive** : Attempts to match the performance of the processor to the current demand. This policy uses both high and low voltage and frequency states. This policy lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage. This policy engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events.
USB selective suspend (Vista and later, AC)	Allows a device's port to be suspended when the device is not in use in order to conserve power.
USB selective suspend (Vista and later, DC)	Allows a device's port to be suspended when the device is not in use in order to conserve power.
Start menu button action (Vista and later, AC)	Specifies whether the computer should Do nothing or go to Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power off or Warm eject. It is not possible to use an action that is not supported by the device.
Start menu button action (Vista and later, DC)	Specifies whether the computer should **Do nothing** or go to **Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power off** or **Warm eject** . It is not possible to use an action that is not supported by the device.
Adaptive display (Vista and later, AC)	Specifies whether Windows automatically adjusts when the display is turned off based on mouse and keyboard usage. Check the box to activate.
	Specifies whether Windows automatically adjusts when the display is turned off based on mouse and keyboard usage. Check the box to activate.

Parameter	Description
Adaptive display (Vista and later, DC)	
Turn off display after (seconds, AC)	Determines whether and when a device's monitor is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the monitor is turned off.
Turn off display after (seconds, DC)	Determines whether and when a device's monitor is turned off to conserve power. Leave the box unchecked to disable the option. Check the option and define a specific value in minutes to define how long the device must be inactive before the monitor is turned off.

Create/Modify Global Power Policies

This step allows you to write global power policies that are not related to power schemes. This step will not work on Vista and later. A power scheme is a collection of settings that controls the power usage of your computer.

Parameters existing for AC and DC options will be explained only once, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop. All parameters need to be activated first, i.e., the left checkbox must be marked before the step will activate the parameter. Only then can the desired values be entered, selected or marked.

Parameter	Description
Broadcast capacity resolution	Defines the resolution of change in current battery capacity that should cause the system to be notified of a system power state changed event. Check the box to activate it and enter the desired value in the text field.
Enable multiple battery display	Enables or disables multiple battery display in the system power meter.
Require a password on wakeup	Enables or disables requiring password login when the system resumes from standby or hibernate.
Enable systray battery-meter	Enables or disables the battery meter icon in the system tray. When this option is deactivated, the battery meter icon is not displayed on the desktop.
Enable monitor dimming	Enables or disables support for dimming the video display when the system changes from running on AC power to running on battery power.
Enable Wake-on-ring	Enables or disables wake on ring support.
Lid close action (AC)	Defines the system power action to initiate when the system lid switch is closed when running on AC power.
Lid close action (DC)	Defines the system power action to initiate when the system lid switch is closed when running on DC power.

Parameter	Description
Lid open wake (AC)	Defines the maximum power state from which a lid-open event should wake the system when running on AC power.
Lid open wake (DC)	Defines the maximum power state from which a lid-open event should wake the system when running on DC power.
Power button action (AC)	Defines the system power action to initiate when the system power button is pressed when running on AC power.
Power button action (DC)	Defines the system power action to initiate when the system power button is pressed when running on DC power.
Power level 0 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 0 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 0 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 0 policy action	Defines the action to take for this battery discharge policy.
Power level 1 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 1 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 1 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 1 policy action	Defines the action to take for this battery discharge policy.
Power level 2 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 2 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 2 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.
Power level 2 policy action	Defines the action to take for this battery discharge policy.
Power level 3 battery level	The battery capacity for this battery discharge policy, expressed as a percentage.
Power level 3 enabled	If this option is marked, the alarm should be activated when the battery discharges below the value set in the battery level parameter.
Power level 3 minimum system state	Defines the minimum system sleep state to enter when the battery discharges below the value set in the battery level parameter.

Parameter	Description
Power level 3 policy action	Defines the action to take for this battery discharge policy.
Sleep button action (AC)	Defines the system power action to initiate when the system sleep button is pressed when running on AC power.
Sleep button action (DC)	Defines the system power action to initiate when the system sleep button is pressed when running on DC power.

Create/Modify Power Plan

This step allows you to create a new power plan. It has parameters to be defined, whereby the AC parameter is applicable to devices with a constant source of alimentation, such as a desktop or a laptop connected to an electrical plug, the DC parameter is applicable to devices running on battery power, such as an unconnected laptop.

Parameter	Description
Active Power Plan	Defines, if the newly defined power plan is to be activated right away and thus is the default plan.
Power Plan Description	A longer textual description of the new power plan, such as after how much time the components is switched off.
Hard Disc Drive Off (AC)	Defines when the hard disk of the device is to be switched off when running on AC power.
Hard Disc Drive Off (DC)	Defines when the hard disk of the device is to be switched off when running on DC power.
Hibernate System (AC)	Defines when the system is put in hibernation when running on AC power.
Hibernate System (DC)	Defines when the system is put in hibernation when running on DC power.
Monitor Off (AC)	Defines when the screen of the device is to be switched off when running on AC power.
Monitor Off (DC)	Defines when the screen of the device is to be switched off when running on DC power.
Power Plan Name	The name for the new power plan.
System Suspend (AC)	Defines when the system is suspended when running on AC power.
System Suspend (DC)	Defines when the system is suspended when running on DC power.

Define Power Plan

This step defines the default power plan which will be used.

Parameter	Description
Replacement Power Plan	Enter into this field the name of the power plan which is to be used by default.

Delete Power Plan

This step deletes an existing power plan and specify the new default plan if appropriate.

Parameter	Description
Power Plan Name to Delete	Enter the name of the power plan to be deleted.
Replacement Power Plan	Enter into this field the name of the power plan which is to be used by default.

Hibernate

This step allows you to immediately put the target device in hibernation.

Parameter	Description
Force	Check this box to force the device to go in hibernation, even if there is activity on the device.

Suspend

This step allows you to immediately put the target device in stand-by mode. It is applicable to Windows and MacOS devices.

Parameter	Description
Force	Check this box to force the device to go in suspend mode, even if there is activity on the device. This parameter is only applicable to Windows devices.

Update Power Management Inventory

This step launches an update of the power management inventory of the device. It is applicable to Windows only.

Parameter	Description
Bypass Transfer Window	Check this box to bypass the transfer window defined for the device. This means that the upload takes place immediately without taking into account any bandwidth definitions. It can only be activated if the **Upload after update** option is activated.
Differential Upload	Specifies if the inventory is to be completely replaced which each upload when differences are detected or only with the delta, that is, the modifications of the inventory.
Force Upload	Defines if the requested inventory is sent regardless of whether it has changed since the last upload. If the box is checked the inventory is uploaded, if it is unchecked the requested inventory is only uploaded if it has changed. The **Force Upload** option can only be activated if the **Upload after update** option is activated.
Upload after update	Defines whether the resulting inventory should be uploaded immediately after being updated. If the box is left unchecked the inventory is not uploaded immediately.

Process Management

- Advanced Process Execution Check
- Check Running Process
- End Processes
- Execute Program
- Execute Program As User

- Process Black List
- Process White List

Advanced Process Execution Check

This step checks if a process is running and waits for the defined maximum wait time for the process to run. If after the maximum wait time the process is still not running, an event is created.

Parameter	Description
Maximum Wait Time (min)	Defines the time to wait for the process to run in minutes.
Process Name	Defines the name of the process to look for. Be sure to enter the name exactly as it is shown in the Task Manager/Processes view, otherwise the operational rule does not find it.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Check Running Process

This step checks if a process is running on the client and stops it on demand (Windows only). An event is generated if the process cannot be found or terminated.

Parameter	Description
Process Name	Defines the name of the process to look for. Be sure to enter the name exactly as it is shown in the **Task Manager /Processes** view, otherwise the operational rule does not find it.
End Process If Found	Check this box if the operational rule is to stop the process if it found it.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

End Processes

This step terminates one or more processes if they are running at step execution time. No event will be generated if a process cannot be ended because it was not running.

Parameter	Description
Process Names	Contains a list of processes to be terminated if they are running. The process names are separated by commas.

Execute Program

This step starts a program on the target devices.

Parameter	Description
Executable Path	Defines the complete command line including parameters to be executed. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Wait for End of Execution	Check this parameter if the step is to wait for the end of the operation before declaring its execution terminated.
Background Mode	Check this box if the program is to be executed in the background without the remote user being aware of it.
Run Program in its Context	Defines if the program is to be launched from its installation location or the agent directory. To launch the application in the agent context this option must be deactivated.
Valid Return Codes	The list of valid return codes for this program execution, separated by commas.
Use a shell	Check this box to run the command in a shell. Output redirection is functional when shell is used.

Execute Program As User

This step allows you to start a program on the target device as a specific user.

Parameter	Description
Executable Path	Defines the complete command line including parameters to be executed. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Wait for End of Execution	Check this parameter if the step is to wait for the end of the operation before declaring its execution terminated.
Background Mode	Check this box if the program is to be executed in the background without the remote user being aware of it.
Run Program in its Context	Defines if the program is to be launched from its installation location or the agent directory. To launch the application in the agent context this option must be deactivated.
Valid Return Codes	The list of valid return codes for this program execution, separated by commas.
Domain	Enter the name of the domain in which the device has to be connected to execute the program.
User Login	Enter into this field the login name of the user as which the program is to be executed. If this field remains empty, the program is executed as the user currently logged on to MyApps, otherwise it is run as LocalSystem.
User Password	Enter here the password corresponding to the specified login.

Parameter	Description
Use a shell	Check this box to run the command in a shell. Output redirection is functional when shell is used.

Process Black List

This step kills all processes which are specified in the below listed specific text file, for example, BlackList.txt.

Parameter	Description
Authorized User Accounts	Enter all user accounts to which the black list of processes does NOT apply, that is, for which the running processes are not limited to those listed in the file. The user accounts must be separated with a comma (,).
Verification Interval (sec)	Defines the interval in seconds at which the agent checks for all concerned user accounts if forbidden processes are running. This value allows you to define a more frequent execution than the most repetitive execution possible for a step, that is, every minute.
Forbidden Processes File	Enter the complete path to the text file containing the forbidden processes.

Process White List

This step kills all processes currently running, apart from a few kernel and the Client Management processes as well as those which are specified in a specific text file, for example, WhiteList.txt.

Parameter	Description
File Containing the Allowed Processes	Enter the complete path to the text file containing the allowed processes.
Authorized User Accounts	Enter all user accounts to which the white list of processes does NOT apply, that is, for which the running processes are not limited to those listed in the file. The user accounts must be separated with a comma (,).
Verification Interval (sec)	Defines the interval in seconds at which the agent checks for all concerned user accounts if forbidden processes are running. This value allows you to define a more frequent execution than the most repetitive execution possible for a step, that is, every minute.

Security Settings Inventory steps

This group of steps is concerned with establishing the Security Settings Inventory for your network. Specific restrictions are noted with the individual steps. The steps specifically concerned with Microsoft Windows Security Center and options also provide explanations as to the default Windows values and what they do.

- Account Policy
- Audit Policy
- Clean Security Settings Inventory
- Domain Member Policy
- Find Service Status

- IPTables Parameters
- Security Center Anti-Spyware
- Security Center Antivirus
- Security Center Firewalls
- Interactive Login Policy
- List of Windows Services
- Log File Policy
- Microsoft Network Client Policy
- Microsoft Network Server Policy
- Network Access Policy
- Network Security Policy
- Number of Administrator Accounts
- Number of Open Windows Sessions
- Open Ports
- Peripheral Device Policy
- Process List
- Recovery Console Policy
- Run Level Commands
- Shared Resources
- System Policy
- USB Drivers
- USB Storage Status
- Unix Service Status
- User Account Control Policy
- Windows Patches
- Windows Registry Extracts
- Windows Start-up Programs
- Windows Update Status

Account Policy

This step collects the settings of the Account Policy and stores them in the security settings inventory.

Parameter	Description
Limit Local Account Use of Blank Passwords to Console Login Only	Determines whether local accounts that are not password protected can be used to login from locations other than the physical computer console. If enabled, then local accounts that are not password protected is only able to log on at the computer's keyboard. Does not apply to guest accounts.
Account Lockout Duration	The amount of time, in minutes, that account lockout is enforced. If you set the **Account Lockout Duration** registry value to *0* , the account is permanently locked out until either an administrator or a user who has a delegated account resets the account.

Parameter	Description
Reset Account Lockout Counter After	You can use the **Reset Account Lockout Counter After** setting to help mitigate lockout issues that are initiated by users. When you enable this setting, the bad password attempt is removed from the server after the number of minutes that you set.
Account Lockout Threshold	The number of times that the user, computer, service, or program can send a bad password during login authentication before the account is locked out. You can adjust the **Account Lockout Threshold** value to prevent both brute force and dictionary attacks, but you can set the value too low to capture user error and other non-attack errors. If you set the **Account Lockout Threshold** value to *0* , no account lockouts occur on the domain.
Maximum Password Age	Determines the period of time (in days) that a user can use their password before the computer requires the user to change it. You can set passwords to expire in between 1 and 999 days, or you can specify that passwords never expire by setting the number of days to 0.
Minimum Password Age	Determines the period of time (in days) that a password must be used before the user can change it. You can set the value to between 1 and 999 days, or allow immediate changes by setting the number of days to 0. If you do not set a minimum password age, users can repeatedly cycle through passwords until they are able to use an old favorite password. This could allow users to circumvent established password policy.
Minimum Password Length	Defines the number of characters a password must at least consist of. The value can be set between 0 and 14 characters. Each additional character increases the total possible password permutations. However, if you set the value to 0, blank passwords are not permitted.
Enforce Password History	Check this box to prevent users from repeatedly using the same password. When you use the password history feature, a user is prevented from using passwords that they used in the past, up to the number of passwords that you specify. You can configure Windows to retain between 0 and 24 passwords by using the *Password History* feature. Microsoft recommends that you set the password history to the maximum value to help ensure the least amount of password reuse by users.

Audit Policy

This step collects the settings of the Audit Policy and stores them in the security settings inventory.

Parameter	Description
Audit Attempts to Modify Accounts and Change Passwords	Determines whether to audit each event of account management on a computer. Examples of account management events include: a user account or group is created, changed, or deleted; a user account is renamed, disabled, or enabled; a password is set or changed. If activated all successes and failures are audited. Success audits generate an audit entry when any account management event is successful. Failure audits generate an audit entry when any account management event fails.
Force Audit Policy Subcategory to Override Audit Policy Category settings (Vista and later)	Prevents domain-based audit policy from overwriting the more detailed audit policy settings on Windows Vista client computers.
Shut Down System Immediately if Unable to Log Security Audits	Determines whether the system should shut down if it is unable to log security events. If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error occurs: *STOP: C0000244 {Audit Failed} An attempt to generate a security audit failed.* To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired.
Audit Specific Events	

Parameter	Description
	Determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. If activated all successes and failures are audited. Success audits generate an audit entry when the process being tracked is a success. Failure audits generate an audit entry when the process being tracked fails.
Audit Access of Global System Objects	Determines whether access of global system objects is audited. When this policy is enabled, it causes system objects such as mutexes, events, semaphores, and DOS Devices to be created with a default system access control list (SACL). If the Audit object access audit policy is also enabled, then access to these system objects is audited.
Audit Attempts to Log On to or Log Off of System	Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account. If activated all successes and failures are audited.
Audit Attempts to Access Defined Objects	Determines whether to audit the event of a user accessing an object (for example, file, folder, registry key, printer, and so forth) which has its own system access control list (SACL) specified.
Audit Attempts to Change Policy Object Rules	Determines whether to audit every incidence of a change to user rights assignment policies, audit policies, or trust policies.
Audit Attempts to Use Privileges	Determines whether to audit each instance of a user exercising a user right.
Audit Use of Backup and Restore Privileges	Determines whether to audit every use of user rights including Backup and Restore
Audit Events that Affect System Security	Defines whether to audit when a user restarts or shuts down the computer; or an event has occurred that affects either the system security or the security log. If activated all successes and failures are audited. Success audits generate an audit entry when a system event is successfully executed. Failure audits generate an audit entry when a system event is unsuccessfully attempted.

Clean Security Settings Inventory

This step deletes entries in the inventory for security settings. Be aware that you need access to the SecurityInventory.xml on the device to be cleaned as the values to be entered into the fields of the step are those of the .xml file.

Parameter	Description
Delete All	Check this box if all entries of a specific name or type in the security settings inventory are to be deleted.
Object Name	The value <OBJECT name="<value>"> of the entry/entries to be deleted from the .xml file. As there may be several objects with the same name of different types all entries of this name will be deleted if you do not specify the respective type in the field above. It is possible to use the wildcard characters *?* for a single letter and *** for several letters.
Object Type	The value <OBJECT type="<value>"> of the entry/entries to be deleted from the .xml file. As there may be several objects of the same type with different names all entries of this type will be deleted if you do not specify the respective name in the field below. It is possible to use the wildcard characters *?* for a single letter and *** for several letters.

Domain Member Policy

This step collects the settings of the Domain Policy and stores them in the security settings inventory.

Parameter	Description
Disable Machine Account Password Changes	Determines whether a domain member periodically changes its computer account password. If this setting is enabled, the domain member does not attempt to change its computer account password. If this setting is disabled, the domain member attempts to change its computer account password as specified by the setting for Domain Member: Maximum age for machine account password.
Maximum Machine Account Password Age	Determines how often a domain member attempts to change its computer account password.
Digitally Encrypt or Sign Secure Channel Data (always)	Determines whether the computer always digitally encrypts or signs secure channel data. If this policy is enabled, all outgoing secure channel traffic must be either signed or encrypted. If this policy is disabled, signing and encryption are negotiated with the domain controller. This option should only be enabled if all of the domain controllers in all the trusted domains support signing and sealing. Note: If this parameter is enabled, then **Secure channel: Digitally sign secure channel data (when possible)** is automatically enabled.
Digitally Encrypt Secure Channel Data (if possible)	Determines whether the computer always digitally encrypts or signs secure channel data. If this policy is enabled, all outgoing secure channel traffic should be encrypted. If this policy is disabled, outgoing secure channel traffic is not encrypted.
Digitally Sign Secure Channel Data (if possible)	Determines whether the computer always digitally encrypts or signs secure channel data. If this policy is enabled, all outgoing secure channel traffic should be signed. If this policy is disabled, no outgoing secure channel traffic is signed.
Require Strong Session Key	Check this box if all outgoing secure channel traffic are to require a strong (Windows 2000 or later) encryption key. If this policy is disabled, the key strength is negotiated with the DC. This option should only be enabled if all of the DCs in all trusted domains support strong keys.

Find Service Status

This step uploads a list of status of specific services to the security settings inventory, which may be defined via the step's parameters. This step is only applicable to Windows devices.

Parameter	Description
Search in Service Path	Check this box if the string is to be looked for in the service directory path.
String to Find	Enter the string which is to identify the desired service(s). This string can be a pattern or a regular expression.

Parameter	Description
Search in Service Description	Check this box if the string is to be looked for in the service directory path.
Search the Display Name of the Service	Check this box if the string is to be looked for in the description of the service.
Search in Service Name	Check this box if the string is to be looked for in the name of the service.

IPTables Parameters

This step collects the list of iptables Firewall filters which are configured on the device and saves those in the security settings inventory. This step is only applicable to Unix environments.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Security Center Anti-Spyware

This step collects the WMI information concerning the Security Center anti-spyware and stores it in the Security Settings (Windows Vista and later).

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Security Center Antivirus

This step collects all WMI information concerning the Security Center antivirus software programs and saves it in the Security Settings. This step is applicable only to Windows devices.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Security Center Firewalls

This step collects all WMI information concerning the Security Center firewalls and saves it in the Security Settings. This step is only applicable to Windows devices.

Parameter	Description
Collect Windows Firewall Information If Present	Check this box if the step is to collect and display any available information for the installed firewall. This retrieves information for both the *Standard* and the *Domain* profile.
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Interactive Login Policy

This step collects the settings of the Interactive Login Policy and stores them in the security settings inventory.

Parameter	Description
Automatic Login	Determines whether the user is automatically logged on after the device is started.
Number of Previous Logins to Cache	Determines the number of times a user can log on to a Windows domain using cached account information. In this policy setting, a value of 0 disables login caching. Any value above 50 only caches 50 login attempts.
Do Not Require Ctrl + Alt + Del	Determines whether pressing CTRL+ALT+DEL is required before a user can log on. If this policy is enabled on a computer, a user is not required to press CTRL+ALT+DEL in order to log on. Not having to press CTRL+ALT+DEL leaves the user susceptible to attacks that attempt to intercept the user's password.
Prompt User to Change Password before Expiration	Defines how far in advance Windows 2000 should warn users that their password is about to expire. By giving the user advanced warning, the user has time to construct a sufficiently strong password.
Do Not Display Last User Name	Determines whether the name of the last user to login to the computer is displayed in the Windows login screen. If this policy is enabled, the name of the last user to successfully log on is not displayed in the Log On to Windows dialog box. If this policy is disabled, the name of the last user to login is displayed. This policy is defined by default in **Local Computer Policy** .
Smart Card Removal Behavior	Determines what should happen when the smart card for a logged-on user is removed from the smart card reader. If **Lock Workstation** is specified, then the workstation is locked when the smart card is removed allowing users to leave the area, take their smart card with them, and still maintain a protected session. If **Force Logoff** is specified, then the user is automatically logged off when the smart card is removed.
Message Title for Users Attempting to Log on	Allows the specification of a title to appear in the title bar of the window that contains the message text for users attempting to log on. For servers, this policy is enabled but there is no default text specified.
Message Text for Users Attempting to Log on	Specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, such as to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. For servers, this policy is enabled but there is no default text specified.
Require Domain Controller Authentication to Unlock Workstation	Login information must be provided to unlock a locked computer. For domain accounts, determines whether a domain controller must be contacted to unlock a computer. If this setting is disabled, a user can unlock the computer using cached credentials. If this setting is enabled, a domain controller must authenticate the domain account that is being used to unlock the computer.

List of Windows Services

This step collects the list of Windows services installed and running on the target and saves it in the security settings inventory. This step is applicable only to Windows devices.

Parameter	Description
Include Stopped Services	Check this box if not only running but also all stopped services installed on the device are to be included in the list.

Log File Policy

This step collects the settings of the Log File Policy and stores them in the security settings inventory.

Parameter	Description
Prevent Local Guest Groups from Accessing Application Log File	Determines if guests are prevented from accessing the application event log, which contains program errors and missing data information. This security setting affects only computers running Windows 2000, Windows XP and Windows Server 2003.
Keep/Overwrite Application Log File	Determines the number of seconds' worth of events to be retained for the application log once the log arrives at its maximum size.
Maximum Application Log File Size	Specifies the maximum size of the application event log, which has a maximum of 4 GB. Log file sizes must be a multiple of 64 KB.
Prevent Local Guest Groups from Accessing Security Log File	Determines if guests are prevented from accessing the security event log. This security setting affects only computers running Windows 2000, Windows XP and Windows Server 2003. A user must possess the Manage auditing and security log user right to access the security log.
Keep/Overwrite Security Log File	Determines the number of seconds' worth of events to be retained for the security log once the log arrives at its maximum size.
Maximum Security Log File Size	Specifies the maximum size of the security event log, which has a maximum size of 4 GB. Log file sizes must be a multiple of 64 KB.
Prevent Local Guest Groups from Accessing System Log File	Determines if guests are prevented from accessing the system event log, which contains startup information, shutdown information, and driver information. This security setting affects only computers running Windows 2000, Windows XP and Windows Server 2003. A user must possess the Manage auditing and security log user right to access the security log.
Keep/Overwrite of System Log File	Determines the number of seconds' worth of events to be retained for the system log once the log arrives at its maximum size.
Maximum System Log File Size	Specifies the maximum size of the system event log, which has a maximum size of 4 GB. Log file sizes must be a multiple of 64 KB.

Microsoft Network Client Policy

This step collects the settings of the Microsoft Network Client Policy and stores them in the security settings inventory.

Parameter	Description
Digitally Sign Communications (if server agrees)	Check this box to cause the Windows 2000 Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing.
Send Unencrypted Password to Third-party SMB Servers	Check this box if the Server Message Block (SMB) redirector is allowed to send clear-text passwords to non-Microsoft SMB servers which do not support password encryption during authentication.
Digitally Sign Communications (always)	Determines whether the computer always digitally signs client communications. The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a *man-in-the-middle* attack, and supports message authentication, which prevents active message attacks. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing use the packet signing protocol during all subsequent sessions.

Microsoft Network Server Policy

This step collects the settings of the Microsoft Network Server Policy and stores them in the security settings inventory.

Parameter	Description
Digitally Sign Communications (if client agrees)	If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default on workstation and server platforms in **Local Computer Policy** . This policy is enabled by default on domain controllers in the **Default Domain Controllers Group Policy** object (GPO).
Idle Time before Suspending Session	Determines the amount of continuous idle time that must pass in a Server Message Block (SMB) session before the session is disconnected due to inactivity. For this policy setting, a value of *0* means to disconnect an idle session as quickly as reasonably possible. The maximum value is *0xFFFFFFFF* , which means disabled.
Disconnect Clients When Login Hours Expire	Determines whether to disconnect users that are connected to the local machine outside of their user account's valid login hours. This setting affects the Server Message Block (SMB) component of a Windows 2000 server. When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's login hours expire. If this policy is disabled, an established client session is allowed to be maintained after the client's login hours have expired.
Digitally Sign Communications (always)	Determines whether the computer always digitally signs client communications. If SMB signing is required on a server, then a client is not able to establish a session unless it is at least enabled for SMB signing. If this policy is disabled, it does not require the SMB client to sign packets. This policy is defined by default in **Local Computer Policy** , where it is disabled by default.

Network Access Policy

This step collects the settings of the Network Access Policy and stores them in the security settings inventory.

Parameter	Description
	Determines whether **Stored User Names and Passwords** saves passwords, credentials, or .NET Passports for later use when it gains domain authentication. If it is enabled, this setting prevents the **Stored User Names and Passwords** from storing passwords and credentials. Note: When configuring this security setting, changes do not take effect until you restart Windows.

Parameter	Description
Do Not Allow Storage of Credentials for Network Authentication	
"Everyone" Permissions to be Applied to Anonymous Users	Determines how network logins using local accounts are authenticated. If this setting is set to *Classic* , network logins that use local account credentials authenticate by using those credentials. If this setting is set to *Guest only* , network logins that use local accounts are automatically mapped to the Guest account. The Classic model allows fine control over access to resources. By using the Classic model, you can grant different types of access to different users for the same resource. By using the Guest only model, you can have all users treated equally.
Sharing and Security Model for Local Accounts	Determines how network logins using local accounts are authenticated. If this setting is set to *Classic* , network logins that use local account credentials authenticate by using those credentials. If this setting is set to *Guest only* , network logins that use local accounts are automatically mapped to the Guest account. The Classic model allows fine control over access to resources. By using the Classic model, you can grant different types of access to different users for the same resource. By using the Guest only model, you can have all users treated equally.
Do Not Allow Anonymous Enumeration of SAM Accounts	Determines what additional permissions is granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust.
Do Not Allow Anonymous Enumeration of SAM Accounts and Shares	Determines whether anonymous enumeration of SAM accounts and shares is allowed. If you do not want to allow anonymous enumeration of SAM accounts and shares, then enable this policy.

Network Security Policy

This step collects the settings of the Network Security Policy and stores them in the security settings inventory.

Parameter	Description
LDAP Client Signing Requirements	Determines the level of data signing that is requested on behalf of clients issuing LDAP BIND requests.
LAN Manager Authentication Level	Determines which challenge/response authentication protocol is used for network logins.
Do Not Store LAN Manager Hash Value on Next Password Change	Determines if, at the next password change, the LAN Manager (LM) hash value for the new password is stored. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT hash. Since the LM hash is stored on the local computer in the security database the passwords can be compromised if the security database is attacked.

Number of Administrator Accounts

This step finds all administrator accounts that exist on the target device and saves them in the security settings inventory.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Number of Open Windows Sessions

This step collects the number of open Windows Sessions and saves it in the security settings inventory. This step is applicable only to Windows devices.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Open Ports

This step collects the list of open TCP and/or UDP ports and saves it in the security settings inventory.

Parameter	Description
Protocol	Select the protocol, either TCP or UDP, for which all open ports are to be found.
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Peripheral Device Policy

This step collects the settings of the Device Policy and stores them in the security settings inventory.

Parameter	Description
Restrict CD-ROM Access to Locally Logged-On User Only	Determines whether a CD-ROM is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable CD-ROM media. If no one is logged on interactively, the CD-ROM may be shared over the network. If this policy is disabled, then the local user and remote users can access the CD-ROM simultaneously.
Unsigned Driver Installation Behavior	Determines what should happen when an attempt is made to install a device driver (by means of the Windows 2000 device installer) that has not been certified by the Windows Hardware Quality Lab (WHQL).
	Determines whether removable floppy media is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable floppy media. If no one is logged on interactively, the floppy media may be shared over the network. If this policy is disabled, then the local user and remote users can access the floppy media simultaneously.

Parameter	Description
Restrict Floppy Access to Locally Logged-On User Only	
Unsigned Non-driver Installation Behavior	Defines what should happen when an attempt is made to install any non-device driver software that has not been certified.
Prevent Users from Installing Printer Drivers	Determines whether members of the *Users* group are prevented from installing print drivers. Note: This policy setting does not affect Power Users.
Allow to Format and Eject Removable Media	Determines who is allowed to eject removable NTFS media from the computer. This policy is defined by default in **Local Computer Policy** . This policy setting can be modified to provide any interactive user with the ability to eject removable NTFS media from the computer.
Allow to undock without Having to Log On	Determines whether a portable computer can be undocked without having to log on. If this policy is enabled, login is not required and an external hardware eject button can be used to undock the computer. If disabled, a user must log on and have the *Remove computer from docking station* privilege to undock the computer.

Process List

This step collects the list of active processes and saves it in the security settings inventory.

Parameter	Description
Process Path	Check this box if the path to the executable file of the process is to be added to the list.
Process User	Check this box if the name of the user who started the process is to be added to the list.

Recovery Console Policy

This step collects the settings of the Recovery Console Policy and stores them in the security settings inventory.

Parameter	Description
Allow Automatic Administrative Login	Check this box if the Recovery Console is not to require you to provide a password and automatically logs on to the system.
Allow Floppy Copy and Access to All Drives and All Folders	Enabling this option enables the Recovery Console SET command, which allows you to set the following Recovery Console environment variables: • **AllowWildCards** : Enable wildcard support for some commands (such as the DEL command). • **AllowAllPaths** : Allow access to all files and folders on the computer.

Parameter	Description
	• **AllowRemovableMedia** : Allow files to be copied to removable media, such as a floppy disk. • **NoCopyPrompt** Do not prompt when overwriting an existing file.

Run Level Commands

This step collects the list of commands executed for a specific run level and saves it in the security settings inventory. It is only applicable to the Unix environment.

Parameter	Description
Command	Select from this drop-down box the command which is to be found for the run level.
Run Level	Select the command which is to be found for the run level.
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Shared Resources

This step collects the list of shared resources and saves it in the security settings inventory.

No parameters need to be defined for this step.

System Policy

This step collects the settings of the System Policy and stores them in the security settings inventory.

Parameter	Description
Default Owner for Objects Created by Members of the Administrator Groups	Determines which users and groups have the authority to run volume maintenance tasks, such as *Disk Cleanup* and *Disk Defragmenter* .
Require Case-insensitivity for Non-Windows Subsystems	Determines whether case insensitivity is enforced for all subsystems. The Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as POSIX. If this setting is enabled, case insensitivity is enforced for all directory objects, symbolic links, and IO objects, including file objects. Disabling this setting does not allow the Win32 subsystem to become case sensitive.
Use FIPS Compliant Algorithms	Determines if the Transport Layer Security/Secure Sockets Layer (TL/SS) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, this means that the provider only supports the Transport Layer Security (TLS) protocol as a client and as a server (if applicable). It uses only the Triple DES encryption algorithm for the TLS traffic encryption, only the Rivest, Shamir, and Adleman (RSA) public key algorithm for the TLS key exchange and authentication, and only the Secure Hashing Algorithm 1 (SHA-1) for the TLS hashing requirements. For Encrypting File System Service (EFS), it supports only the Triple Data Encryption

Parameter	Description
for Encryption, Hashing, and Signing	Standard (DES) encryption algorithm for encrypting file data supported by the NTFS file system. By default, EFS uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key in the Windows Server 2003 family and DESX algorithm in Windows XP for encrypting file data. For Terminal Services, it supports only the Triple DES encryption algorithm for encrypting terminal services network communication.
Strengthen Default Permissions of Internal System Objects	Determines the strength of the default discretionary access control list (DACL) for objects.
Clear Virtual Memory Pagefile	Determines whether the virtual memory pagefile should be cleared when the system is shut down. Enabling this security option also causes the hibernation file (hiberfil.sys) to be zeroed out when hibernation is disabled on a laptop system. When this policy is disabled, the virtual memory pagefile is not cleared during system shutdown.
Allow System to be Shut Down without Having to Log On	Determines whether a computer can be shut down without having to log on to Windows. When this policy is enabled, the **Shut Down** command is available on the Windows login screen. When this policy is disabled, the option to shut down the computer does not appear on the Windows login screen. In this case, users must be able to log on to the computer successfully and have the **Shut down the system** user right in order to perform a system shutdown.

USB Drivers

This step finds the list of all installed USB drivers of any type and uploads this list to the security settings inventory. This step is only applicable to Windows devices.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

USB Storage Status

This step uploads the status of the USB storage to the security settings inventory. This step is only applicable to Windows devices.

Parameter	Description
Security Settings Inventory Instance Name	Enter the prefix for the instance name for the security settings inventory item, for example, entering *Instance* here labels the columns *Instance0, Instance1* , etc.

Unix Service Status

This step collects the status list of services of which the specified name corresponds to the searched parameter and saves it in the security settings inventory. It is only applicable to the Unix environment.

Parameter	Description
String to Find	Enter the string which is to identify the desired service(s). This string can be a pattern or a regular expression.

User Account Control Policy

This step collects the settings of the User Account Control Policy (UAC) and stores them in the security settings inventory. This step is only applicable to Windows Vista editions.

Parameter	Description
Admin approval mode for the built-in administrator account	Defines the behavior of **Admin Approval Mode** for the built-in administrator account: • **Enabled** : The built-in administrator logs on in **Admin Approval Mode** . By default, the consent prompt is displayed for any operation that requires elevation of privilege. • **Disabled** : The built-in administrator logs on in XP-compatible mode and run all applications by default with full administrative privilege.
Only elevate executables that are signed and validated	Enforces public key infrastructure (PKI) signature checks on any interactive application that requests elevation of privilege. Enterprise administrators can control which administrative applications are allowed through the certificates in the local computer's Trusted Publishers certificate
Behavior of elevation prompt for administrators in admin approval mode	Determines the behavior of the elevation prompt for administrators: • **Prompt for consent** : An operation that requires elevation of privilege prompts an administrator in **Admin Approval Mode** to click either **Continue** or **Cancel** . If the administrator clicks **Continue** , the operation continues with the administrator's highest available privilege. This option allows users to enter their user name and password to perform a privileged task. • **Prompt for credentials** : An operation that requires elevation of privilege prompts an administrator in **Admin Approval Mode** to enter a user name and password. If valid credentials are entered, the operation continues with the applicable privilege. • **Elevate without prompting** : This value allows an administrator in **Admin Approval Mode** to perform an operation that requires elevation without providing consent or credentials. This is the least secure option.
Behavior of the elevation prompt for standard users	Determines the behavior of the elevation prompt for standard users: • **Prompt for credentials** : An operation that requires elevation of privilege prompts the user to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. • **Automatically deny elevation requests** : A standard user receives an access-denied error message when an operation that requires elevation of privilege is attempted. Most enterprises running workstations as standard user configure this policy to reduce help desk calls.
Detect application installations and prompt for elevation	Determines the behavior of application installation detection for the computer:

Parameter	Description
	• **Enabled** : Detects application installation packages that require an elevation of privilege to install and displays the configured elevation prompt. • **Disabled** : Enterprises running standard user workstations that use delegated installation technologies such as **Group Policy Software Installation** or **Systems Management Server** (SMS) automatically disables this setting. In this case, installer detection is unnecessary and thus not required.
Run all administrators in admin approval mode	Determines the behavior of all UAC policies for the entire system: • **Enabled** : **Admin Approval Mode** and all other UAC policies are dependent on this option being enabled. Changing this setting requires that the computer be restarted. • **Disabled** : The **Admin Approval Mode** user type and all related UAC policies is disabled. If the **Disabled** value is selected, the **Security Center** provides notification that the overall security of the operating system has been reduced.
Switch to secure desktop when prompting for elevation	Determines whether the elevation prompt appears on the interactive user's desktop or the secure desktop: • **Enabled** : All elevation prompts appear on the secure desktop. • **Disabled** : All elevation prompts appear on the interactive user's desktop.
Only elevate UIAccess applications that are installed in secure locations	Enforces the requirement that applications requesting to be run with a UIAccess integrity level must reside in a secure location on the file system. Secure locations are limited to the following directories: ?Program Files (and subfolders) ?WindowsSystem32r- ?Program Files (x86) (and subfolders, in 64-bit versions of Windows only).
Virtualize file and registry write failures to per-user locations	Enables the redirection of application write failures to defined locations in both the registry and file system. This feature mitigates those applications that historically ran as administrator and wrote runtime application data to protected locations (*%ProgramFiles%, %Windir%, %Windir%system32, or HKLMSoftware...*).

Windows Patches

This step collects the list of all Windows hotfixes and patches installed on the device and saves it in the security settings inventory. This step is only applicable to Windows devices.

No parameters need to be defined for this step.

Windows Registry Extracts

This step uploads the values, subkeys and their values of a given Windows registry key to the security settings inventory. This step is only applicable to Windows. Please note that the execution of this step is very resource consuming.

No parameters need to be defined for this step.

Windows Start-up Programs

This step collects the list of programs which are started at Windows start-up on the device and saves it in the security settings inventory. This step is applicable only to Windows devices.

No parameters need to be defined for this step.

Windows Update Status

This step verifies the status of Windows Update and uploads its configuration to the security settings inventory. This step is only applicable to Windows devices.

No parameters need to be defined for this step.

Software Distribution steps

The software distribution group contains all steps concerned with the distribution of software packages to be installed throughout your network.

- Install Package

Install Package

This step installs a package on the target devices. The package contains a file named INSTALL.CHL which will be extracted and called to carry out the actual installation on the local target.

If a reboot is scheduled, you can define the reboot parameters and message, which may also be localized. The logo of the message box may be customized as well. For this you only need to store the following customized images in their exact sizes in the *//data//core//res* directory of the BCM agent: FullSized.bmp (575 x 575 pixels), MediumSized.bmp (575 x 510 pixels), SmallSized.bmp (575 x 455 pixels), RebootAfterLogOut.bmp (575 x 275 pixels).

If files were locked during the installation and thus could not be updated on a device, an error message appears in the Error Details column of the assigned devices view of the operational rule installing the package. In this case, the files in question will be updated during the next reboot.

Parameter	Description
Package Name	Defines the name of the package to be sent to the targets. The package is defined with its relative or full path. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Package Checksum	Contains the checksum of the package which is stored in a directory next to the package directory on the master server. If the checksum of the package and the stored value of the package checksum are not identical the step fails.
Valid Return Codes	The list of valid return codes for this package, separated by commas.

Parameter	Description
Reboot if needed	Check this box if the target device must be rebooted to finish the installation of the package. If this box is left unckecked and the installation requires a reboot you must reboot the device manually. In this case the operational rule finishes successfully and you can find an entry in the **Error Details** column, reminding you that a final device reboot is required.nIf the MSI installation itself is executed forcing a reboot (for example via /forcerestart), any assigned reboot windows or maximum restart limits are ignored.
Check Package Integrity	Check this parameter if the integrity of the package is to be verified via its checksum before extracting the data.
Deferred Reboot	Check this box to activate the deferred reboot option. This allows the user to postpone the necessary reboot, if it appears at an inconvenient time. You can then define how often and for how long the user can postpone the reboot in the next two boxes. If you leave the box unchecked, the reboot is executed as scheduled.
Postpone Count	Defines how often the user may decide to postpone the reboot for the below specified number of minutes.
Postpone Delay (min)	The interval in minutes that the reboot may be postponed.
Timeout before auto-accept (min)	The number of minutes defines the timeframe the user has to accept or postpone the reboot in the displayed message. If the user does not react before the counter expires, the reboot proceeds as defined.
Localized Message 1	To display the message in the language of the local operating system enter the localized message here in the format *CodePage : Message* . The CodePages represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Localized Message 2	Defines the localized message for an alternative local operating system language in the format *CodePage : Message* . The CodePages represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Default Text	Enter the default message text of the message box, that is displayed if the local operating system is not one of those defined below.
Force Reboot if Client is Locked	Check this box if the reboot is to be executed even if the client is locked. Otherwise the reboot waits until the client becomes unlocked.

Tools steps

This group of steps includes any type of steps usable as 'tools' for other operations.

- Change the Lock Window Message
- Check Agent Version
- Verify that the Device is Not the Master
- Check Operating System
- Execute Operational Rule
- Generate Custom Alert
- Lock Device

- Reboot Device
- Send Extended Mail
- Send Mail
- Send SNMP Traps
- Shutdown Device
- Unlock Device
- Verify Last Device Boot Time
- Wait
- Wait for Days
- Wake on LAN

Change the Lock Window Message

This step customizes the text of the message box that appears when locking the remote device.

Parameter	Description
Message Text	Enter into this field the text to be displayed in the message box on the screen.

Check Agent Version

This step checks the version number of the currently installed agent.

Parameter	Description
Version	Enter into this field the version number that the agent should have.

Verify that the Device is Not the Master

This step verifies that the device is not the Master.

No parameters need to be defined for this step.

Check Operating System

This step verifies if the operating system of the target device corresponds to one of those selected in the step's list.

Parameter	Description
Windows 10 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 10. You may select more than one OS.
Windows 10 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 10. You may select more than one OS.
Windows 8.1 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 8.1 . You may select more than one OS.
Windows 8.1 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 8.1. You may select more than one OS.
Windows 8 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 8. You may select more than one OS.

Parameter	Description
Windows 8 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 8. You may select more than one OS.
Windows 7 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 7. You may select more than one OS.
Windows 7 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 7. You may select more than one OS.
Windows 2016 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64-bit Windows 2016. You may select more than one OS.
Windows 2012 R2 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 2012 R2. You may select more than one OS.
Windows 2012 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 2012. You may select more than one OS.
Windows 2008 R2 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 2008 R2. You may select more than one OS.
Windows 2008 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows 2008. You may select more than one OS.
Windows 2008 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 2008. You may select more than one OS.

Pre-Windows 7 Versions

Parameter	Description
Windows Vista (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows Vista. You may select more than one OS.
Windows Vista (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows Vista. You may select more than one OS.
Windows XP (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Windows XP. You may select more than one OS.
Windows XP (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows XP. You may select more than one OS.
Windows ME	Check this box if the operating system to which the OS of the target device must correspond is Windows ME. You may select more than one OS.
Windows 98	Check this box if the operating system to which the OS of the target device must correspond is Windows 98. You may select more than one OS.
Windows 95	Check this box if the operating system to which the OS of the target device must correspond is Windows 95. You may select more than one OS.
Windows 2003 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64-bit Windows 2000. You may select more than one OS.
Windows 2003 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Windows 2003. You may select more than one OS.
Windows 2000	Check this box if the operating system to which the OS of the target device must correspond is Windows 2000. You may select more than one OS.

Parameter	Description
Windows NT	Check this box if the operating system to which the OS of the target device must correspond is Windows NT. You may select more than one OS.

Linux and Mac

Parameter	Description
Mac OS X	Check this box if the operating system to which the OS of the target device must correspond is a MAC OS.
Ubuntu (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Ubuntu. You may select more than one OS.
Ubuntu (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Ubuntu. You may select more than one OS.
Red Hat Linux Release 9 (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Red Hat Release 9. You may select more than one OS.
Red Hat Linux Release 9 (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Red Hat Release 9. You may select more than one OS.
Red Hat Enterprise Linux (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Red Hat Enterprise Linux. You may select more than one OS.
Red Hat Enterprise Linux (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Red Hat Enterprise Linux. You may select more than one OS.
CentOS (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Cent OS. You may select more than one OS.
CentOS (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Cent OS. You may select more than one OS.
SuSe (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit SUSE. You may select more than one OS.
SuSe (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit SUSE. You may select more than one OS.
Debian (64 bit)	Check this box if the operating system to which the OS of the target device must correspond is 64 bit Debian. You may select more than one OS.
Debian (32 bit)	Check this box if the operating system to which the OS of the target device must correspond is 32 bit Debian. You may select more than one OS.
Other Linux (32 & 64 bit)	Check this box if the operating system to which the OS of the target device must correspond is any other Linux version (32 and/or 64 bit) not specifically mentionend in this list. You may select more than one OS.
Solaris	Check this box if the operating system to which the OS of the target device must correspond is Solaris.

Execute Operational Rule

This step executes an operational rule on the target device. Be aware that the rule must already be available on the respective device, otherwise this step will fail.

Parameter	Description
Execute Once	Defines if the operational rule is to be executed only once or if it is to follow the schedule defined at the time of its assignment: • If the schedule for the operational rule exists but is deactivated it is activated. • If there is no more schedule assigned to the rule (this may be the case for example if the rule was schedule to execute three times, and these three executions have already been done), the original schedule is reactivated. In this case, if the original schedule is deactivated, this option does not reactivate it.
Operational Rule Name	Enter the name of the operational rule to be executed.

Generate Custom Alert

This step generates a custom alert.

Parameter	Description
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Lock Device

This step locks the mouse and keyboard of the device. Once the operation necessitating the lock is terminated, it must always be followed by the unlock step, otherwise the remote device will remain locked.

Parameter	Description
Message Text	Enter the text to be displayed in the message box on the screen.

Reboot Device

This step reboots a client with any of the supported operating systems. This step ignores if a reboot window is assigned to the device and does not increase the reboot count.

No parameters need to be defined for this step.

Send Extended Mail

This step sends an email with extended capabilities to a predefined address.

Parameter	Description
Attachments	Contains a list of files that are to be attached to the mail. The individual paths, preferable absolute paths, must be separated by commas (,) and must be local to the sending device.
Allow Login Protocol	Check this box if the mail server requires login authentication.
Allow Plain Text Protocol	Check this box if the mail server requires plain text authentication.
Allow CRAM-MD5 Protocol	Check this box if the mail server requires CRAM-MD5 authentication.
Password	The corresponding password. This parameter is mandatory if the option **Force Authentication** or **Authenticate if possible** is selected for the **Authentication Policy** parameter.
Authentication Policy	Defines if the mail server requires authentication for its communication.
User Name	Enter a valid login to the mail server. This may be any login, not necessarily that of the user defining his preferences in via these options. This field is mandatory if the option **Force Authentication** or **Authenticate if possible** is selected for the **Authentication Policy** parameter.
BCC	This parameter is optional as well and may contain the address of the blind carbon copy recipient to be added to the mail message.
CC	This parameter is optional and may contain the address of the carbon copy recipient to be added to the mail message.
Allow SSLv2 Protocol	Check this box if the mail server requires SSLv2 encryption.
Allow SSLv3 Protocol	Check this box if the mail server requires SSLv3 encryption.
Allow TLSv1 Protocol	Check this box if the mail server requires TLSv1 encryption.
Ciphering Policy	Defines if the mail server requires encryption for its communication.
From	Enter the name of the sender into this field.
Message Text	Enter into this field the text to be added to the message part of the mail message.
MIME Header	Allows you to define a MIME type, that is to be used for sending the mail. To indicate for example that the body of the message is in HTML format use the following header: *Content-Type:text/html; charset* .
Port Number	Enter the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** .
Server Name	Enter into this field the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** . The name may either be entered as the full or short network name such as *mail* or *mail.enterprise.starfleet.com* or as its IP address in dotted notation, for example, *213.2.146.1* or *2001:db8:85a3::8a2e:370:7334* .
Subject	Defines the text of the subject field or title of the mail.
To	Enter the email address of the recipient to which the mail is to be sent.

Send Mail

This step sends an email to a predefined address.

Parameter	Description
BCC	This parameter is optional as well and may contain the address of the blind carbon copy recipient to be added to the mail message.
CC	This parameter is optional and may contain the address of the carbon copy recipient to be added to the mail message.
From	Enter the name of the sender into this field.
Message Text	Enter into this field the text to be added to the message part of the mail message.
Port Number	Enter the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** .
Server Name	Enter into this field the name of the mail server, as defined in the **Mail** tab in the **System Variables** of the **Global Settings** . The name may either be entered as the full or short network name such as *mail* or *mail.enterprise.starfleet.com* or as its IP address in dotted notation, for example, *213.2.146.1* or *2001:db8:85a3::8a2e:370:7334* .
Subject	Defines the text of the subject field or title of the mail.
To	Enter the email address of the recipient to which the mail is to be sent.

Send SNMP Traps

This steps allows to send SNMP traps with a maximum of three trap variables (varbinds) to an SNMP server.

Parameter	Description
Community	Contains the community string used when sending SNMP traps to the agent, for example, public.
Destination Name	Enter the address of the host the trap is sent to inform of an IP address in dotted notation, for example, *213.2.146.1* or *2001:db8:85a3::8a2e:370:7334* .
Organization ID	Enter the OID of the management enterprise that defines the trap message, for example, *1.3.6.1.4.1.976* .
Parameter Type 1	Defines the type of the variable through its numeric representative: • 1: Object ID (SNMP_OID) • 2: String (SNMP_STR) • 3: Integer (SNMP_INT)
Parameter Value 1	Enter the actual value for the trap variable in form of a string.
Parameter Type 2	Defines the type of the variable through its numeric representative:

Parameter	Description
	• 1: Object ID (SNMP_OID) • 2: String (SNMP_STR) • 3: Integer (SNMP_INT)
Parameter Value 2	Enter the actual value for the trap variable in form of a string.
Parameter Type 3	Defines the type of the variable through its numeric representative: • 1: Object ID (SNMP_OID) • 2: String (SNMP_STR) • 3: Integer (SNMP_INT)
Parameter Value 3	Enter the actual value for the trap variable in form of a string.
Specify Type Identifier	Defines the type of the specific enterprise trap message through its numeric representative, for example, *10200* .
Standard Type Identifier	Defines the standard type of the trap message through its numeric representative: 0 = coldStart, 1 = warmStart, 2 = linkDown, 3 = linkUp, 4 = authenticationFailure, 5 = egpNeighborLoss and 6 = enterpriseSpecific.
Port	The port number on which the target listens for incoming traps.

Shutdown Device

This step allows you to completely shut down a client with any of the supported operating systems.

Parameter	Description
Clear Virtual Memory Pagefile	Determines whether the virtual memory pagefile should be cleared when the system is shut down. Enabling this security option also causes the hibernation file (hiberfil.sys) to be zeroed out when hibernation is disabled on a laptop system. When this policy is disabled, the virtual memory pagefile is not cleared during system shutdown.
Allow System to be Shut Down without Having to Log On	Determines whether a computer can be shut down without having to log on to Windows. When this policy is enabled, the **Shut Down** command is available on the Windows login screen. When this policy is disabled, the option to shut down the computer does not appear on the Windows login screen. In this case, users must be able to log on to the computer successfully and have the **Shut down the system** user right in order to perform a system shutdown.

Unlock Device

This step allows to unlock the mouse and keyboard of the device. This step must always be used after the operation for which the device was locked has finished, otherwise the remote device will remain locked. Be also aware, that, if the step is executed after a step with the stop on error option activated and the step fails, this step will not be executed and the remote device will remain locked.

No parameters need to be defined for this step.

Verify Last Device Boot Time

This step checks the uptime of a device, i.e., the time since the device was last booted and compares it with a specified maximum device uptime.

Parameter	Description
Max. Timeframe (min)	Specifies the maximum number of minutes that may have elapsed since the device booted for the last time. If the device uptime exceeds this value, a step error is returned.

Wait

This step stops the execution of the operational rule for a defined number of seconds before resuming the operation.

Parameter	Description
Seconds to Wait	Specifies the number of seconds to halt the execution before continuing.

Wait for Days

This step allows you to halt the execution of the operational rule for a number of days before continuing. This action fails if the number of specified days is exceeded and succeeds in the opposite case. Be aware, that for this step the Stop Condition parameter must be set to Stop on successful step.

Parameter	Description
Counter Identifier	Allows several operational rule assignments to use this step to interact between them. If for example, a rule is scheduled for each 10th of the month as well as every Tuesday (via two assignments), and it is requested, that it waits for 7 days, the rule executing on the 10th updates the common counter. This means, that the rule executing on Tuesday 13th takes the counter into consideration.
Days to Wait	Specifies the number of days to halt the execution before continuing.

Wake on LAN

This step launches a wake up call to a list of defined target clients to remote power on these devices.

Parameter	Description
Number of Retries	Defines the number of retries the step is to execute before abandoning if it fails.
Retry Interval (sec)	Defines the interval at which the step is to effect its retries in seconds.
IP Address List	Defines the list of IP addresses of the target machines, separated by a comma (,).
MAC Address List	The list of MAC addresses of the target machines, separated by a comma (,). This list must be in the same order as the IP address list and have the same number of addresses which must correspond to the IP addresses listed above.

User Message Box steps

This group collects any step concerned with presenting information to users on the remote clients in different types of message boxes. This group of steps is only applicable to Windows systems.

- Advanced Message Box
- Advanced Message Box With Image
- Close Information Dialog
- Display Information Dialog
- Localized Message Box
- Send Customized Form
- User Acknowledgement via Advanced Message Box
- User Acknowledgement
- User Acknowledgement via Message Box
- User Message Box

Advanced Message Box

This step displays an advanced message box to the user. An advanced message box is a dialog box that appears on the display asking for confirmation from the user.

Parameter	Description
Validation Button Label	Defines the text to be displayed on the confirmation button in the dialog box, such as for example *OK* or *Yes* .
Cancel Button Label	Defines the text to be displayed on the cancel button in the dialog box, such as for example *Cancel* or *No* . This button does not appear in the final message box if the text field is left empty.
Full Screen	Check this box if the message box is to be displayed in full screen mode.
Message Title	Defines the title string to display at the top of the dialog box.
Message Text	Enter into this field the main text displayed to be displayed in the dialog box.
Always display in foreground	Defines if the window is to be displayed always in the foreground, that is, every other window called is not positioned on top of the window but stays behind it.

Parameter	Description
Timeout (sec)	Defines the time to wait in seconds for the user to confirm or cancel. If the user does not react within this timeframe, the window is automatically validated and closed.
Success after timeout	Check this box if the step is to be executed after the defined timeout passed without user action (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Success if no one is logged on to device	Check this box if the step is to be executed if no user is logged on to the device (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Action if Screen Saving	Select from this dropdown box the way the step is to behave if the screen saver is active: • **Wait for End of Screen Saver** : do nothing until the screen saver is ended and the user takes action • **Success** : execute the step without waiting (this is the same as if the user clicked the validation button). • **Failure** : Do not execute the step (this is the same as if the user clicked the cancel button).

Advanced Message Box With Image

This step displays an advanced message box with a customizable background image to the user. An advanced message box is a dialog box that appears on the display asking for confirmation from the user.

Parameter	Description
Validation Button Label	Defines the text to be displayed on the confirmation button in the dialog box, such as for example *OK* or *Yes* .
Cancel Button Label	Defines the text to be displayed on the cancel button in the dialog box, such as for example *Cancel* or *No* . This button does not appear in the final message box if the text field is left empty.
Local Image File Path (bmp only)	Enter into this field the path to the image file which must be of type .bmp. If the image cannot be found, that is, because it is of another type, or it is too small, the default BCM image is used. If the image is too large it is cropped to fit the window. The default size of the BCM image is 460x310 pixels.
Message Title	Defines the title string to display at the top of the dialog box.
Message Text	Enter into this field the main text to be displayed in the dialog box.
Success after timeout	Check this box if the step is to be executed after the defined timeout passed without user action (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Success if no one is logged on to device	Check this box if the step is to be executed if no user is logged on to the device (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Success if the device is in screen saver mode	Select from this dropdown box the way the step is to behave if the screen saver is active: • **Wait for End of Screen Saver** : do nothing until the screen saver is ended and the user takes action

Parameter	Description
	• **Success** : execute the step without waiting (this is the same as if the user clicked the validation button). • **Failure** : Do not execute the step (this is the same as if the user clicked the cancel button).
Timeout (sec)	Defines the time to wait in seconds for the user to confirm or cancel. If the user does not react within this timeframe, the window is automatically validated and closed.
Always display in foreground	Defines if the window is to be displayed always in the foreground, that is, every other window called is not positioned on top of the window but stays behind it.

Close Information Dialog

This step allows you to close the information dialog that appeared for the Display Information Dialog step.

No parameters need to be defined for this step.

Display Information Dialog

This step displays an information message in form of a dialog box without a button. Reexecuting the step allows you to update the displayed message. This dialog must be closed again with the Close Information Dialog step.

Parameter	Description
Message Text	Enter the text of the message box here, for example, *The software program xyz is installed on your computer. Do you want to proceed with the installation now?*

Localized Message Box

This step allows you to display the contents of a message box in the language of the local operating system language. You may define four different target languages, for any other language the specified default message will be displayed. This step is only applicable to Windows operating systems.

Parameter	Description
Text Button 1	Enter the localized button text of the message box.
Text Button 2	Enter the localized button text of the message box.
Text Button 3	Enter the localized button text of the message box.
Text Button 4	Enter the localized button text of the message box.
Default Button Text	Enter the default text to appear on the button of the message box, that is displayed if the local operating system is not one of those defined below.

Parameter	Description
Default Message Title	Enter the default title of the message box, that is displayed if the local operating system is not one of those defined below.
Default Text	Enter into this field the default message text of the message box, that is displayed if the local operating system is not one of those defined below.
Language 1	Select the language for which the text specified in the following three fields is defined. The language selected here encompasses all 'versions' of the language, such as selecting English includes British English, American English, New Zealand English, etc.
Language 2	Select the language for which the text specified in the following three fields is defined. The language selected here encompasses all 'versions' of the language, such as selecting English includes British English, American English, New Zealand English, etc.
Language 3	Select the language for which the text specified in the following three fields is defined. The language selected here encompasses all 'versions' of the language, such as selecting English includes British English, American English, New Zealand English, etc.
Language 4	Select the language for which the text specified in the following three fields is defined. The language selected here encompasses all versions of the language, such as selecting English includes British English, American English, New Zealand English, etc.
Text 1	Enter the localized message text of the message box.
Text 2	Enter the localized message text of the message box.
Text 3	Enter the localized message text of the message box.
Text 4	Enter the localized message text of the message box.
Title Message 1	Enter the localized message title of the message box.
Title Message 2	Enter the localized message title of the message box.
Title Message 3	Enter the localized message title of the message box.
Title Message 4	Enter the localized message title of the message box.

Send Customized Form

This step creates a form to update the custom inventory of the local target client. Once the rule is executed, a browser window opens on the target, in which a form with several fields is to be filled by the local user.

The form has two buttons, OK to confirm the filled in form and Later to postpone the filling in of the values. Once the form is completed and confirmed the custom inventory .xml file is updated with the new information. This newly added information will be added to the custom inventory in the Console and the agent interface pages at the next update. The fields are prefilled in for a personal information form. This step is not applicable for Linux operating systems.

Parameter	Description
Validation Button Label	Defines the text to be displayed on the confirmation button in the dialog box, such as for example *OK* or *Yes* .
Cancel Button Label	Defines the text to be displayed on the cancel button in the dialog box, such as for example *Later* . This button does not appear in the final message box if the text field is left empty.
Labels of Custom Inventory Fields	Contains the semi-colon separated list of field names as which they appears in the custom inventory. Make sure that the order and the number of the fields is the same as in the **Form Fields** above. for example, Field List: *Name; FirstName;Phone,* these are the 'internal' references to the new fields, Labels: *Family Name;First Name;Office Phone Number,* this is the text as which the fields appears in the HCHL form and under the custom inventory node.
Footer Text	This free text field is below the list of fields to be filled in and may contain additional information.
Form Field Data Type	Contains the semi-colon separated list of the data types of the fields defined above to be filled into the form. Possible values are **string, integer, combo:string, combo:integer** and **boolean** . For example, *string;integer;boolean; combo:string* for the above listed form fields of *Name;Age;Driving License;Mobile Phone Operator* .
Default Field Values	Allows you to define default values for the form fields that is displayed to be selected via a drop down list. The entry default values are separated by commas (,), the default values for each field are separated by a semi-colon (;).
Form Fields	Contains the semi-colon separated list of fields of the form to be filled in, for example, *Name;Age;Driving License; Mobile Phone Operator* .
Title	Enter the title of the form into this field, for example, *Custom Inventory - Local Information* .
Header Text	A short textual explication for the local regarding the fields of the form below.
Insert a logo	Check this box if the background of the title is to show a logo. The default logo is the BCM logo, but the logo may be customized. It is located in directory *<InstallationDirectory>/master/ui/custom/common/images* . The 'logo' consists of two files *logo.gif* and *text.jpg* which are put next to each other. To customize modify the contents of the files but do NOT modify the names.
Retry Interval (min)	The retry interval defines the interval at which the step is to effect its retries in minutes.

User Acknowledgement via Advanced Message Box

This step allows the user to acknowledge information on his screen. If the timeout for the last try expires, this has the same effect as if OK was clicked.nNote: If you want to add another step after this one, the Stop on failed step condition must be set for this step.

Parameter	Description
Message Title	Enter the title of the message box into this field, for example, Installation.
Message Text	Enter the text of the message box here, for example, *The software program xyz is installed on your computer. Do you want to proceed with the installation now?*
Validation Button Label	Define the label of the validation button, such as *OK* to indicate to the operational rule to proceed with its execution.

Parameter	Description
Cancel Button Label	Define the label of the cancel button, such as *Later* , to indicate not now, proceed later.
Number of Retries	Defines how often the user has the choice to postpone the announced operation.
Retry Interval (min)	Defines the interval in minutes at which the user is presented with this user message box.
Always display in foreground	Defines if the window is to be displayed always in the foreground, that is, every other window called is not positioned on top of the window but stays behind it.
Full Screen	Check this box if the message box is to be displayed in full screen mode.
Timeout (sec)	Defines the time to wait in seconds for the user to confirm or cancel. If the user does not react within this timeframe, the window is automatically validated and closed.
Success after timeout	Check this box if the step is to be executed after the defined timeout passed without user action (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Success if no one is logged on to device	Check this box if the step is to be executed if no user is logged on to the device (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Action if Screen Saving	Select from this dropdown box the way the step is to behave if the screen saver is active: • **Wait for End of Screen Saver** : do nothing until the screen saver is ended and the user takes action • **Success** : execute the step without waiting (this is the same as if the user clicked the validation button). • **Failure** : Do not execute the step (this is the same as if the user clicked the cancel button).

User Acknowledgement

This step sends a message box to the local client which informs the user of actions that will be taken on his/her device and provide him/her with the possibility to postpone these operations until he/she has taken the steps necessary to save all current work. A situation in which this step is useful is before a remote software installation, for instance.

Parameter	Description
Title	Enter a title for the window and the message below, such as *Application Installation* .
Message	Enter here the message to the user to inform him of what is undertaken on his machine.
Number of Retries	Defines how often the user has the choice to postpone the announced operation.
Retry Interval (min)	Defines the interval in minutes at which the user is presented with this user message box.

User Acknowledgement via Message Box

This step creates a message box on the target device. The purpose is to allow the end user to acknowledge information. The end user can accept or delay the operation; however, the user cannot completely cancel the operation. After the specified number of retries and retry intervals, the execution will be forced.nNote: If you want to add another step after this one, the Stop on failed step condition must be set for this step.

Parameter	Description
Validation Button Label	Define the label of the validation button, such as *OK* to indicate to the operational rule to proceed with its execution.
Cancel Button Label	Define the label of the cancel button, such as *Later* , to indicate not now, proceed later.
Message Title	Enter the title of the message box into this field, for example, Installation.
Message Text	Enter the text of the message box here, for example, *The software program xyz is installed on your computer. Do you want to proceed with the installation now?*
Number of Retries	Defines how often the user has the choice to postpone the announced operation.
Retry Interval (min)	Defines the interval in minutes at which the user is presented with this user message box.

User Message Box

This step displays a message box to the user on the target devices. A message dialog box is a small box that appears on the display screen to give you information or to warn you about a potentially damaging operation.

For example, it might warn you that the system is deleting one or more files. Unlike normal dialog boxes, message boxes do not require any user input. However, you need to acknowledge the alert box by pressing the Enter key or clicking a mouse button to make it go away. The functions of this Chilli module enable you to create such boxes.

Parameter	Description
Button Text	Defines the text to be displayed on the single button in the dialog box.
Message Title	Defines the title string to display at the top of the dialog box.
Message Text	Enter into this field the main text displayed to be displayed in the dialog box.
Success if no one is logged on to device	Check this box if the step is to be executed if no user is logged on to the device (this is the same as if the user clicked the validation button). If the box remains unchecked the step is not executed (this is the same as if the user clicked the cancel button).
Action if Screen Saving	Select from this dropdown box the way the step is to behave if the screen saver is active: • **Wait for End of Screen Saver** : do nothing until the screen saver is ended and the user takes action

Parameter	Description
	• **Success** : execute the step without waiting (this is the same as if the user clicked the validation button). • **Failure** : Do not execute the step (this is the same as if the user clicked the cancel button).

Virtual Infrastructure Management steps

This class contains all steps that are concerned with the management of virtual devices within your network.

- Change the state of a machine

Change the state of a machine

This action allows to change the state of a virtual machine by entering its guest member ID or the name, that was given to it by the user. The available options are: start, stop, shut down and pause.

Parameter	Description
Guest Member ID	Enter the unique identifier of the virtual machine, if this value is to be used to identify the machine. This is the ID in form of a number that you can find in the **Guest Member ID** column of the list of **Virtual Guests** , for example, *5148c4a2-7b24-f909-eb1a-29fc30347672* .
Virtual Machine Name	Name of the virtual machine.
Use Virtual Machine Name	Check this box if you want to identify the virtual machine by the name, that the user has given the machine. In this case the field **Guest Member ID** is not used.
State to apply to the machine	You need to specify the state you want to apply to the virtual machine: either **start** , **stop** , **shut down** or **pause** .

Windows steps

eThis class groups all steps concerned with any aspect of the Microsoft Windows operating systems.

- Advanced User Profile Extraction via MigrationManager
- Advanced User Profile Injection via MigrationManager
- Advanced Reboot
- Advanced Registry Management
- Automated Execution of MyApps after User Login
- Automatic Authentication Parameter Modification
- Create Shortcut
- Create Shortcut as Current User

- Delete Shortcut
- Delete Shortcut Group
- Disconnect Current Windows User
- Group Management
- Logged User
- Main Device User
- Modify PATH System Variable
- Modify Shortcut
- Modify Shortcut as Current User
- Mount Network Drive
- Mount Network Drive as Current User
- Registry Key Verification
- Registry Management
- Restore Windows Data and Profile
- Restore Windows Data and Profile (USMT 4)
- Save Windows Data and Profile
- Save Windows Data and Profile (USMT 4)
- Service Management
- Sharing Windows Folders
- Uninstall MSI Package
- Unmount Network Drive
- Unmount Network Drive as Current User
- User Management
- User Profile Extraction via MigrationManager
- User Profile Injection via MigrationManager
- Windows Session Status Verification

Advanced User Profile Extraction via MigrationManager

This step allows you to extract user profiles of a device using specific filters via the MigrationManager.

Parameter	Description
MigrationManager's host name	Enter the name or IP address of the device on which the MigrationManager server is located.
Use relay	Check this box to use the relay device as the MigrationManager server.
Shared folder	Enter the name of the network share of the MigrationManager server.
Data Storage Path	Enter the name of the directory in which the profiles are stored. The name must have the format NetworkPathNameProfileDirectoryName.
Configuration File Path	Enter the name of the configuration file that specifies the profile data to save. The name must have the format NetworkPathNameConfigurationFileName.
All Users	Check this box to extract all user profiles of the device.
Exclude local users	Check this box to extract all profiles with the exception of the local profiles of this device.

Parameter	Description
Users to include	Allows you to specify the user profiles to extract. The values of this list must be separated by semi-colons (;).
Users to Exclude	Allows you to specify the user profiles that are not to be extracted. The values of this list must be separated by semi-colons (:).
Domains to exclude	Allows you to specify the domains that are to be igored during extraction. The values of this list must be separated by semi-colons (:).
Domain Name	Enter the domain name of the administrator who is to execute the extraction.
Administrator Name	Enter the name of the administrator who is to execute the extraction.
Administrator Name	Enter the name of the administrator who is to execute the extraction.

Advanced User Profile Injection via MigrationManager

This step allows you to inject user profiles into a device using specific filters via the MigrationManager

Parameter	Description
MigrationManager's host name	Enter the name or IP address of the device on which the MigrationManager server is located.
Use relay	Check this box to use the relay device as the MigrationManager server.
Shared folder	Enter the name of the network share of the MigrationManager server.
Data Storage Path	Enter the name of the directory in which the profiles are stored. The name must have the format NetworkPathNameProfileDirectoryName.
Configuration File Path	Enter the name of the configuration file that specifies the profile data to restore. The name must have the format NetworkPathNameConfigurationFileName.
Use Target File	Check this box if you want to use the target file located on the MigrationManager server. This allows you to use the profiles of a device on another device as well.
All Users	Check this box to inject all user profiles of the device.
Exclude local users	Check this box to inject all profiles with the exception of the local profiles of this device.
Users to include	Allows you to specify the user profiles to inject. The values of this list must be separated by semi-colons (;).
Users to Exclude	Allows you to specify the user profiles that are not to be injected. The values of this list must be separated by semi-colons (;).
Domains to exclude	Allows you to specify the domains that are to be igored during injection. The values of this list must be separated by semi-colons (;).
Domain Name	Enter the domain name of the administrator who is to execute the injunction.
Administrator Name	Enter the name of the administrator who is to execute the injunction.
Administrator Name	Enter the name of the administrator who is to execute the injunction.

Advanced Reboot

This step defines the parameters and window contents of the device reboot. This reboot may be executed immediately or be postponed by the user. If the reboot is immediate, a message box is displayed on the target device, informing the user of that the device will be rebooted after a specified number of seconds.

The logo of the message box may be customized as well. For this you only need to store the following customized images in their exact sizes in the datacoreres directory of the BCM agent: FullSized.bmp (575 x 575 pixels), MediumSized.bmp (575 x 510 pixels), SmallSized.bmp (575 x 455 pixels), RebootAfterLogOut.bmp (575 x 275 pixels).

Parameter	Description
Deferred Reboot	This box defines if the user can defer a reboot when it is requested by CM. If checked, it allows the user to postpone the reboot, if it appears at an inconvenient time. You can define how often and for how long the user can postpone the reboot in the next two boxes. If you uncheck the box, the reboot is executed as scheduled.
Timeout before auto-accept (min)	The number of minutes defines the timeframe the user has to accept or postpone the reboot in the displayed message. If the user does not react before the counter expires, the reboot proceeds as defined.
Postpone Count	Defines how often the user may decide to postpone the reboot for the below specified number of minutes.
Postpone Delay (min)	The interval in minutes that the reboot may be postponed.
Localized Title 1	To display the title in the language of the local operating system enter the localized title here in the format *CodePage:title* , for example, *1033:The New Customizable Title* . The *CodePages* represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Localized Title 2	Defines the localized title for an alternative local operating system language in the format *CodePage:Title* , for example, *2057:The New Customisable Title* . The *CodePages* represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Default Title	Enter the default title of the message box, that is displayed if the local operating system is not one of those defined below.
Localized Message 1	To display the message in the language of the local operating system enter the localized message here in the format *CodePage : Message* . The CodePages represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Localized Message 2	Defines the localized message for an alternative local operating system language in the format *CodePage : Message* . The CodePages represents that language of the local operating system, the most common are English (UK): 2057, English (US): 1033, French: 1036, German: 1031, Portuguese (Brazil): 1046, Spanish: 1034 and Japanese: 1041.
Default Text	Enter the default message text of the message box, that is displayed if the local operating system is not one of those defined below.

Parameter	Description
Force Reboot if Client is Locked	Check this box if the reboot is to be executed even if the client is locked. Otherwise the reboot waits until the client becomes unlocked.

Advanced Registry Management

This step adds a new registry key, or to modify or delete an existing one.

Parameter	Description
Registry Key	The name of the registry key to be added, modified or deleted.
Operation to Execute	Defines which operation is to be executed in the Registry, either to add or modify (**Add/Modify**) the key specified following, to delete it (**Delete**) or to delete it with all its children (**Delete recursively**).
Value Name	The name of the value of the key to be modified or added. This field is not required for the **Delete** operation. If this field is left empty for a modify operation, the *"(DEFAULT)"* registry key is targeted.
Value Type	The value type of the registry key. It is not required for the **Delete** operation.
Registry Key Value	The value of the key to be modified or added. This field is not required for the **Delete** operation.
Binary Value in Hexadecimal Format	Check this box if the provided binary value is a hexadecimal translation.

Automated Execution of MyApps after User Login

This step automatically executes the rules assigned to specific users when they have opened a session on the device. These rules will not be executed if the assigned user is not logged on to the device. Also rules which are part of the automated kiosk MyApps will not be displayed in MyApps to which the local user has access via the agent interface.

Parameter	Description
Prefix to Filter	Any rules that have this prefix are NOT executed via MyApps. These rules appears in MyApps without their prefix. If this feature is not to be used leave this field emtpy.
Max. Interval Between Verifications (h)	Defines the interval at which the agent verifies if rules are to be executed in hours.

Automatic Authentication Parameter Modification

This step permits modifying the automatic authentication parameters at Windows startup with backup and restoration of previous parameters. This allows you to change the current automatic administrator login data to be able to log on to the device with the right administrator at the next reboot. At the same time, the parameter values of the currently logged-in user, such as domain and user name are saved and may be restored.

Parameter	Description
Domain Name	The domain of the administrator.

Parameter	Description
Administrator Name	Enter the name of the administrator login.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
Restore Previous Parameters	Check this box if the above backed up settings are to be restored.
Save Current Parameters	Check this box if the currently existing automatic authentication parameters are to be backed up before being overwritten with the above defined new settings.

Create Shortcut

A shortcut creates a quick access to a specified action by passing Windows-based messages and parameters. This function allows you access to all the same functions as provided by the Windows Shortcut Designer to create a shortcut. The .lnk extension of the mandatory path parameter of this functions is optional.

Parameter	Description
Description	Enter a descriptive text for the shortcut. This entry is used for identification purposes only and does not affect the operation of the shortcut itself.
Icon File	Defines the file which contains the icon to be displayed with the shortcut. If it contains more than one icon the requested icon may be specified via its index separated from the file name by a comma (,), for example, *explorer.exe* to use the icon at index 0 or *explorer,3* to use the icon at index 3.
Parameters	Defines any type of parameter to be taken into account when the shortcut is executed. For example you may define here the homepage to be automatically opened in browser for which you create the shortcut.
Shortcut Group Name	Defines the respective group if the shortcut is to be part of a shortcut group.
Shortcut Path	Defines the relative or full path of the shortcut file to be created. You can also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables might be very useful if the configurations of your clients are heterogeneous. After the shortcut path you can also add, separated with a space, additional parameters for the shortcut target. For example, when launching a browser window you can add a default web page with which the browser opens, for example, *c:Program FilesInternet Exploreriexplorer.exe www.bmc.com* .
Target Path	Defines the relative or full path of the file that the shortcut points to. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Working Directory	Defines the relative or full path of the working directory used when the target is started. By default the working directory path is the current working directory set by the shell program represented by the shortcut it starts. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Create Shortcut as Current User

A shortcut creates a quick access to a specified action by passing Windows-based messages and parameters. This function allows you access to all the same functions as provided by the Windows Shortcut Designer to create a shortcut as the currently logged-in user. The .lnk extension of the mandatory path parameter of this functions is optional.

Parameter	Description
Description	Enter a descriptive text for the shortcut. This entry is used for identification purposes only and does not affect the operation of the shortcut itself.
Icon File	Defines the file which contains the icon to be displayed with the shortcut. If it contains more than one icon the requested icon may be specified via its index separated from the file name by a comma (,), for example, *explorer.exe* to use the icon at index 0 or *explorer,3* to use the icon at index 3.
Parameters	Defines any type of parameter to be taken into account when the shortcut is executed. For example you may define here the homepage to be automatically opened in browser for which you create the shortcut.
Shortcut Group Name	Defines the respective group if the shortcut is to be part of a shortcut group.
Shortcut Path	Defines the relative or full path of the shortcut file to be created. You can also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables might be very useful if the configurations of your clients are heterogeneous. After the shortcut path you can also add, separated with a space, additional parameters for the shortcut target. For example, when launching a browser window you can add a default web page with which the browser opens, for example, *c:Program FilesInternet Exploreriexplorer.exe www.bmc.com* .
Target Path	Defines the relative or full path of the file that the shortcut points to. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Working Directory	Defines the relative or full path of the working directory used when the target is started. By default the working directory path is the current working directory set by the shell program represented by the shortcut it starts. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Delete Shortcut

This step deletes a shortcut.

Parameter	Description
Shortcut	Defines the relative or full path of the shortcut file to be deleted. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Delete Shortcut Group

This step deletes a group of shortcuts.

Parameter	Description
Shortcut Group Name	Defines the relative or full path of the shortcut group to be deleted. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Disconnect Current Windows User

This step disconnects the user that is currently logged on to Windows.

No parameters need to be defined for this step.

Group Management

This step adds, removes or modifies local user groups.

Parameter	Description
Add	Check this box if the above defined path is to be added.
Remove	Check this box if the group defined below is to be removed or if the users listed in the field below are to be removed from the group.
Domain	This check box defines if the if the operations to be performed on the primary domain controller (PDC) of the current domain. If the box is not checked the operation is performed only on the local device. This option only applies to Windows XP Professional clients that are members of a domain. By default, server computers perform operations on the primary domain controller.
Group Name	Enter either the name of a new group to be created or the name of an existing group which is to be removed or modified.
User List (optional)	Enter the names of the users to either be added to or to be removed from the group listed in the field above. If it contains more than one name, they must be separated with a comma. Names can be local users, users on other domains, or global groups but no other local groups. If a user is from another domain, preface the user name with the domain name, for example, *EnterpriseScotty* . Be aware that the group to which a list of users is to be added to must already exist, because the step does not create it otherwise.

Logged User

This step verifies which user(s) is/are currently logged on to the device and stores this information in the .xml file for further use, such as updating the custom inventory. The step collects the login name and the date and time at which the user was found to be logged on. At the next verification, the date and time value will be updated if the user is still connected. If a user is no longer connected at the next verification, the entry will not be erased, it will be left as it is, that is, with the timestamp of the last verification.

No parameters need to be defined for this step.

Main Device User

This step verifies the name of the user which is most often logged on to the device the step is assigned to and then inserts an entry into the custom inventory regarding this user.

Parameter	Description
All User History	Check this box to upload the complete history of all users ever connected to this device. If this box remains unchecked the information is uploaded only for the user most often connected to the device.
Maximum User Login Count (History)	Specified the number of logins which are stored in memory to verify which is the user logged on most often. When the number is reached, the oldest login is dropped to add the newest.

Modify PATH System Variable

This step modifies an entry in the PATH system variable, that is, either adding a new entry or removing an existing entry.

Parameter	Description
Add	Check this box if the above defined path is to be added.
Path	Enter into this field the full path to be added or the existing one to be removed, for example, *C:WindowsSystem32* .
Remove	Check this box if the above defined path is to be removed.

Modify Shortcut

This step modifies any parameter of an existing shortcut. The .lnk extension of the mandatory path parameter of this functions is optional.

Parameter	Description
Description	Enter a descriptive text for the shortcut. This entry is used for identification purposes only and does not affect the operation of the shortcut itself.
Icon File	Defines the file which contains the icon to be displayed with the shortcut. If it contains more than one icon the requested icon may be specified via its index separated from the file name by a comma (,), for example, *explorer.exe* to use the icon at index 0 or *explorer,3* to use the icon at index 3.
Parameters	Defines any type of parameter to be taken into account when the shortcut is executed. For example you may define here the homepage to be automatically opened in browser for which you create the shortcut.
Shortcut Group Name	If the shortcut is to be part of a shortcut group this field defines the respective group. This parameter is optional.
Shortcut Path	Defines the relative or full path of the shortcut file to be created. You can also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables might be very useful if the configurations of your clients are heterogeneous. After the shortcut path you can also add, separated with a space, additional parameters for the shortcut target. For example, when launching a browser window you can add a default web page with which the browser opens, for example, *c:Program FilesInternet Exploreriexplorer.exe www.bmc.com* .
Target Path	Defines the relative or full path of the file that the shortcut points to. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Working Directory	Defines the relative or full path of the working directory used when the target is started. By default the working directory path is the current working directory set by the shell program represented by the shortcut it starts. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Modify Shortcut as Current User

This step modifies an existing shortcut as the currently logged-in user. The .lnk extension of the mandatory path parameter of this function is optional.

Parameter	Description
Description	Enter a descriptive text for the shortcut. This entry is used for identification purposes only and does not affect the operation of the shortcut itself.
Icon File	Defines the file which contains the icon to be displayed with the shortcut. If it contains more than one icon the requested icon may be specified via its index separated from the file name by a comma (,), for example, *explorer.exe* to use the icon at index 0 or *explorer,3* to use the icon at index 3.
Parameters	Defines any type of parameter to be taken into account when the shortcut is executed. For example you may define here the homepage to be automatically opened in browser for which you create the shortcut.
Shortcut Group Name	If the shortcut is to be part of a shortcut group this field defines the respective group. This parameter is optional.
Shortcut Path	Defines the relative or full path of the shortcut file to be created. You can also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables might be very useful if the configurations of your clients are heterogeneous. After the shortcut path you can also add, separated with a space, additional parameters for the shortcut target. For example, when launching a browser window you can add a default web page with which the browser opens, for example, *c:Program FilesInternet Exploreriexplorer.exe www.bmc.com* .
Target Path	Defines the relative or full path of the file that the shortcut points to. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.
Working Directory	Defines the relative or full path of the working directory used when the target is started. By default the working directory path is the current working directory set by the shell program represented by the shortcut it starts. You may also use one or more environment variables to indicate the path. The variable must be enclosed in *${}* . These variables may be very useful if the configurations of your clients are heterogeneous.

Mount Network Drive

This step allows mounting a network drive with a LocalSystem account. The drive will be created with the SYSTEM account and its permissions. Sometimes the drive may appear to be disconnected in Windows Explorer; however, it is accessible. The visibility of the drive in the Windows Explorer depends on the rights of the connected user.

Parameter	Description
User Domain	Enter the name of the user domain.
Add Access Rights to the Privacy List	Check this box if the access rights to this share are to be added to the Privacy settings of the local agent.
Destination Share	Enter the name of the share to mount.
Drive Letter	Enter the letter that is to be attributed to the mounted drive.
Persistent	Check this box if the drive is to be mounted at every startup. If this option is not checked it is only mounted once after the execution of the step.
	Enter the name of the device on which the shared drive is located.

Parameter	Description
Name of the Share Device	
User Login	Enter a valid user login for this domain.
User Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).

Mount Network Drive as Current User

This step allows mounting a network drive as the currently logged-in user.

Parameter	Description
Destination Share	Enter the name of the share to mount.
Drive Letter	Enter the letter that is to be attributed to the mounted drive.
Name of the Share Device	Enter the name of the device on which the shared drive is located.

Registry Key Verification

This step checks for the presence of a specific registry key and verifies if a value name exists and if yes, checks the key value.

Parameter	Description
Registry Key to Check	The name of the registry key of which you are not sure it exists.
Value Name	The name of the key value that is to be found. This field is optional.
Registry Key Value	The value of the registry key which is verified by the agent. This field is mandatory if a **Value Name** is provided in the field above. It may remain empty if the value you are looking for is actually empty, otherwise the key will not be found. Depending on the type the following conditions apply: • **REG_MULT_SZ** : In this case only the first line of the value is verified. • **REG_DWORD** : If the value is of type DWORD, the value must mandatorily be entered in hexadecimal format exactly as shown in the registry, including the "0x" and leading zeros. • **REG_BINARY** : If the value is of type BINARY, the value must be entered in its translated value NOT as its hexadecimal value. If, however, the corresponding box is checked, it must be entered as its hexadecimal value after all, for example CCAA015A33.
Binary Key in Hexadecimal Notation	Check this box if the value is a binary key that is expressed in hexadecimal notation.

Registry Management

This step adds a new registry key, or to modify or delete an existing one.

Parameter	Description
Registry Key	The name of the registry key to be added, modified or deleted.
Operation to Execute	Defines which operation is to be executed in the Registry, either to add or modify (**Add/Modify**) the key specified following or to delete it (**Delete**).
Value Name	The name of the value of the key to be modified or added. This field is not required for the **Delete** operation. If this field is left empty for a modify operation, the *(DEFAULT)* registry key is targeted.
Value Type	The value type of the registry key. It is not required for the **Delete** operation.
Registry Key Value	The value of the key to be modified or added. This field is mandatory if a **Value Name** is provided in the field above. It may remain empty if the value you are looking for is actually empty, otherwise the key will not be found. Depending on the type the following conditions apply: • **REG_MULT_SZ** : In this case only the first line of the value is verified. • **REG_DWORD** : If the value is of type DWORD, the value must mandatorily be entered in hexadecimal format exactly as shown in the registry, including the "0x" and leading zeros. • **REG_BINARY** : If the value is of type BINARY, the value must be entered in its translated value NOT as its hexadecimal value. This field is not required for the **Delete** operation.
Binary Value in Hexadecimal Format	Check this box if the provided binary value is a hexadecimal translation.

Restore Windows Data and Profile

You must run this step on Windows XP from an account with administrative credentials, or some operating system settings may not migrate - for example, wallpaper settings, screen saver selections, modem options, media player settings, and Remote Access Service (RAS) connection phone book(.pbk) files and settings. For this reason, we recommend that you run it using an account with administrative credentials.

When running this step on Windows Vista, you need to run it in “Administrator” mode from an account with administrative credentials to ensure that all specified users are migrated. This is because User Access Control (UAC) is turned on in Windows Vista. If you do not run the step in “Administrator” mode, only the user profile that is logged on will be included in the migration.

The following operating systems are supported:n- Windows XPn- Windows Vistan- Windows 2008

Start the Microsoft loadstate.exe file to migrate the files and settings from the store created by scanstate.exe launched by the Save Windows Data and Profile step, to the destination computer.

LoadState migrates each file (one by one) from the store to a temporary location on the destination computer. The files are decompressed (and decrypted if necessary) during this process. Next, loadstate transfers the file to the correct location, deletes the temporary copy, and begins migrating the next file.

Parameter	Description
Absolute Path	Defines if the path entered in the above **Backup Source Path** field is to be taken as an absolute path. This might be useful, if a backup of another client is to be used for restoring.
Administrator Name	Enter a valid login name to the backup device into this field, with which the operational rule is to log on to the device.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
All Users	Checking this option migrates all of the users on the computer.
XML Configuration File Path	Specifies the *Config.xml* file that the process should use to recuperate the store. The path must be a full path.
Continue on Error	If activated, the process continues to run even if there are nonfatal errors. Without this option, LoadState exits on the first error. When you specify this option, any files or settings that cause an error and are ignored is logged on the progress log. In addition, if a file is open or in use by an application, USMT is not able to migrate the file and logs an error.
Additional Customized XML File Path	Specifies an .xml file that contains rules that define what state to migrate. The path must be a full path.
Decryption Key	Decrypts the store data with the specified key (password). With this option, you need to specify the decryption key.
Users to Exclude	Excludes the specified user(s) from the migration. You can specify multiple users separated by semi-colons (;). Domain name and user name can contain the asterisk (*) wildcard character with the format *DomainNameUserName* .
Local User Restoration	Checking this box activates local account creation and enabling. If the account being migrated is local (a non-domain account), and the account does not exist, then this option enables USMT to create a new local account. If you are migrating local accounts (as opposed to domain accounts), settings are not migrated unless you check this option.
Migrate Application Data	Defines if the contents of the Migapp.inf are to be taken into account. This configuration file controls which application settings are migrated. The file contains a list of standard applications, such as Adobe Applications (Acrobat, Photoshop), Eudora, all Microsoft Office Applications, Lotus Applications, etc.
Migrate System Data	Defines if the contents of the Migsys.inf are to be taken into account. This configuration file controls which operating system and browser settings are migrated. It includes amongst others the following options: Accessibility Options, Display Properties, Folder Options Fonts, Internet Settings, Internet Security Settings, Localization / International Settings, Mouse and Keyboard, etc.
Migrate User Data	Defines if the contents of the Miguser.inf are to be taken into account. This configuration file controls which user file types and desktop settings are migrated. The components in this file include amongst others: Desktop, Favorites, My Pictures, My Documents, Shared Documents, Start Menu Items, etc.
Former Domain or Local Device Name	Specifies the old domain of the user(s). It may contain the asterisk (*) wildcard character. If you specify an old domain that did not exist on the source computer, LoadState appears to complete successfully (without an error or warning). However, in this case, users are not moved to the new domain but remain in their original domain. For example, if you miss-spell *domain1* and you specify *domai1* , the users remain in domain1 on the destination computer.
Target Domain Name	Specifies a new domain for the user(s). You should use this option to change the domain for users on a computer or to migrate a local user to a domain account.

Parameter	Description
No Compression	Indicates that the stored data is not compressed. You should only use this option in testing environments because we recommend that you use a compressed store during your actual migration. This option cannot be used in with the **Decryption** option.
Only Local User	Migrates only the specified users. You can specify multiple users in form of a semi-colon separated list. This option is helpful when there are multiple users on the source computer who are all getting their own computer.
Create Log File	Defines if a log file is to be created. It is located in the directory of the Mig file.
Backup Location	Enter the name of the device on which the backup is stored. If the backup device is the relay leave the field empty.
Backup Source Path	Enter the path to the backup location on the backup device, for example, *C:backupscotty* for an absolute path to be used, or *C:backup* for a root backup path.
Backup Located on Relay	Check this box if the backup is stored on the relay. In this case do not provide a name in the field above, otherwise there is conflicts.
USMT Installation Path	Specifies the location of the *loadstate.exe* file which restores the backed up data and profiles.

Restore Windows Data and Profile (USMT 4)

You should log off after you run LoadState. Some settings (for example, fonts, wallpaper, and screensaver settings) will not take effect until the next time the user logs in.

When running this step on Windows Vista, you need to run it in “Administrator” mode from an account with administrative credentials to ensure that all specified users are migrated. This is because User Access Control (UAC) is turned on in Windows Vista. If you do not run the step in “Administrator” mode, only the user profile that is logged on will be included in the migration.

The following operating systems are supported:n- Windows Vistan- Windows 7

Start the Microsoft loadstate.exe file to migrate the files and settings from the store created by scanstate.exe (launched by the Save Windows Data and Profile step) to the destination computer.

LoadState migrates each file (one by one) from the store to a temporary location on the destination computer - the files are decompressed (and decrypted if necessary) during this process. Next, loadState transfers the file to the correct location, deletes the temporary copy, and begins migrating the next file.

Parameter	Description
Absolute Path	Defines if the path entered in the above **Backup Source Path** field is to be taken as an absolute path. This might be useful, if a backup of another client is to be used for restoring.
Administrator Name	Enter a valid login name to the backup device into this field, with which the operational rule is to log on to the device.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).

Parameter	Description
All Users	Checking this option migrates all of the users on the computer.
XML Configuration File Path	Specifies the *Config.xml* file that the process should use to recuperate the store. The path must be a full path.
Continue on Error	If activated, the process continues to run even if there are nonfatal errors. Without this option, LoadState exits on the first error. When you specify this option, any files or settings that cause an error and are ignored is logged on the progress log. In addition, if a file is open or in use by an application, USMT is not able to migrate the file and logs an error.
Additional Customized XML File Path	Specifies an .xml file that contains rules that define what state to migrate. The path must be a full path.
Decryption Key	Decrypts the store data with the specified key (password). With this option, you need to specify the decryption key.
Users to Exclude	Excludes the specified user(s) from the migration. You can specify multiple users separated by semi-colons (;). Domain name and user name can contain the asterisk (*) wildcard character with the format *DomainNameUserName* .
Local User Restoration	Check this box to enable local account creation and enabling. If the account being migrated is local (a non-domain account), and the account does not exist, then this option enables USMT to create a new local account. If you are migrating local accounts (as opposed to domain accounts), settings are not migrated unless you check this option.
Migrate Application Data	Defines if the contents of the MigApp.xml are to be taken into account. This configuration file controls which application settings are migrated. The file contains a list of standard applications, such as Adobe Applications (Acrobat, Photoshop), Eudora, all Microsoft Office Applications, Lotus Applications, etc.
Migrate Documents	Defines if the contents of the MigDocs.xml are to be taken into account. This file controls which personal documents/files are migrated.
Migrate User Data	Defines if the contents of the MigUser.xml are to be taken into account. This configuration file controls which user file types and desktop settings are migrated. The components in this file include amongst others: Desktop, Favorites, My Pictures, My Documents, Shared Documents, Start Menu Items, etc.
Former Domain or Local Device Name	Specifies the old domain of the user(s). It may contain the asterisk (*) wildcard character. If you specify an old domain that did not exist on the source computer, LoadState appears to complete successfully (without an error or warning). However, in this case, users are not moved to the new domain but remain in their original domain. For example, if you miss-spell *domain1* and you specify *domai1* , the users remain in domain1 on the destination computer.
Target Domain Name	Specifies a new domain for the user(s). You should use this option to change the domain for users on a computer or to migrate a local user to a domain account.
No Compression	Indicates that the stored data is not compressed. You should only use this option in testing environments because we recommend that you use a compressed store during your actual migration. This option cannot be used in with the **Decryption** option.
Only Local User	Migrates only the specified users. You can specify multiple users in form of a semi-colon separated list. This option is helpful when there are multiple users on the source computer who are all getting their own computer.
Create Log File	Defines if a log file is to be created. It is located in the directory of the Mig file.

Parameter	Description
Backup Location	Enter the name of the device on which the backup is stored. If the backup device is the relay leave the field empty.
Backup Source Path	Enter the path to the backup location on the backup device, for example, *C:backupscotty* for an absolute path to be used, or *C:backup* for a root backup path.
Backup Located on Relay	Check this box if the backup is stored on the relay. In this case do not provide a name in the field above, otherwise there is conflicts.
USMT Installation Path	Specifies the location of the *loadstate.exe* file which restores the backed up data and profiles.

Save Windows Data and Profile

You must run this step on Windows XP from an account with administrative credentials, or some operating system settings may not migrate - for example, wallpaper settings, screen saver selections, modem options, media player settings, and Remote Access Service (RAS) connection phone book(.pbk) files and settings. For this reason, we recommend that you run it from within an account with administrative credentials.

When running this step on Windows Vista, you need to run it in “Administrator” mode from an account with administrative credentials to ensure that all specified users are migrated. This is because User Access Control (UAC) is turned on in Windows Vista. If you do not run the step in “Administrator” mode, only the user profile that is logged on will be included in the migration.

This step starts the Microsoft scanstate.exe file that creates an intermediate store that contains the user files and settings from the source computer.

The loadstate.exe file, launched by the Restore Windows Data and Profile step, then restores these files and settings to the destination computer. Scanstate does not modify the source computer. By default, scanstate compresses the files and stores them as an image file (USMT3.MIG).

The following operating systems are supported:n- Windows XPn- Windows Vistan- Windows 2008

Parameter	Description
Administrator Name	Enter a valid login name to the backup device into this field, with which the operational rule logs on to the device.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
All Users	Checking this option migrates all of the users on the computer.
Data Compression	Enables compression of data and saves the files to a hidden folder named File at StorePathUSMT3. This option cannot be used in combination with the encryption option below.
XML Configuration File Path	Specifies the *Config.xml* file that the process should use to recuperate the store. The path must be a full path.

Parameter	Description
Continue on Error	If activated, the process continues to run even if there are nonfatal errors. Without this option, ScanState exits on the first error. When you specify this option, any files or settings that cause an error and are ignored is logged on the progress log. In addition, if a file is open or in use by an application, USMT may not be able to migrate the file and logs an error.
Additional Customized XML File Path	Specifies an .xml file that contains rules that define what state to migrate. The path must be a full path.
Destination Host Name	Enter the name of the host on which the backup is stored. If the destination host is the relay leave the field empty.
Backup on Relay	Check this box if the backup is to stored on the relay. In this case do not provide a name in the field above, otherwise there is conflicts.
Shared Target Folder	Indicates a folder where to save the files and settings
Encryption Key	Encrypts the data to store with the specified key (password). With this option, you need to specify the encryption key. We recommend that encryption key be at least 8 characters long, but it cannot exceed 256 characters. This option cannot be used in combination with the **Data Compression** parameter above.
Users to Exclude	Excludes the specified user(s) from the migration. You can specify multiple users separated by semi-colons (;). Domain name and user name can contain the asterisk (*) wildcard character, for example, *DomainNameUserName* .
Only Local Directories	Specifies that only files that are stored on the local computer is migrated, regardless of the rules in the .inf files. You should use this option when network drives are mapped on the source computer and is mapped again in the same way on the destination computer (for example, if you map drives using login scripts). If this box is not checked, then Scanstate copies files from network drives into the store.
Migrate Application Data	This check box defines if the contents of the Migapp.inf are to be taken into account. This configuration file controls which application settings are migrated. The file contains a list of standard applications, such as Adobe Applications (Acrobat, Photoshop), Eudora, all Microsoft Office Applications, Lotus Applications, etc.
Migrate System Data	Defines if the contents of the Migsys.inf are to be taken into account. This configuration file controls which operating system and browser settings are migrated. It includes amongst others the following options: Accessibility Options, Display Properties, Folder Options Fonts, Internet Settings, Internet Security Settings, Localization / International Settings, Mouse and Keyboard, etc.
Migrate User Data	Defines if the contents of the Miguser.inf are to be taken into account. This configuration file controls which user file types and desktop settings are migrated. The components in this file include amongst others: Desktop, Favorites, My Pictures, My Documents, Shared Documents, Start Menu Items, etc.
Only Local User	Migrates only the specified users and/or domains. Enter the desired user into the field. You can specify multiple users through a semi-colon separated list. If you have checked the **All Users** option above, any values entered in this field is ignored.
Overwrite	Overwrites any existing data in the store. If not specified, Scanstate fails if the store already contains data.
Create Log File	Defines if a log file is to be created. It is located in the directory of the Mig file.
USMT Installation Path	Specifies the location of the scanstate.exe file which launches the data and profile backup.
Windows XP Target	

Parameter	Description
	Optimizes ScanState when the destination computer is running Windows XP. You should use this option as this optimizes ScanState because the store only contains components that pertain to Windows XP. This shortens the amount of time that ScanState takes.

Save Windows Data and Profile (USMT 4)

You must run this step on Windows XP Pro from an account with administrative credentials, or some operating system settings may not migrate - for example, wallpaper settings, screen saver selections, modem options, media player settings, and Remote Access Service (RAS) connection phone book(.pbk) files and settings. For this reason, we recommend that you run it from within an account with administrative credentials.

When running this step on Windows Vista, you need to run it in “Administrator” mode from an account with administrative credentials to ensure that all specified users are migrated. This is because User Access Control (UAC) is turned on in Windows Vista. If you do not run the step in “Administrator” mode, only the user profile that is logged on will be included in the migration.

This step starts the Microsoft scanstate.exe file that creates an intermediate store that contains the user files and settings from the source computer.

The following operating systems are supported:n- Windows XP Pron- Windows Vistan- Windows 7

The loadstate.exe file, launched by the Restore Windows Data and Profile step, restores these files and settings to the destination computer. Scanstate does not modify the source computer. By default, scanstate compresses the files and stores them as an image file (USMT3.MIG).

Parameter	Description
Administrator Name	Enter a valid login name to the backup device into this field, with which the operational rule logs on to the device.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
All Users	Checking this option migrates all of the users on the computer.
Data Compression	Enables compression of data and saves the files to a hidden folder named File at *StorePathUSMT* . This option cannot be used in combination with the encryption option below.
XML Configuration File Path	Specifies the *Config.xml* file that the process should use to recuperate the store. The path must be a full path.
Continue on Error	If activated, the process continues to run even if there are nonfatal errors. Without this option, ScanState exits on the first error. When you specify this option, any files or settings that cause an error and are ignored is logged on the progress log. In addition, if a file is open or in use by an application, USMT may not be able to migrate the file and logs an error.
Additional Customized XML File Path	Specifies an .xml file that contains rules that define what state to migrate. The path must be a full path.

Parameter	Description
Destination Host Name	Enter the name of the host on which the backup is stored. If the destination host is the relay leave the field empty.
Backup on Relay	Check this box if the backup is to stored on the relay. In this case do not provide a name in the field above, otherwise there is conflicts.
Shared Target Folder	Indicates a folder where to save the files and settings
Encryption Key	Encrypts the data to store with the specified key (password). With this option, you need to specify the encryption key. We recommend that encryption key be at least 8 characters long, but it cannot exceed 256 characters. This option cannot be used in combination with the **Data Compression** parameter above.
Users to Exclude	Excludes the specified user(s) from the migration. You can specify multiple users separated by semi-colons (;). Domain name and user name can contain the asterisk (*) wildcard character, for example, *DomainNameUserName* .
Only Local Directories	Specifies that only files that are stored on the local computer is migrated, regardless of the rules in the .inf files. You should use this option when network drives are mapped on the source computer and is mapped again in the same way on the destination computer (for example, if you map drives using login scripts). If this box is not checked, then Scanstate copies files from network drives into the store.
Migrate Application Data	This check box defines if the contents of the MigApp.xml are to be taken into account. This configuration file controls which application settings are migrated. The file contains a list of standard applications, such as Adobe Applications (Acrobat, Photoshop), Eudora, all Microsoft Office Applications, Lotus Applications, etc.
Migrate Documents	Defines if the contents of the MigDocs.xml are to be taken into account. This file controls which personal documents/files are migrated.
Migrate User Data	Defines if the contents of the MigUser.xml are to be taken into account. This configuration file controls which user file types and desktop settings are migrated. The components in this file include amongst others: Desktop, Favorites, My Pictures, My Documents, Shared Documents, Start Menu Items, etc.
Only Local User	Migrates only the specified users and/or domains. Enter the desired user into the field. You can specify multiple users through a semi-colon separated list. If you have checked the **All Users** option above, any values entered in this field is ignored.
Overwrite	Overwrites any existing data in the store. If not specified, Scanstate fails if the store already contains data.
Create Log File	Defines if a log file is to be created. It is located in the directory of the Mig file.
USMT Installation Path	Specifies the location of the scanstate.exe file which launches the data and profile backup.
Windows XP Target	Optimizes ScanState when the destination computer is running Windows XP. You should use this option as this optimizes ScanState because the store only contains components that pertain to Windows XP. This shortens the amount of time that ScanState takes.

Service Management

This step manages the Windows services, that is, it verifies the current running status of an installed service and then may start/restart/stop the service or change the default start type.

Parameter	Description
Action to execute	

Parameter	Description
	Select in this box the action to be executed on the specified service.: • **Start if Stopped** : to start the Windows service if it is currently stopped, • **Stop if Started** : to terminate the Windows service if it is currently running, • **Restart** : to restart the currently running service, • **None** : Execute no action. This option must be selected if the start type is to be modified.
Service Name (Windows only)	Defines the name of the service to be managed.
Start Type	If the option was chosen in the field above you must select the new default start type for the specified service. The possible options and their behavior are the same as in Windows.
Send an alert	Check this box to send an alert.
Alert Description	Description of the alert to be sent. The values within the parenthesis are data that is replaced during execution. The description can contain environment variables (${}).
Alert Severity	Select the severity to be assigned to the alert.
Alert Sub-category	Enter the sub-category to which the alert is to be added. Be aware that this sub-category name may not have more that 64 characters.

Sharing Windows Folders

This step allows you to create and delete network shares. The shares are created with full access rights.

Parameter	Description
Share Name	Enter the name of the share.
Directory Path	Enter the path to the share to be created or deleted, for example: C:Temp.
Action	Define if a share is to be created or deleted by selecting the respective option in the dropdown field.

Uninstall MSI Package

This step uninstalls a software that was installed via an MSI package.

Parameter	Description
MSI Application Product Name or Code	Enter the name or the product code of the application to uninstall in this field. This must be the exact value as it can be found in the software inventory for the product name or the Uninstall string key of the Registry.
Wait for End of Execution	Check this parameter if the step is to wait for the end of the operation before declaring its execution terminated.

Unmount Network Drive

This step allows unmounting a network drive with a LocalSystem account.

Parameter	Description
Delete Access Rights of the Privacy List	Check this box if the access rights to this share are to be removed from the privacy settings of the local agent.
Drive Letter	Enter the letter of the share to be unmounted.

Unmount Network Drive as Current User

This step allows you to unmount a network drive as the currently logged-in user.

Parameter	Description
Drive Letter	Enter the letter of the share to be unmounted.

User Management

This step permits adding, removing or modifying user profiles.

Parameter	Description
Enable User	Activates or deactivates the user account. If the account is not active the user cannot have access to the server.
Add	Check this box if the user listed below is to be added to the list of local accounts.
User Password Authorisation	Defines if the user can modify his password.
Remove	Check this box if the user account listed below is to be removed from the local client.
Domain	This check box defines if the if the operations to be performed on the primary domain controller (PDC) of the current domain. If the box is not checked the operation is performed only on the local device. This option only applies to Windows XP Professional clients that are members of a domain. By default, server computers perform operations on the primary domain controller.
User Root Directory	Defines the path to the user's home directory. This entry is mandatory and the path entered must already exist, otherwise the account cannot be created.
Password Needed	Defines whether the user account must have a password.
User Profile Path	Sets a path for the user's login profile.
Login Script Path	Enter the location of the user's login script in this field.
User Name	The name of the user account to be added, deleted or modified. The name may have no more that 20 characters.
User Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).

User Profile Extraction via MigrationManager

This step alllows you to extract user profiles of a device using the MigrationManager

Parameter	Description
MigrationManager's host name	Enter the name or IP address of the device on which the MigrationManager server is located.
Use relay	Check this box to use the relay device as the MigrationManager server.
Shared folder	Enter the name of the network share of the MigrationManager server.
Data Storage Path	Enter the name of the directory in which the profiles are stored. The name must have the format NetworkPathNameProfileDirectoryName
Configuration File Path	Enter the name of the configuration file that specifies the profile data to save. The name must have the format NetworkPathNameConfigurationFileName.
Domain Name	Enter the domain name of the administrator who is to execute the extraction.
Administrator Name	Enter the name of the administrator who is to execute the extraction.
Administrator Name	Enter the name of the administrator who is to execute the extraction.

User Profile Injection via MigrationManager

This step alllows you to inject user profiles into a device using the MigrationManager

Parameter	Description
MigrationManager's host name	Enter the name or IP address of the device on which the MigrationManager server is located.
Use relay	Check this box to use the relay device as the MigrationManager server.
Shared folder	Enter the name of the network share of the MigrationManager server.
Data Storage Path	Enter the name of the directory in which the profiles are stored. The name must have the format NetworkPathNameProfileDirectoryName.
Configuration File Path	Enter the name of the configuration file that specifies the profile data to restore. The name must have the format NetworkPathNameConfigurationFileName.
Use Target File	Check this box if you want to use the target file located on the MigrationManager server. This allows you to use the profiles of a device on another device as well.
Domain Name	Enter the domain name of the administrator who is to execute the injunction.
Administrator Name	Enter the name of the administrator who is to execute the injunction.
Administrator Name	Enter the name of the administrator who is to execute the injunction.

Windows Session Status Verification

This step allows you to verify if the Windows session is open on the target.

No parameters need to be defined for this step.

Windows Device Management steps

This class groups all steps that are available for the management of all peripheral devices managed under Windows.

Create Device Management Rule

This step creates a management rule for a given peripheral device class. It is strongly recommended to not define rules for more than one device class per operational rule, that is, an operational rule for the scanners, another for the printers, etc.

Parameter	Description
Authorize	Defines if the selected device class is to be authorized of forbidden.
Filter Type	Defines according to which system the peripheral devices are to be filtered for activation/deactivation.
Filter	Enter the filter according to the above selected filter type. The possibilities are: • the exact name of the peripheral device to be managed for **Exact Match** ; • if you have selected **Contains** enter a combination of characters to find all devices of a specific vendor or type, for example, *Kingston* for all devices of the manufacturer Kingston, • enter a pattern to be found into the field if you have selected the **Pattern** option, for example, ***King*6*** , the asterisks (*) finds all devices, • or you may search for specific peripherals by entering a regular expression if you have selected the option **Regular Expression** .
Filtered Field	Select from this list of available fields the one to be filtered.
Class Type	Defines for which type of peripheral device the step is to be defined, for example, *USB HUB, USB Scanners, USB Storage Devices* , etc.

Disable USB Storage Write Access

This step disables write access to all peripheral USB storage devices that are either already connected to the devices in your network or that will be connected in the future. Once connected, these devices can be accessed in read mode only.

No parameters need to be defined for this step.

Disable WiFi for LAN Connection

This step disables all WiFi connections which are established for a device.

No parameters need to be defined for this step.

Disable Windows Burning Service

This step disables the built-in Windows' CD-ROM burning service.

No parameters need to be defined for this step.

Enable USB Storage Write Access

This step enables the usage of all currently connected peripheral USB storage mediums. This also enables any storage medium connected after the execution of the step.

No parameters need to be defined for this step.

Enable Windows Burning Service

This step allows you to enable the built-in Windows' CD-ROM burning service.

No parameters need to be defined for this step.

Reset Device Management Rule

This step allows you to cancel all existing management rules for a specific Windows peripheral device class.

Parameter	Description
Class Type	Select the class of peripheral devices for which all existing rules are to be cancelled, for example, for all USB HUBs, USB Scanners, USB Storage Devices, etc.

Wifi Status Verification

This step, executed during the verification phase, checks the Wifi connection status. If the connection is active it will stop with an error. If the LAN is enabled in addition to the Wifi the verification will fail depending on the setting of the parameter. The step is used, for example, to stop /forbid package downloads if a device uses a Wifi connection.

Parameter	Description
Do not stop on error if the LAN is active in addition to the Wifi	Check this box if the verification is not to fail if the LAN connection is also active. For a package download, for example, this would mean that it is allowed.

Windows XP and 2003 Firewall steps

This group of steps allows you to define the firewall settings for Windows XP SP2 (32 bit), Windows XP SP1 (64 bit), Windows 2003 SP1 (32 or 64 bit) and Windows 2003 SR2 (32 bit).

- Add or Edit a Firewall Rule
- Add or Edit an Open Port
- Change Firewall Status
- Configure ICMP Settings
- Delete Firewall Rules
- Delete Open Port

- Firewall Settings Inventory
- Restore Backup Settings
- Restore Default Settings
- Setting Backup

Add or Edit a Firewall Rule

This step allows you to add new rules (exceptions) or modify existing rules of the Windows firewall. Editing a program exception allows you to change the path or file name that is associated with the program and configure scope settings for the exception.

Parameter	Description
Application Name	Specifies the friendly name for the exception, which is displayed in the graphical user interface. This may be any string with less than 256 characters.
Address Range	Specifies one or more IPv4 addresses or IPv4 address ranges separated by commas (with no spaces). When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as *10.47.81.0/255.255.255.0*) or by using an IPv4 address within the range (such as *10.47.81.231/255.255.255.0*). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as *10.47.81.0/24*) or by using an IPv4 address within the range (such as *10.47.81.231/24*). The following is an example custom list: *10.91.12.56,10.7.14.9/255.255.255.0,10.116.45.0/255.255.255.0,172.16.31.11/24,172.16.111.0/24* .
Application Path	Specifies the absolute path to the executable (*.exe*) file used by the program or system service. You may use system variables to specify the location where the program is located on your target device.
Profile	Defines if the Windows Firewall settings are to be configured in the standard profile or the domain profile: • **Domain Profile** : Used when a computer is connected to a network in which the computer's domain account resides. • **Standard Profile** :Used when a computer is connected to a network in which the computer's domain account does not reside, such as a public network or the Internet. • **All** : If it is to be applicable to both profiles.
Scope	Select whether you want to allow this application to communicate to any source (*), which could include any device on the Internet, or your local network only (*Local Subnet*), which limits communications to devices on your local subnet.
Status	Select the value for the application.

Add or Edit an Open Port

You can configure the Windows Firewall to block all outside sources from connecting to the device, or you can open selected ports and mappings to allow specific services that you trust. This step allows you to add, i.e., open a port or modify an open port of the Windows Firewall.

Windows Firewall allows you to open ports to allow only traffic from addresses on your local subnet, or globally to allow traffic from any network location, local or on the Internet. The local setting is useful for allowing file and printer sharing, and other local networking services. When you configure ports, you can specify the port number and protocol, and then selectively turn that port setting on or off.

When you add a port to the exceptions list, you must specify the protocol (TCP or UDP) and port number. You cannot specify protocols other than TCP or UDP and you cannot add a port number without specifying either TCP or UDP. (For example, you cannot exclude traffic based on protocol alone.) When you add a TCP or UDP port to the exceptions list, the port is open (unblocked) whenever Windows Firewall is running, regardless if there is a program or system service listening for incoming traffic on the port. For this reason, if you need to allow unsolicited incoming traffic through Windows Firewall, you should create a program exception instead of a port exception. When you add a program to the exceptions list, Windows Firewall dynamically opens and closes the ports required by the program. When the program is running and listening for incoming traffic, Windows Firewall opens the required ports; when the program is not running or is not listening for incoming traffic, Windows Firewall closes the ports.

Parameter	Description
Name	Enter the port name of the service or program you want to allow to communicate through a port. This is the user friendly name that appears in the exceptions list in the graphical user interface, it may be any string less than 256 characters.
Address Range	Specifies one or more IPv4 addresses or IPv4 address ranges separated by commas (with no spaces). When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as *10.47.81.0/255.255.255.0*) or by using an IPv4 address within the range (such as *10.47.81.231/255.255.255.0*). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as *10.47.81.0/24*) or by using an IPv4 address within the range (such as *10.47.81.231/24*). The following is an example custom list: *10.91.12.56,10.7.14.9/255.255.255.0,10.116.45.0/255.255.255.0,172.16.31.11/24,172.16.111.0/24.* If you define values for this parameter, the previous parameter **Scope** is ignored.
Port Number	Enter here the port number of the program or service. To find the port number, consult the documentation for the program or service you want to use. Adding this port signifies the port is always open; unsolicited incoming traffic is always allowed to pass through the port unless you uncheck the **Allow Exceptions** option when changing the Firewall settings with the **Change Firewall Status** step.
Profile	Defines if the Windows Firewall settings are to be configured in the standard profile or the domain profile: • **Domain Profile** : Used when a computer is connected to a network in which the computer's domain account resides. • **Standard Profile** :Used when a computer is connected to a network in which the computer's domain account does not reside, such as a public network or the Internet. • **All** : If it is to be applicable to both profiles.
Protocol	Select the protocol, either TCP or UDP, which is to be allowed to pass the port from the drop down list.
Scope	Select whether you want to open this port for *Any source* , which could include any computer on the Internet, or *Local network only* , which limits opening the port to computers on your local network. There are two scope options: • * : signifies any computer including those on the Internet • **Local Subnet** : Allows traffic only from IPv4 or IPv6 addresses that can be reached directly by your computer.

Parameter	Description
Status	Select the value for the port.

Change Firewall Status

This step allows you to changes the status of the Windows Firewall, i.e., to enable or disable it.

Parameter	Description
Allow Exceptions	Check this box to specify that all unsolicited incoming traffic is dropped, including traffic that has been added to the exceptions list. This turns on the Windows Firewall and allows all exceptions to take effect. It is useful when you are connected to a public network, such as the Internet, or a non-secure private network. When you perform this procedure, all of the exceptions in the exceptions list are enabled.
Allow Notifications	When allowing notifications, Windows Firewall displays a **Windows Security Alert** dialog box (referred to as a notification) when a program attempts to listen for unsolicited incoming traffic. If you are a member of the *Administrators* group on the computer, the notification gives you the ability to add the program to the exceptions list. If you are not a member of the *Administrators* group on the computer, the notification informs you that a program attempted to listen for incoming traffic but was blocked.
Profile	Defines if the Windows Firewall settings are to be configured in the standard profile or the domain profile: • **Domain Profile** : Used when a computer is connected to a network in which the computer's domain account resides. • **Standard Profile** :Used when a computer is connected to a network in which the computer's domain account does not reside, such as a public network or the Internet. • **All** : If it is to be applicable to both profiles.
Status	Select the value for the change operation.

Configure ICMP Settings

This step configures the ICMP settings of Windows Firewall. In Windows Firewall, the ICMP settings are off by default. This means that no incoming or outgoing ICMP communications are allowed.

This protects the device against attacks such as cascading ping floods. ICMP is also used for network discovery and mapping, and allows computers on a network to share error and status information. Also you should use these settings if your organization uses the ping or tracert commands for troubleshooting. Usually, you configure these settings only once or on an as-needed basis.

Parameter	Description
Allow Incoming Echo Request	Check this box if messages sent to this computer is repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine. If disabled, commands that use the ICMP Echo message, such as ping or tracert, do not work.
	Check this option if the device is to listen for and respond to requests for more information about the public network to which it is attached.

Parameter	Description
Allow Incoming Mask Request	
Allow Incoming Router Request	Check this option if the device is to respond to requests for information about the routes it recognizes.
Allow Incoming Timestamp Request	Check this option if data sent to this device can be acknowledged with a confirmation message indicating the time that the data was received.
Allow Outgoing Destination Unreachable	Data sent over the Internet that fails to reach this computer due to an error is discarded and acknowledged with a "destination unreachable" message explaining the failure. If you are running network management software that uses ICMP Destination Unreachable messages, you need to enable this option.
Allow Outgoing Packet Too Big	Corresponds to ICMPv6 Type 2 (Packet Too Big) messages.
Allow Outgoing Parameter Problem	Check this option if a device is to reply to the sender with a "bad header" error message when it discards data it has received due to a problematic header.
Allow Outgoing Source Quench	Check this option if the device is to drop data and to ask the sender to slow down when its ability to process incoming data cannot keep up with the rate of a transmission.
Allow Outgoing Time Exceeded	Check this option if the device is to reply to the sender with a "time expired" message when it discards an incomplete data transmission because the entire transmission required more time than allowed.
Allow Redirect	Check this option if data sent from a device is rerouted if the default path changes.
Profile	Defines if the Windows Firewall settings are to be configured in the standard profile or the domain profile: • **Domain Profile** : Used when a computer is connected to a network in which the computer's domain account resides. • **Standard Profile** :Used when a computer is connected to a network in which the computer's domain account does not reside, such as a public network or the Internet. • **All** : If it is to be applicable to both profiles.

Delete Firewall Rules

Deleting a program exception (rule) removes the exception from the exceptions list and prevents the program from receiving unsolicited incoming traffic (unless a port exception or some other exception allows unsolicited incoming traffic to reach the program).

Parameter	Description
Application Path	Specifies the absolute path to the executable (*.exe*) file used by the program or system service. You may use system variables to specify the location where the program is located on your target device.
Profile	Specifies if the rule is currently applied to a specific profile such as the domain or standard profile, or if it is applicable to all profiles.

Delete Open Port

Deleting a port exception closes (blocks) the port and prevents the port from receiving unsolicited traffic (unless another port exception or some other exception allows unsolicited incoming traffic to reach the program).

Parameter	Description
Port Number	Enter the port number to be removed from the list of exceptions.
Profile	Defines if the Windows Firewall settings are to be configured in the standard profile or the domain profile: • **Domain Profile** : Used when a computer is connected to a network in which the computer's domain account resides. • **Standard Profile** :Used when a computer is connected to a network in which the computer's domain account does not reside, such as a public network or the Internet. • **All** : If it is to be applicable to both profiles.
Protocol	Select the protocol, either TCP or UDP, for which the port was defined.

Firewall Settings Inventory

This step gets the Windows Firewall settings and stores them in the custom inventory.

Parameter	Description
Authorized Applications	Defines if the list of exceptions concerning the applications are listed in the inventory.
Firewall Status	Uncheck this box if the status of Windows Firewall is not to be included in the custom inventory.
ICMP Settings	Clear this option if either you are not using ICMP settings or you do not want to include them in the custom inventory.
Open Ports	Clear this option if the open ports on the list of exceptions are not to be included in the inventory.
Profile	

Parameter	Description
	Defines if the values are to be included for all profiles or only for a specific type of profile, that is, the domain or the standard profile.

Restore Backup Settings

This step restores the Windows Firewall settings to the backup settings created by the Setting Backup step.

Parameter	Description
Backup Path	Enter the path to the directory in which the backup to be restored is located.

Restore Default Settings

This step restores all default settings of the Windows firewall.

No parameters need to be defined for this step.

Setting Backup

This step creates a backup of the current settings of the Windows Firewall in a specifically defined directory.

Parameter	Description
Backup Path	The relative or absolute path, including the file name, in which the backup is to be created.

Object Parameters

This section provides information about all object specific parameters. You will find information about the following CM objects here:

- Administrator
- Agent configuration
- Application Monitoring
- Compliance Management
- Custom Inventory
- Device
- Device Group
- Directory Server
- Operational Rule
- OS Deployment
- Packages
- Patch Management
- Query
- Report
- Resource Management

- Rollout
- Software License Management
- Transfer Window
- User

Administrator parameters

Parameter	Description
Login	The login name used by that administrator to get access to the system.
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Office Phone	The office telephone number of the administrator.
Home Phone	The home phone number of the administrator.
Mobile Phone	The mobile phone number of the administrator.
Email	The email address of the administrator.
Company	The name of the company the administrator works for.
Department	The department in which the administrator works.
Title	The job title of the administrator.
Employee ID	The unique identifier of the employee.
Location	The location of the user.
Account Enabled	Indicates if the account of the administrator is enabled. If an account was created but not yet enabled its login cannot be used to log on to the Console and the database. If the account is not enabled the administrator icon appears dimmed.
Modify Personal Information	Defines if an administrator who does not have write access to his account may still modify part of the accounts properties, that is, personal information such as name, home phone and the password.
Last Login	The time and date of the last login of the selected administrator in the default time format defined in the user preferences.
Created By	The name of the creator of the object such as an administrator.
Create Time	The date and time at which the object was originally created.
Last Modified By	Displays the name of either the last person that last modified the object or its contents, such as the administrator, or it may be the system that last executed any modifications.
Last Modification Time	The date and time of the last modification of the object.

Agent Configuration parameters

The following parameters are provided:

Security parameters

The parameters in this node define the options for secure agent communication. This includes the way the agents communicate between each other as well as the certificates being used for secure communication. For Windows devices the access to the MyApps Kiosk may also be defined.

Parameter	Description
Access Control	Defines the security when agents communicate with each other, that is, if the Precision Access Control (PAC) handshake is to be used for inter-agent communication: • **No** : as a server, allow PAC connections with client authentication as well as non PAC connections. As client, no PAC connections are required. • **Securised Send, Receive Both** : as server, allow PAC connections with client authentication as well as non PAC connections. As client, only allow PAC connections. • **Yes** : Only allow PAC connections (as server or client). • **Yes with mutual authentication** : Only allow PAC connections (as server or client) with mutual authentication.
Secure Communication	Defines if the agent communicates in secure format. The possible values are: • **No** : The agent accepts both securized and non-securized communication, however it sends only non-securized communications. • **Securized Send, Receive Both** : The agent accepts both securized and non-securized communication, however it sends only securized communications. • **Yes** : The agent only communicates in secure mode, that is, it only receives and sends securized communication. • **Yes with mutual authentication** : The agents communicate in secure mode and in addition authenticate each other via SSL.
Authority Certificate	Defines the name of the certificate authority which is currently configured.
Trusted Authorities	Defines the list of names of the trusted authorities configured which the local agent may trust for communication.
User Certificate	

Parameter	Description
	The integration defined final certificate to be used for the server role. It expects a certificate name (without extension) registered in the Agent certificate store (integration section), for example, *Numara, enterprise, starfleet* .
Integration Certificate	Defines the list of names of the trusted authorities configured which the local agent may trust for communication.
Current Integration Certificate	The currently used integration defined final certificate for the server role. This is a certificate name (without extension) registered in the Agent certificate store (integration section), for example, *Numara, enterprise, starfleet* .
Block Navigation from Agent User Interface	Check this box if the agent user interface is to be run in the browser's kiosk mode (fullscreen without menus or naviation bar). The installation of an add-on may be necessary to be able to use this mode (for example, with Firefox).
Strict Agent User Interface Authentication	Indicate ifthe user can apply operational rules assigned to the device without explicit authentication. If the strict authentication mode is disabled the user is able to execute operational rules locally without authentication. Enabling this parameter forces user authentication for all cases. This parameter is ignored for rules that are assigned to users.

Communication

The parameters of this node define the basic access settings for the communication between the agents via different methods for relay selection as well as agent and console, such as the different ports of communication, the timeouts for different types of communication and the frame and connection queue sizes.

The following topics are provided:

- Parameters parameters
- Advanced parameters

Parameters parameters

This panel defines how client agents determines which relay agent to use for all communication. nThere are two basic modes:nn- Static Relay: clients always use the selected relay and do not attempt communication with another relay. This is typically used for smaller LAN environments that do not use many relays.n- Auto-select Relay: clients attempt to find a relay using one or more of the selected methods in the order defined below: if a method cannot find the relay, it returns and the next method in the list is tried.nnConfiguring auto-selectionnIt is advised to use the DHCP method first in well-configured DHCP environments, by adding a new extended option that provides the relay information.nAnother common primary method is the **Relay List** which is hosted on the master server and allows mapping of IP subnets to relays.nnThese can be well complemented by the **Static Relay** or **Backup Relay** as secondary methods (that is, if **DHCP** and **Relay List** were not able to find a suitable relay, a list of backup or a static relay is used).n **Backup Relay** is also well suited for agents that connect through the internet and do not have access to DHCP or the master server. In this case, one or more Internet facing relays can be added to the backup relays.nn **Auto-discovery** lets client agents perform a network scan on either a pre-defined range of IP addresses or a number of neighbors surrounding their IP address. This has to be used

cautiously as it creates network traffic and requires good configuration so agents efficiently find their relays.nn **Custom Script** is used when none of the built-in methods mentioned above fits the environment and a customized script is available to handle relay discovery.

Parameter	Description
Port	The TCP port number of the parent on which it communicates with its children.
Console Port	The number of the port that the console uses for communication with the agent.
Parent Name	The name of the direct parent to which the target device is to be connected. This is either the master or the new device's relay on the next higher level. The name may be entered as the short or long network name, that is, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, that is, *192.168.1.1* or *2001:db8:85a3::8a2e:370:7334* . You may also select the parent from the list of available devices by clicking the **Add Device** icon and selecting the desired parent from the appearing list.
Parent Port	The port number of the direct parent to which the device is connected.

Related topics

- Auto-discovery parameters
- Backup Relay parameters
- Custom Script parameters
- DHCP Extended Option parameters
- Relay List Server parameters
- Static Relay parameters

Auto-discovery parameters

The autodiscovery mechanism provides an automatic parent discovery based on network probes for which the AutoDiscovery module must provide the list of available relays. The autodiscovery results are processed in sequence taking into account the priorities; two relays with the same priority will be processed arbitrarily.

Parameter	Description
Address Range	The list of addresses to be verified. The IP addresses can be listed in the following different notations: • Dotted notation, for example, 94.24.127.24 • With the short or complete network name such as *scotty* or *scotty.enterprise.com* • A mixture of both: *94.24.127.24, scotty.enterprise.com* .If the complete IP address range declaration is incorrect, the current subnet is scanned by default from address x.x.x.1 to x.x.x.254. If no IP address range is specified, the current subnet is scanned by default from address x.x.x.1 to x.x.x. 254.
Can Learn	If set to true, this value specifies if the agent can get other agents' autodiscovered devices in order to establish its list.

Parameter	Description
Fast Address Verification Interval (sec)	Defines a fast search option to find the client's relay. If the list of devices is empty, the **Fast Address Verification Interval** value is used to verify devices until the **Scan Count** value is reached and all devices have been verified or a relay was found. If the client has a relay the **Address Verification Interval** value is used. If the IP address is modified, the **Fast Address Verification Interval** value is used to verify devices. The option is deactivated if the value is set to the same value as the **Address Verification Interval** value. As long as the AutoDiscovery is at the research for the device's relay, the **Parent Selection Retry Interval** to find the backup server is ignored.
HTTP Port Range	The range of ports to scan for an agent HTTP server. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 1610 and 8080 is scanned.
Maximum Device Age (sec)	The maximum age in seconds for an entry in the device list. This displays the maximum time a device can stay in the list of devices after last being verified.
Maximum Hop Count	The number of routers between the device providing the list and the device being read. The hop count is determined at discovery time using the ping. It provides an indication of the distance between the two devices and is used at the time of relay selection to sort the devices which are farther to the end of the list of relays being contacted. For example, all devices on the same LAN segment have a hop count of 0 as they can contact each other directly.
Number of Neighbors	Defines how many neighboring addresses to scan. The default value is 10, meaning 5 addresses below the device's own address and 5 addresses above it.
Only Learn Relays	Defines if the complete list of autodiscovered devices is sent to the master or if only the list of relays is uploaded.
Operating System Detection	Specifies if the operating system is discovered on the device found by AutoDiscovery.
Same Network Only	Specifies if devices found on other networks are to be accepted. The possible values are the following: • **No filter applied** : There is no filter applied to any of the discovered devices. • **Clients only** : All discovered client devices must be on the same network as the discovering device. • **Relays only** : All discovered devices, which have their relay function enabled, must be on the same network. • **All devices** : All discovered devices must be on the same network.
Scan Count	Each time scan count addresses have been verified, the module refreshes the list of addresses to verify by using the **Address Range, Number of Neighbors** and **Use Network Neighborhood** settings.
Timeout (sec)	The timeout in seconds for pings.
TCP Port Range	The range of ports to scan for a TCP connection. This is used in place of ping when raw sockets are not available. All specified port ranges is scanned for ALL listed IP address ranges! If no port range is specified only default ports 23, 25 and 139 is scanned. Each port range can consist of: • only one port number • one port range with the start and end port numbers separated by a dash , • several port ranges and/or individual port, for example: 10000-10100,20000,21000-22000 • Several port ranges must be separated by either a space, a comma (,), a semicolon (or a colon (.If the whole range declaration is incorrect only default port 10000 is scanned.

Parameter	Description
Upload AutoDiscovery Objects	Defines if the objects discovered by the AutoDiscovery are uploaded.
Upload Interval (sec)	Defines the upload period for the autodiscovered list in seconds. If it is set to 0, no uploads are configured by the module, but they can still be managed through operational rules. The setting only configures the upload of existing data, it does not include an update of the inventory.
Upload on Startup	Defines if the autodiscovered list is uploaded to the master after being updated the first time on agent startup. It is not recommended to activate this option as, depending on the size of your network, this might be a very time and resource consuming process.
Use Network Neighborhood	Defines whether the network neighborhood should be used to get machine names and addresses.
Address Verification Interval (sec)	The gap in seconds between each address verification.

Backup Relay parameters

This mechanism uses the values of the Backup Relays parameter. The listed candidates will be processed in sequence, taking into account the configuration order. If the Backup Relays parameter is empty the mechanism exits and the next listed mechanism is tried. This method should be the last in the list, as it provides fallback parents.

Parameter	Description
Backup Relays	A list of backup parents to be scanned if during the auto selection no suitable parent is found through AutoDiscovery. The format is *host1:port1,host2:port2,* etc. *Host 1* is the closest alternative to the regular relay and the last host listed is typically the master. The host name can be entered either as its long or short network name, for example, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, for example, *192.168.56.4* or *2001:db8:85a3::8a2e:370:7334* . If the port number is not listed the default port *1610* is assumed.
Execute Script at Connection to Backup Relay	Allows to execute a specific Chilli script every time when a connection is established with a backup relay. Enter here the absolute path to the Chilli script.
Execute Script at Disconnection from Backup Relay	Allows to execute a specific Chilli script every time when the connection with a backup relay is terminated. Enter here the absolute path to the Chilli script.

Custom Script parameters

This option offers a generic mechanism to implement any algorithm if the built-in solutions are not sufficient. It requires the Script Path parameter to be filled in to locate the script to executed. If this parameter is empty, the mechanism exits and the next listed mechanism is tried.

Parameter	Description
Script Path	Provides the relative or absolute path to the script. The path may also be entered as a valid URL starting with _ http://_ or _ https://_ , in which case the script is downloaded every time it is referenced. This parameter is mandatory of the **script** option is listed as a dynamic relay selection mechanism in the **Mechanism List** field.

DHCP Extended Option parameters

The DHCP mechanism executes a DHCP request with the option defined via the Dhcp Extended Option parameter. If this parameter is empty, the mechanism exits and the next listed mechanism is tried.

Parameter	Description
DHCP Extended Option	The number of the option defined in the DHCP Server that corresponds to the relay.

Relay List Server parameters

This method calls an action on the defined list server URL to map the agent IP subnet to a preferred relay by order of priority. By default, it is advised to use the master server as list server. If the List Server URL parameter is empty, the mechanism exits and the next listed mechanism is tried.

Parameter	Description
List Server URL	The URL to the BCM agent on which the actions to find the appropriate relay are to be executed, generally this is the Master.

Static Relay parameters

This mechanism is the simplest one. The mechanism will exit if no parent name is configured. In this case, subsequent mechanisms configured in the sequence would be tried. The static mechanism represents the static mode capabilities offered to the dynamic mode. Having such a mechanism can be interesting since users may decide to revert back to a static configuration if none of the configured dynamic mechanisms succeed.

Parameter	Description
Static Parent Name	The name of the direct parent to which the target device is to be connected in static mode. This value is ignored if the dynamic relay selection is activated, that is, at least one value is entered in the **Mechanism List** field. The direct parent is either the master or the new device's relay on the next higher level. The name may be entered as the short or long network name, that is, *scotty* or *scotty.enterprise.com* or as its IP address in dotted notation, that is, *192.168.1.1* or *2001:db8:85a3::8a2e:370:7334* . You may also select the parent from the list of available devices by clicking the **Add Device** icon and selecting the desired parent from the appearing list.
Static Parent Port	The port number of the direct parent to which the device is connected in static mode. This value is ignored if the dynamic relay selection is activated, that is, at least one value is entered in the **Mechanism List** field.

Advanced parameters

The parameters of this tab allow you defined specific aspects of the communication between the agents and agents and console.

Parameter	Description
Default Timeout for TCP Based Communications (sec)	A timeout defined in seconds used by the agent for network communication.
Default Timeout for TCP Based Connections (sec)	A timeout defined in seconds used by the agent for network connection.
Frame Size (Bytes)	Defines the frame size of the network type which the device uses for communication. This parameter must only be modified for devices using non-ethernet networks, such as token ring, frame relays or ATM networks.
Connection Queue Max Size	The maximum number of queued incoming connections.
Tunnel Timeout (sec)	The timeout in seconds is used to verify if the tunnel connection is still alive.

User Interface parameters

These parameters define the settings for the MyApps kiosk, that is, if packages that are published to a device, appear in the systray, and, if not, if a message is displayed on the local device in its stead.

Parameter	Description
Icon Mode in SysTray	Defines the mode of the icon in the systray.
Publish New Packages	Check this box if a package icon is to be displayed with the agent systray icon whenever a new package is published. This parameter is only applicable if the systray mode is set to **dynamic** . If set to **hidden** the parameter **Message for New Packages** applies.
Message for New Packages	The value of this entry indicates, if a pop-up window must appear, when an operational rule is published while the systray is hidden.
New Advertisment Banner (Days)	Define the length of time in days that the **New** banner should be shown for operational rules that are newly published in MyApps. Setting this number to zero disables the new banner.

Reboot Management parameters

The parameters defined in this section define the default reboot settings.

Parameter	Description
Non-intrusive Reboot Mode	

Parameter	Description
	Check this box if the reboot requested by an operational rule or a patch installations is to be effected in a non-intrusive way. If activated, any rule or patch waits after its execution for a specified amount of time for another object to arrive to combine their required reboot requests into one. If no other rule or patch arrives, the device is rebooted as defined.
Reboot Interval	Defines the waiting time in seconds that the agent waits after receiving the reboot command and executing it. If the rollout is of type uninstall, it is recommended to reboot the device after the uninstall has terminated.
Max. Number of Reboots	Specifies the maximum number of times a device can be rebooted per day. The default value is 2 reboots per day, 99 is the maximum number of times a device can be rebooted per day. 0 deactivates this option, that is, the device is not rebooted, even if a patch requests it or it is assigned a reboot window; all reboots must be launched manually.
Synchronize at Startup	Check this box if the reboot windows are to be synchronized at every startup of the agent. In this case the local agent compares its list of reboot windows with the master list and updates it accordingly by downloading missing reboot windows, updating modified ones and deleting removed ones.
Additional Automatic Synchronization Hour	Enter here the hour at which an additional reboot window synchronization is to be effected, that is, the comparison of locally available reboot window with the reboot window master list. The format is 24-hour format, for example, *23* for *11 pm* .
Minimum Gap between Two Automatic Synchronizations (sec)	Defines the minimum interval in seconds at which the reboot window synchronisations are to be done. This means that if a default synchronisation is executed at 23:00 at night and the client is started at 6 am with agent startup synchronisation defined, no synchronisation will be executed until at least 11 am even if the agent is started/restarted before, as the interval is fixed for 12 hours minimum.

Module Configuration

This node provides access to all CM modules that are currently loaded on the selected device. Here you may modify configuration parameters and access local information on the respective module.

Modules in CM are responsible for a certain functionality in the product. Their settings are defined through individual configuration files, one per module which are stored in the config directory. The modules themselves are stored in the modules/agent directory in the form of one .dll file for computers with a Windows operating system, for MAC OS or Linux systems you can see there one .so file per module

For detailed information on the available modules and their parameters refer to section Module Parameters of this manual.

Application Management parameters

The following parameters are provided:

- Custom Applications
- Application Monitoring

Custom Applications

Parameter	Description
Application Type	Indicates via which type the application was added to the list of managed applications, that is, if it was added from the software inventory or as a user defined application.
Installed Count	The number of times the application is installed on the devices in the network.
Version	The version number of the application.
File Name	The name of the executable file of the application.
File Checksum	The checksum of the executable file of the application.
File Size (Bytes)	The size of the executable file of the application.

Application Monitoring

Parameter	Description
Type	Select the application type of the application list, that is, if the applications of the list are to be monitored, protected or prohibited.
Local Backup Copy	Defines if a copy of the protected application is to be stored on the local device.
Protect Sub-directories	Defines if the protection scheme includes the sub-directories of the application directory. This may be applicable for larger applications having sub-directories with do not only contain user created but application data, such as libraries or filters.
File Type Filter	By default all files in the main directory as well as the sub-directories if specified are included. If you do not want to include all files enter into this field the list of file extension which are to be included in the selfhealing package. The files are a comma separated list with wildcard characters, such as **.exe,**.dll,**.bat, etc. If you are limiting the files to be protected they should not include any type of file that is user created, such as *.doc,**.txt, etc., as newer files may be erased by older ones in case of a selfhealing operation. You may also exclude these via the next parameter.
Exclude File Types	By default all file types are included for protection and selfhealing. In this field you may specify a list of file types which are not to be protected and thus included in the selfhealing package. The files are a comma separated list with wildcard characters, such as **.txt,**.doc,*.tmp, etc. In this field you may limit for example any type of file that is user created, such as Word documents, Excel spreadsheet, etc., as newer files may be erased by older ones in case of a selfhealing operation.

Compliance Management parameters

The following compliance parameters are noted.

Configuration

Parameter	Description
Evaluation Frequency (min)	Defines the interval in minutes at which the compliance rules is newly evaluated. If no value is specified, the rules are evaluated at agent startup, otherwise the automatic evaluation feature is deactivated.

Compliance Rule

Parameter	Description
Last Evaluation Date	The date and time of the last evaluation.

Constants

Parameter	Description
Type	Select the type of the constant, this may be either *Integer, String* or *Date/Time* .
Value	Enter the value the constant is to represent, that is, a specific path *C:Program FilesBMC SoftwareClient Management* , a specific value such as a service name *BCM Agent* , etc.

Custom Inventory Object Type parameters

Parameter	Description
Attribute	Enter the name for the new attribute.
Data Type	Select the data type.
Alias	Enter the alias under which the new attribute is displayed in reports. The default value is the attribute name.

The parameters of a Device object

The device object is one of the main objects of CM , it can have different roles and functions in the network and thus a lot of different information is available for it. This information displays in the form of tables in the right window of the **General** tab. In the **Properties** window of a device this information it is divided into different panels to make it easier to find.

- Basic Device Information
- Advanced Device Information
- Agent Details
- Operating System Details
- Agent Roles
- Customized Information

Basic Device Information

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
User	Click the icon next to this field and select the user to assign from one of the appearing list views.
Location	The country/region/town/building/geographical area at which the asset is located.
Last Update	The date and time at which the device information was last updated.
Type	

Parameter	Description
	The type of the device, that is, which purposes the device server, if it is a server, a workstation, a printer or a game console, etc. You can manually modify this value. However, in this case you also need to deactivate the automatic updates, otherwise the device type reverts to its original type at the next update. To switch to manual update click the icon next to the box, which appears when you manually change the type.
IP Address	The IP address of the device in its dotted version, such as *194.50.68.255* or *2001:db8:85a3::8a2e:370:7334* .
Topology Type	The topology type of the device, that is, if the managed device is a master, a relay or a simple client. It may also be an unconnected, a scanned, a deprecated or an unknown device.
Domain Name	The full name of the domain the currently selected device belongs to, that is, *kirk.enterprise.starfleet.com* .
Operating System Name	The name of the operating system installed on the currently selected device.
Host ID	If the operating system is Window it either displays the asset tag or the BIOS serial number depending on the manufacturer of the client. If the operating system is Linux this is the equivalent of the_hostid_ command. If the operating system is MacOS this value displays the system serial number that appears in the **About This Mac** window or in the **System Information** .
Parent	Displays the name or the IP address of the parent of the device. In case of the master or unconnected devices this field is empty.
Virtualized on	Defines the type of virtual machine running on the host, that is, the name of the software used. This may be either *None* if no virtual machine is installed on the device, *VM Ware Server, Microsoft VirtualPC Server, VirtualBox* or *Parallels* .

Advanced Device Information

Parameter	Description
Hosts a hypervisor	Displays if the agent device hosts a hypervisor, in which case this field displays the name of the virtualizing software, otherwise it is empty.
Hypervisor Version	The version number of the hypervisor.
Network Name	The network name of the machine, either as its short or complete network name, for example, *scotty* or *scotty.enterprise.com* , or as its IP address in dotted notation, for example, *194.45.245.5* or *2001:db8:85a3::8a2e:370:7334* .
NetBIOS Name	The NetBIOS name of the currently selected client. For managed devices which have Linux or MAC OS as their operating system this field is empty.
Subnet Mask	The subnet mask of the device.
MAC Address	The MAC (hardware) address of the discovered device.
Disk Serial Number	The serial number of the hard disk of the device.
Under NAT	Indicates if at least one piece of hardware of the device uses network address translation. This box is automatically checked if this is the case.
	Indicates if the device is equipped with Intel's vPro firmware.

Parameter	Description
Intel VPro Available	

Agent Details

Parameter	Description
HTTP Port	The range of ports on which the HTTP server listens for and sends data from.
HTTP Console Port	The number of the port that the console uses for communication with the agent.
Secure Communication	Defines if the agent sends any communication in secure format.
Agent Version	The version number of the BCM agent if it is installed on the device.
Patch Knowledge Base Version	The currently installed version of the configuration files of the Patch Management functionality.

Operating System Details

Parameter	Description
Operating System Version Major	The major version number of the operating system installed on the device.
Operating System Version Minor	The minor version number of the operating system installed on the device.
Operating System Revision	The revision number of the operating system installed on the currently selected device.
Operating System Build	The build number of the operating system installed on the device.

Agent Roles

Parameter	Description
Packager	Indicates if the currently selected device is a *Packager* in the **Package Factory** , that is, if packages may be created on it. If this option is set to **No** , the device is not visible under the **Package Factory** node.
Patch Manager	Indicates if the currently selected device is serving as a Patch Manager, that is, if it may handle MS Secure files and all other options pertaining to patch management. If this option is set to **No** the device is not displayed under the **Patch Manager** node.
OSD Manager	Indicates if the currently selected device is a OSD Manager, that is, if it can create and manage operating system deployments as well as install them on the defined target devices. If this option is set to **No** , the device is not displayed under the OS Deployment node.
Asset Discovery Scanner	Check this box if the device is to be an Asset Discovery Scanner.
Rollout Server	Check this box if the device is to be a Rollout Server.
Web Service	Check this box if the Web services are to be active on this device.
Directory Server Proxy	Check this box if the device is to be a Directory Server Proxy.

Customized Information

This panel displays the list of all device attributes that are defined as visible with their respective values. You can change the individual values in this window.

The parameters of a Device Group object

The device group object is one of the main objects of CM because it is used by many different CM functionalities. Its information displays in the form of tables in the right window of the **General** tab.

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
Display Nodes	Defines which subnodes the new group node should display. Possibilities are: • **Members** only displays all group members. • **Functionalities** displays only all the maintenance and manipulation subnodes for a groups. • **All** displays both types of subnodes.
Device Type	Defines which types of devices are to be displayed, if above you have decided to do so. Possible options are: • **All Devices** displays all devices which are known in the database. This includes scanned devices as well as deprecated devices. • **Devices with Agent** displays only devices on which a BCM agent is installed.

Directory Servers parameters

The following directory server parameters are provided:

- MS Active Directory
- LDAP Server
- IBM Domino
- Novell eDirectory

MS Active Directory

Parameter	Description
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.
Type	Select from this dropdown list the type of directory server that is to be defined.
AD Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .

Parameter	Description
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Domain Alias	By default this field remains empty. If a value is supplied, it is used as the user domain for Administrator and User objects instead of the domain name retrieved from BaseDN.
Anonymous Access	Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.
Authenticated Access	Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in.
User	Defines the name uniquely identifying the user: • **sAMAccountName notation** , example *DOMAINUser* , this is the recommended syntax • **LDAP notation** , for example, *cn=username, cn=usergroup* where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory *Users and Computers* • as the **simple user name** , for example, *administrator* (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain). • **UPN notation** , for example, *user@domain.com* (for users in other than the AD domain).
Password	Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).

LDAP Server

Parameter	Description
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.
Type	Select from this dropdown list the type of directory server that is to be defined.
LDAP Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Base DN	Enter the unique name of the base DN to which you want to connect. The base DN is the entry point to the directory organization and different from all others. You can enter this value either in LDAP or UNC format. For example: the entry *world.entreprise.com* of Active Directory can be entered in LDAP notation as *dc=world, dc=enterprise, dc=com* or as *world.enterprise.com* in UNC notation.
Domain Alias	This field is empty by default. If you enter a value it is used as the user domain for the object types **Administrator** and **User** instead of the domain name that was recovered via the base DN. For example, a user who is registered under *europe.world.enterprise.com* could be indicated via his OU called *Americas* .

Parameter	Description
Anonymous Access	Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.
Authenticated Access	Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in.
User	Defines the name uniquely identifying the user: • **sAMAccountName notation** , example *DOMAINUser* , this is the recommended syntax • **LDAP notation** , for example, *cn=username, cn=usergroup* where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory *Users and Computers* • as the **simple user name** , for example, *administrator* (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain). • **UPN notation** , for example, *user@domain.com* (for users in other than the AD domain).
Password	Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).

IBM Domino

Parameter	Description
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.
Type	Select from this dropdown list the type of directory server that is to be defined.
Domino Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Organizational Unit	The name of the Domino organizational unit to which the user belongs, similar entity to the alias and OU of Directory Server, for example, a Domino directory of which the organization name is *World* and which includes the organizational units *Americas* , *Europe* and *Asia* .
Anonymous Access	Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.
Authenticated Access	Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in.
User	Defines the name uniquely identifying the user:

Parameter	Description
	• **sAMAccountName notation** , example *DOMAINUser* , this is the recommended syntax • **LDAP notation** , for example, *cn=username, cn=usergroup* where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory *Users and Computers* • as the **simple user name** , for example, *administrator* (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain). • **UPN notation** , for example, *user@domain.com* (for users in other than the AD domain).
Password	Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).

Novell eDirectory

Parameter	Description
Name	Enter the user-friendly name of the directory server, under which it is known, into this field. This name may be any combination of characters.
Type	Select from this dropdown list the type of directory server that is to be defined.
eDirectory Server Name	Enter the known network name of the directory server in this field. This value may be either the complete (recommended) or short network name, such as *scotty.bridge.enterprise.com* or *scotty* , or it may be the IP address of the server in its dotted notation, for example, *175.175.2.1* or *2001:db8:85a3::8a2e:370:7334* .
Port Number	Enter the number of the port in this field at which the directory server database may be accessed (389 by default).
Context	The name of the context that is to be referred in eDirectory. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings and is the same as a complete domaine name in Active Directory. A context called *world.enterprise.com* that redirects to the directory part referencing the desired user.
Tree	The name of the eDirectory tree to which you want to connect. It corresponds to the client field of the same name provided by Novell in the **Advanced** settings; it is the same as an Active Directory **Alias** and may be required in certain cases. A user of context *europe.world.enterprise.com* may for example be part of a tree called *Americas* in which exists a unit *USA* .
Anonymous Access	Check this radio button if you want to log on to the directory server with an anonymous login. Depending on the ACL lists of the server you may or may not be allowed to connect and/or synchronize. For security reasons it is recommended to not use this option. Checking this option is the same as using an authenticated access without specifying a user and password.
Authenticated Access	Check this radio button to log on to the directory server with a specific user login. The two fields below becomes accessible and need to be filled in.
User	Defines the name uniquely identifying the user: • **sAMAccountName notation** , example *DOMAINUser* , this is the recommended syntax • **LDAP notation** , for example, *cn=username, cn=usergroup* where username is the user you wish to connect as, and usergroup is the folder that contains username in LDAP/Active Directory *Users and Computers*

Parameter	Description
	• as the **simple user name** , for example, *administrator* (may be used if it is a login of the local AD domain and the server is entered as an IP address or short network name. If the AD is entered as a long network name if the login is a user in the specified domain). • **UPN notation** , for example, *user@domain.com* (for users in other than the AD domain).
Password	Enter the password for the directory server into this field through which the above defined user may access it. Be sure to enter the correct password, otherwise the directory server cannot be accessed from the Console. For security reasons the password is displayed in the form of asterisks (*).

Operational Rule parameters

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
Type	The type of the operational rule, which may be: **Quick Link** if the rule is to be published to the application kiosk containing only a URL. **Software Distribution** if a package is assigned to the operational rule for a software distribution, **Patch Distribution** if the rule distributes and installs a patch, or **Operational Rule** if it is any other type of action that is executed. An operational rule is always created with type *Operational Rule* . Once a package is assigned to it, its type is automatically set to *Software Distribution* . If the operational rule has been created through the assignment of a device under the **Packages** node, the type is automatically set to *Software Distribution* and the name of the operational rule is *[pkgname.ext]* , *pkgname* being the name of the package to be distributed, *ext* indicating the type of the package. The same is true for patch rules, which may not be created manually, they are always created automatically when a patch package is added to a patch group. In this case the *pkgname* is the name of the downloaded patch and the extension is always *.cst* for custom packages.

OS Deployment parameters

The following parameters are explained:

- Configuration
- Project
- Image
- Driver
- Disk Configuration
- Disk Configuration: Partition
- Target List
- Target List: Target Device: General Information
- Target List: Target Device: Parameters
- Target List: Target Device: Unattended Information

Configuration

Parameter	Description
Windows AIK Installation Path	The complete path of the Windows Automated Installation Kit (AIK). If not path is specified the default installation path (*C:Program FilesWindows AIK*) is used.

Parameter	Description
Driver Root Folder	The complete path of the directory into which the drivers are copied to for later use. Format: *[InstallDir] MasterdataOSDeploymentdrivers* .
TFTP Local Path	The local full path of the TFTP server root directory, for example, *C:PXETFTP* .
TFTP UNC Path	Enter into this field the network path to the shared TFTP server directory, for example, *[IP address OSD Manager] PXETFTP* .
TFTP UNC Credentials	The login name to the share on the TFTP server.
Use the internal TFTP server	Check this box if you want to use the internal TFTP server of the OSD module instead of specifically configuring your own TFTP server. Only use this option if you do not have another TFTP server running. If another server is running see the **Configure TFTP Server** section of your OSD manual on how to configure your existing TFTP server for use with the BCM OSD functionality first.
Internal TFTP Status	Shows the current status of the internal TFTP server. If the status *Executing* is displayed the TFTP server runs as expected. If another TFTP server is running at the same time an error is displayed in the Status due to a conflict between the internal and external server.
Internal DHCP	Check this box if you want to use the DHCP gateway of the OSD module instead of specifically configuring your own DHCP server. In this case a DHCP gateway is installed that is redirecting the computers to the OSD manager and get installed, instead of adding the necessary options to your existing DHCP server. If you do not use this option make sure you have a DHCP server on a different machine that is configured as explained in the configuration options of the **Prerequisites** topic, preferably with the 066/067 options.
Internal DHCP Status	Shows the current status of the internal DHCP server. If the status *Executing* is displayed the DHCP server runs as expected. If any other status value is displayed check if the DHCP server is configured as explained in the prerequisites.
DHCP Server Address	The IP address or DNS name of the DHCP server which redirects the PXE requests to the local TFTP server. The DHCP server must have the protocol BOOTP activated.
Skip DHCP Check	If the DHCP server is installed on the same device as the OSD Manager device you must check this box, as the DHCP server cannot be verified in this case. This test verifies if the BOOTP protocol is activated on the DHCP server.
Status	Displays the configuration verification status of the OSD Manager. If the status is not OK you finds an error message to indicate which parameter is incorrect.

Project

Parameter	Description
Description	Optional free text field in which you may enter additional information regarding the object.
Architecture	Select the type of architecture the project is to deploy.
Operation after Installation	The possible actions which may be executed after the installation of the operating system has finished on the target. This option is not applicable to the *Setup* mode.
Target Drive	Select from this field the drive letter for/of the operating system. If the project is for a Vista setup, the selected target drive must exist in the disk configuration selected for the project.

Image

Parameter	Description
Description	Optional free text field in which you may enter additional information regarding the object.
Architecture	Select the type of architecture the image is to be applicable to.
Type	Select the image type, that is, which operating system type it is to deploy.
Location	The network path to the image or setup folder, where the image files are located, for example, the *setup.exe* file for a setup deployment. This directory may be located on any device in your network, as long as it can be accessed by the OSD Manager. Depending on the mode selected for the image this may be for example: *192.168.196.13Vista32* .
Connection Parameters	The login and password to be used by the deploying device to access the network location in the required mode, that is, read and write mode for WIM Capture, read and execute for all other modes. To enter the login information click the **Edit** button next to the non-editable fields. A **Properties** window appears on the screen in which you must enter the login name and corresponding password in the respective fields and reenter the password for confirmation. The login name must have one of the following formats: *[domain name][user login] [local host name] [user login]* If the image share is located on the OSD Manager, the login and password MUST be the same to access this share as well as the access to the PXETFTP share. For security reasons the passwords is only displayed in the form of asterisks. To view the passwords you may also uncheck the **Hide Passwords** check box. Both password fields are now displayed in clear text format. To confirm the credentials click the **OK** button at the bottom of the window.
Custom Image Command Line	This field contains the command required to deploy the image, for example, *ghost32.exe -clone,mode* .
Status	Displays the verification status of the image. If the status is not OK you finds an error message to indicate which parameter is incorrect.

Driver

Parameter	Description
Driver .inf File	Enter the name and path of the .inf file of the driver. This is the path on the local device (OSD Manager) and to be entered as such with the drive letter as well as the name of the file, for example, *D:/Drivers/TEXTORM/chipset /Vista32/Ethernet/nvfd6032.inf* . You can also indicate a path to a removable device, such as a DVD drive, as the driver files is copied to a specific directory in the BCM Deploy. To find the file in its directory structure click the **Select** button next to the field. The **Driver File from [Device]** window appears on the screen. Browse the directories to find the correct file, select it and then click the **OK** button to add it.
Name	The user access name. It is simply used as a display name, but it must be unique anyway.
Version	The release date and version of the driver.
Manufacturer	The company that created the driver.
Type	The type of hardware the driver enables.
Description	A brief description of the driver by the manufacturer.
Supported OS	The list of operating systems supported by the driver.
Supported Hardware	The list of hardware devices supported by the driver.

Parameter	Description
Deployment Driver	Indicates is the new driver is a deployment driver (WinPE driver).
Status	The driver import status.

Disk Configuration

Parameter	Description
Name	Enter a name for the new disk configuration, for example *FullDisk_3Partitions* .
Description	Optional field. If it is used it should be a brief descriptive entry of the disk and what it represents.
Size (GB)	The size of the disk. It is only used to estimate if the partitions overall size is sensible. It has no impact on the real disk.
Delete Disk Partitions	Defines if any partitions that already exist on the target device are deleted. This option should be used with caution, as any data on the disk is lost irretrievably if selected.
Disk Number	The physical disk number on the device, 0 indicating the first disk, 1 the second, etc.
Status	Displays the current status of the disk configuration. If the status is not OK, the error message indicates the incorrect parameter.

Disk Configuration: Partition

Parameter	Description
Name	Enter a name for the new partition, for example, *Boot Partition* .
Description	Optional field. If it is used it should be a brief descriptive entry of the partition and what it represents.
Format	The format of the partition. Select **Do Not Format** , if the disk is not to be formatted but to use the current configuration, such as to keep another partition type for Linux or to keep partitions with existing data.
Type	The type of the partition if formatting the partition. Operating systems should be installed on primary partitions.
Extend	Use this option if the defined disk partitions do not completely use up the available disk space. Possible values are **Yes** (extend partition), in this case the size fixed for the disk is ignored and the remaining disk space is added to the respective partition. If you select **No** (do not extend the partition) the remaining disk space can not be used. Only one partition per disk may be extended. As FAT-32 disks may not be larger than 32 GB, extending it over this limit generates an error.
Size (GB)	The size of the partition. It is ignored if the **Extend** option is set.
Label	The unique name of the partition, for example, *SYSTEM, DATA* or *BACKUP* .
Drive Letter	The logical drive letter from C to Z assigned to the drive, each letter may only be assigned once. You may assign the partition a specific drive letter, however, WinPE may change this after rebooting if this does not coincide with its internal sorting logic.
Active Partition	Defines if a partition is active, that is, if it is potentially bootable. This partition must be used to install the operating system on, which is to be booted. Only one partition can be active per disk.
Partition Number	The unique physical partition number on the disk the currently selected entry belongs to, 1 is the first partition, 2 the second, etc.

Target List

Parameter	Description
Description	Optional free text field in which you may enter additional information regarding the object.
Architecture	Select the type of architecture the target list is to be applicable to.
Unattended File	The complete path to the template of the unattended file that is to be used for the OS deployment if the deployment type is *Setup* . BCM Deploy provides such templates for Windows XP and later. To select the location of the file instead of manually entering it, click the **Select** button next to the field. Select the location of the file. Click **OK** to confirm.

Target List: Target Device: General Information

Parameter	Description
Name	The user access name. It is simply used as a display name, but it must be unique anyway.
Description	Optional free text field in which you may enter additional information regarding the object.
Architecture	Select the type of architecture the target list is to be applicable to.
Enabled	Defines if the target device is active, that is, if it recuperates the image or setup file to install. If a target device is disabled, it must be activated manually via this option. If the associated project is already active then the files is generated automatically, without rebuilding the project.
Target	Defines that an individual target device is defined as opposed to a subnet mask. Only one of the following parameters must be defined.
Mac Address	Enter into this field the current MAC address of the target device. This is the most precise information to identify the device and should be preferred to the other two following identification options. The MAC address may be entered in one of the following formats: *xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx* or *xxxxxxxxxxxx* .
IP Address	Enter into this field the current IP address of the target device in its dotted notation. This option may be used if the MAC address is unknown and device is already running. In this case the respective target device tries to find its MAC address and provides this information.
DNS	Enter into this field the current DNS information of the target device. This option may be used if the MAC and IP addresses are unknown and device is already running. In this case the respective target device tries to find its IP address which in turn then searches for the MAC address and provides this information.
Description	This field displays the IP address for the subnet which contains the target devices. A new field next to the **Name** field appears in the window. You may enter into this field the way the device names within a subnetwork are automatically incremented. The default value here is *001* , that is, the name with the suffix *001, 002* , etc., for example, *HQ001, HQ002, ... HQ099* . This option may only be used for setup and sysprep deployments.
PXE Subnet Filter	This is a filter in the format *192.* **or *192.168.*** or *192.168.0.** to easily target an entire subnet.

Target List: Target Device: Parameters

Parameter	Description
Edition	Select from the drop-down box the Windows edition that is being installed, for example, Windows Vista Enterprise. The listed editions have been automatically detected from the installation CD/DVD.
Language	

Parameter	Description
	Select from the drop-down box the language. This language setting is applicable to the setup, the operating system to be installed, the keyboard layout and the user locale. The listed languages have been automatically detected from the installation CD/DVD.
Product Key	Defines the preformatted input for the OS product key (for example: *ABCDE-FGHIJ-KLMNO-PQRST-UVWXY*). Replace the standard key already entered in this field with the key provided by Microsoft on your installation DVD.
Dynamic IP	Select this radio button to dynamically assign the IP addresses for the devices. This option is only applicable to *Setup* projects.
Static IP	Select this radio button if the IP addresses are statically assigned to the devices. The following fields must be defined for static IP addressing:
IP Address	Enter into this field the current IP address of the target device in its dotted notation. This option may be used if the MAC address is unknown and device is already running. In this case the respective target device tries to find its MAC address and provides this information.
Subnet Mask	Enter into this field the subnet mask for the target device.
Gateway	Enter into this field the IP address of the gateway of the target device.
Preferred DNS Server	Enter into this field the IP address of the preferred DNS server of the target device.
Alternate DNS Server	Enter into this field the IP address of the alternate DNS server of the target device.

Target List: Target Device: Unattended Information

Parameter	Description
Screen Resolution	Defines the resolution in pixels of the target screen. The value in parenthesis behind the value indicates for which screen size the respective resolution is generally used.
Color Depth	Defines the color depth in bits per pixel of the target screen.
Refresh Rate (hz)	Defines the refresh rate in Hertz of the target screen (for example: *85* for CRT, *60* for LCD).
Resolution (DPI)	Defines the resolution in dpi that is to be used for the fonts displayed on the screen of the device to be installed.
Organization	Defines the name of your organization, for example, *BMC Software* .
Workgroup	The network workgroup of the target devices, for example, *WORKGROUP* . If you enter a value here and as well into the **Domain** field later on, this value is ignored.
Administrator Login	Enter into this field the login name to which is to be created for the newly installed OS with the full administrator rights accorded on the new device. For Vista and later versions this field is ignored, as the login name is predefined by Microsoft and can not be modified.
Administrator Password	Enter into this field the corresponding password. The default is *PasswordD123* and it fits most domain complexity policies.
User Login	Enter into this field the login name with which the user is to log on to his device which provides him with the required user rights. This parameter is only applicable to Vista and later.

Parameter	Description
User Password	Enter into this field the respective password to be used. This parameter is only applicable to Vista and later. The default is *PassworD123* and it fits most domain complexity policies.
Time Zone	The timezone in which the target device is located.
Domain	Enter into this field the name of the domain the new device should belong to, for example, *TESTLAB* . If you entered a name for the workgroup above the domain value prevails.
Domain Administrator Name	Enter into this field the login name of the domain administrator with which he may access the new device without the domain prefix. for example, *Administrator* and not *TESTLABAdministrator* or *.Administrator* .
Domain Administrator Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).
First Login Command	Defines the commands to be executed on the first login, this may be a path to a batch file to execute, for example, *E:Apps.bat* or *cmd /c REGEDIT /S E:Appspatch.reg* . This parameter is both applicable to Windows setup as well as sysprep.

Package parameters

Parameter	Description
Archive Name	The name of the archive which is distributed for the software distribution, its name is composed of the name of the package with a zip extension.
Archive Type	The type of file in which the package is stored. Possible values are the .zip format and the BCM Deploy proprietary .pkg format.
Package Type	The type of the package. *Custom* indicates that the package may either be a manually created custom package or a patch package.
Patch Package	Indicates if the package is a patch package, that is, either the MS Secure file package or any other patch package which was manually created.
Package Size (KB)	The size in bytes of the respective package.
Compressed Package Size (KB)	The size of the respective package in its compressed form in KB.
File Count	The number of files which are contained in the respective package.
Relay	The name of the relay on which the package is stored and to be collected from the target devices.
Dynamic Package	Defines if the package contents are to be dynamically updated. Be aware, that dynamic packages, that is, when this option is activated, the package cannot be copied to other packagers, as the package content is build during the publishing process.
Force Reassignment	Automatically forces the reassignment whenever the package is published.
Mapping Activated	Defines if the package is to be installed under another directory or some of the files shall be mapped to one or more different locations.
Checksum	The checksum of the respective package.
Referenced	

Parameter	Description
	Defines if a package is only to be referenced by the master, that is, the master receives all information concerning the package but not the package itself. In this case the package is stored in a specific location, which, for example, can also be a removable unit such as a CD/DVD or a USB key, and a relay, which requires the package for itself or its clients, verifies the given location before requesting it from the master.

Patch Management parameters

The following patch management parameters are provided.

Configuration

Parameter	Description
Enable Internet Check for Knowledge Base Update	Check this box to activate the verification for new versions of the Knowledge Base via the Internet. This value is only applicable to the Patch Manager, for all other devices this value should be deactivated.
Internet Check Schedule for Knowledge Base Update	Click the **Edit** icon to the right of the field to define or modify the schedule for the Knowledge Base update via Internet. Select the desired values from the options in the appearing window.
Automatic Knowledge Base Update after Check	Check this box to automatically update the configuration files with the newly found version of the files. If activated this option only downloads the file if the file is of a newer version than the version currently available on the Patch Manager, or if the **Force Parse** parameter is activated. It then directly updates the local file.
Knowledge Base Update Delay from Parent (sec)	Defines the interval in seconds between the automatic update of the Knowledge Base on all BCM devices apart from the master. If the value is set to 0, the automatic update functionality is deactivated. To update the local Knowledge Base at the defined interval the clients ask their direct parent if a newer version is available and if yes request its download.
Archive Type	Defines if the patch packages are to be of type zip or pkg.
Archiving of Downloaded Patches after Publication	Defines if the patches are stored in the **download** directory of the Patch Manager after the patch custom package was created and successfully published to the Master. If the option **Move** is selected, you need to fill in the following field **Path for Local Patch Repository** which defines the path to the local storage location.
Path for Local Patch Repository	Defines the local path which the patch module checks if the patch to be downloaded is already available locally there before actually downloading it from the Internet.
Download Retry Count	Specifies the number of retries for a patch download.
Download Retry Interval (sec)	Defines the interval in seconds between each retry for the patch download.
Maximum number of concurrent downloads	Defines the number of patches that can be downloaded simultaneously.

Parameter	Description
Force Parsing	Defines if the Knowledge Base is to be parsed again, even if it was already parsed before.
Update Type	Defines if the local device is to update its version of the Knowledge Base locally or via the Internet.

Proxy Options

Parameter	Description
Host Name	Enter the name of the device on which the proxy is installed.
Port	The TCP port number of the parent on which it communicates with its children.
User	Enter the user name to use for proxy authentication.
Password	Enter the corresponding password. For security reasons the keyword is only displayed in the form of asterisks (*).

Query parameters

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
Type	Select the target type of the query from all principal objects available in the BCM database.
Free Query	Defines if the query is a free SQL query.

Report parameters

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
Encoding	Defines the encoding to be used for report generation.
Font Size	Defines the font size for this report. This may be a number between 8 and 18.
Font Type	Defines the font type family for this report. This is also the font type used for the PDF generation.
Logo	Select the logo to use for this report from the dropdown list.
Report File Name	Defines the file name of the published report. If this field is empty, the file name of the report is generated with the date and time of its generation.
Report Style	Select the general layout of the report. This defines into how many subreports the report is divided into.
Report Template	Select from the drop-down box the report template to use. This field is only applicable to template-based reports.
Report Title	Enter the title of the new report.
Report Type	Select the type of the report, that is, if it is style or template based.
Style Sheet	Defines the style sheet to use when displaying the report.

Resource Management parameters

The following resource management parameters are provided.

Monitored Object

Parameter	Description
Object Type	Defines the type of the monitored object.

Performance Counter

Parameter	Description
Object Name	The name of the monitored object that is measured.
Counter Name	Displays the name of the performance counter of the object to be monitored.
Instance	The name of the instance of the counter to be monitored.
Operation	The type of operation which is monitored on the counter.
Count	Displays the number of times -1 the threshold is allowed to exceed, for example, if the count is 5, the threshold can exceed the value 4 times, and at the fifth time, the defined operation is executed.
Threshold	The threshold fixed for this counter.
Operator	The operator of the monitored performance counter, for example, if the threshold of the monitored value is to be larger or smaller than the above fixed value.
Period (h)	Defines the number of seconds within which the threshold may not be exceeded the number of times defined in the **Count** field.
Frequency (s)	Defines at which interval per second the value of the object is measured, for example, if this field defines 5 this indicates that the value is measured every five seconds.
Generate Event	Specifies if an event model is created for the Event Log Manager.

Monitored Object

Parameter	Description
Object Name	The name of the monitored event.
Log Source	The source of the event to be logged, that is, which of the Windows events is to be monitored.
Type	Defines the type of event to be monitored, the values depend on the source chosen above.
Event ID	Defines if only events of a specific ID are to be monitored.
Generate Event	Specifies if an event model is created for the Event Log Manager.

Rollout parameters

Parameter	Description
Auto-extractable Name	Enter the name of the autoextractible rollout file, if the rollout is to be also available for download on the Rollout Server agent interface, for example, *FPAC_XP32BitUninstall.exe* .
Silent mode Installation	Check this box if the agent installation is to be executed without any user information windows on the target device. This parameter is only applicable for Windows targets.
Rollout Type	Select from this list the type of the rollout that is to be executed, that is, a new agent installation (**Install**), a reinstallation or repair (**Reinstall**) or removing the agent (**Uninstall**) from one or more devices.
Operating System	Define the operating system type for the rollout targets, they are grouped by type.
Installation Directory	Enter the directory path into which the agent is installed on the target devices, for example, */usr/local/bmc-software /client-management/client* . It is possible to configure an installation path starting with an environment variable, for example, *$[ProgramFiles]BMC SoftwareClient ManagementClient* .
Agent Service Name	The name of the BCM agent service.
Start service after rollout	Uncheck this box if the agent service is not to be started directly after the successful rollout.
Service Startup Type	Defines the startup type of the agent service, possible values are **Automatic** to automatically start the agent at every device restart and **Manual otherwise** . This option is only applicable to Windows operating systems.

Software License Management parameters

The following software license management parameters are provided:

- Configuration
- Licensed Software
- Licenses

Configuration

Parameter	Description
Number of days before sending a license expiring alert	Defines the number days that may remain until the license expires to send an alert.
License underinstallation percentage threshold to send an alert	Defines the percentage of uninstalled software licenses under which an alert is sent. This means that if the threshold is set at 50% and 51% of the licenses are installed no alert is sent. If only 50% or less of the available licenses are installed an alert is generated.

Parameter	Description
Exceeded license usage percentage threshold to send an alert	Defines from which percentage value onwards of used licenses an alert is sent, that is, if the threshold is defined at 80% and 80% or more of the available licenses are used, an alert is sent. If only 79% of the licenses are used no alert is generated.

Licensed Software

Parameter	Description
Category	A free text field that provides information about the content of the licensed software, that is, it is for example a development tool, an accounting software or an office software suite.
Evaluation Type	Specifies the way the licensed software is evaluated, that is, as an application or via a query. • **Scanned Application** : The licensed software is populated with individual, scanned applications, that are under the same license scheme. • **Query** : The licensed software is populated via the result of a query, that is, all devices that answer the software criteria specified in the query. • **Software Catalog** : The licensed software is populated with applications of the Software Catalog, that are under the same license scheme. This option may not be available depending on your product licenses.
Status	Displays the current evaluation status of the licensed application. This value is not editable and is automatically updated.

Licenses

Parameter	Description
Vendor	Enter the name of the vendor from which the software and license(s) were purchased. This may be the manufacturer as well as an independent third-party vendor.
Product Serial Number	Enter the serial number of the product.
Quantity	Enter the number of purchased licenses.
Purchase Date	Define the date at which the licenses were purchased by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
Purchase Order Number	Enter the order number of the license purchase under which it may be found in your books.
Expiration Date	Define the date at which the licenses expires, if applicable, by clicking the arrow to the right of the field and selecting the date from the appearing calendar.
License Type	Select the type for the license, for example, if it is a license that covers an entire **site** , if it is limited to a number of users (**Per Seat**), if it is counted by **processor** or by **client access** , is it a **Volume** license. If none of these apply select **Other** .

Transfer Window parameters

Parameter	Description
Channel	Select the channel of the newly created transfer window: • **Notification** : the master server or relay informs its children that data (for example, packages, operational rules) are waiting for them on the parent. • **Data** : inter-agent data transfer from one level to another: upstream/downstream or downstream /upstream. Data can be operational rules, packages, inventories, etc. • **Multicast send** for multicast distributions.
Shareable	Defines if the transfer window is inherited by the child devices of the device this window is assigned to. If Multicast send is selected as channel, this option is automatically deactivated.
Slot Type	The unit in which the bandwidth is calculated.
UTC Time	Defines if the UTC time system is to be used. This is useful if the managed systems are spread over many different time zones.

User parameters

Parameter	Description
Name	The name of the object under which it is known in BCM. This name may be any combination of characters.
User Domain	Enter the name of the domain for which the user is defined.
User Login	Enter the login name of the user with which he may log on to any client within the network.
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Office Phone	The office telephone number of the administrator.
Location	The location of the user.
Employee ID	The unique identifier of the employee.
User Enabled	Define if the user and his login are currently enabled, that is, if when using this login to a client he may access the specified user options.

Error Codes

This topic provides the list of all error codes for the individual modules and objects of the BMC Client Management , such as operational rules, rollouts and performance counters. The table displays to which modules/object types and or situations it applies, the error code number, its translation and possibly an explanation where required:

Common Error Codes

The following error codes are common to all modules:

Error Code	Description
0	Done.
1	Operation failed.
2	The calling action is not registered on the agent. Please check if the module is loaded.
3	An action with this name is already registered.
10	The requested object could not be found.
11	An object is already registered under this name.
12	Access denied. Please verify your access rights.
13	Incorrect parameter. Please verify the supplied parameters.
14	Incorrect parameter value. Please verify the values of the supplied parameters.

Error Code	Description
22	Could not connect to the remote client.
24	HTTP communication problem.
28	The operation was postponed.
30	The keyword does not exist.
990	Connection failed: the host is either unreachable on the given port or there is a wrong SSL configuration
991	Server access denied: wrong login/password supplied.
992	The folder for the specified certificate does not exist!
993	Connection failed: the host is reachable on the given port but the service is not ready yet. Please try again later.
994	Connection reset: the host closed the connection abruptly. Please check your SSL configuration.
995	Connection failed: The device is unreachable. It may be powered off or inaccessible. Make sure that the device and the agent are started and running.

Agent Core

Error Code	Description
14001	The file could not be found.

Custom Packages

Error Code	Description
41001	General error.
41004	Impossible Operation: The package is under construction.
41010	A mapping already exits for this entry.
41011	A file is already mapped to this destination.

Database

Error Code	Description
16001	There is no database connection present.
16002	SQL execution error
16003	No handler found for the required operation.
16010	Login failed.
16020	Invalid group type name.
16021	Group not found.
16022	Invalid group / child relation.

Error Code	Description
16023	Invalid group / child relation which would cause a circular relationship.
16024	Cannot create a parent/child relation because the child is not allowed to have any or more than 1 parent.
16025	The target data type for the query is not compatible with a device group.
16028	One or more objects could not be assigned.
16029	The device group is assigned to at least one inactive query.
16030	A directory server is already assigned to this group.
16031	A query is already assigned to this group.
16032	This group is not empty, it already contains members.
16033	The group is inactive.
16035	The group is already assigned to query with criteria, it may not be assigned a free query.
16036	This query can not be set to free query. It is assigned to a dynamic group which is assigned to more than one criteria queries.
16040	Bad object type.
16041	Bad object name.
16042	The object can not be deleted as it is currently in use.
16043	The supplied attribute name does not exist.
16044	The requested object is busy.
16045	The device has no GUID.
16046	The device is linked to objects.
16047	This object is used by a query and cannot be deleted.
16048	Mandatory attribute that cannot be deleted.
16049	The user is linked to objects.
16050	Invalid operational step type name.
16051	The operational rule could not found.
16052	The operational rule is already activated.
16053	The operational rule does not have any steps.
16054	The operational rule is assigned indirectly through a device group.
16055	The operational rule can not be modified while it is waiting to be sent.
16056	The rule assignment has been deleted.
16057	The rule has been automatically unassigned.
16058	The group is already assigned to the operational rule.
16059	The operational rule is scheduled.
16060	No query is defined for this subreport.

Error Code	Description
16061	No columns are defined for this subreport.
16062	Incompatible Format.nnYou must set the format to table, add a second column to your subreport or modify your columns.nTo use one of the chart formats your subreport must have at least one data column returning a numeric type.
16063	No file could be found for one of the subreports.
16064	The report is larger than 500MB, you can only view it via an export.
16065	No query is assigned to the subreport and the report is not assigned to any device or device group.
16066	The report is assigned to at least one device group.
16067	No report result is available.
16068	The report cannot be deleted as it is currently being generated.
16069	This object is used by a report and cannot be deleted.
16070	License is not valid.
16071	The number of objects permitted by the BMC Client Management license was exceeded.
16072	It is not possible to add {1} scanner(s). You only have a license for {2} scanner(s).
16073	The number of devices to assign is higher than the remaining BMC Client Management licenses.
16074	The BMC Client Management license has expired.
16075	Unable to load the license file. The BMC Client Management master server requires a license for version {1}. Please use your support profile to download an updated license file.
16080	The Administrator does not have the necessary access rights on all parents.
16081	The administrator does not have the necessary access rights on all scans assigned to the scanner.
16082	The administrator does not have the necessary access rights on all scan directories assigned to the scanner.
16090	The query is currently in use, thus its type may not be modified.
16091	This query is assigned to device groups or security profiles. Any modification of the criteria may cause a reevaluation of the group members, thus causing assignments or unassignments of operational rules and/or a reevaluation of the administrators' rights. Are you sure you want to continue?
16092	The sql syntax is not correct.
16093	The query must contain the object type specific table.
16094	The SELECT of the query may not contain operators like AVG, COUNT, MAX, MIN and SUM or sql commands like UNION, INTERSECT, EXCEPT, MINUS
16095	The relation between the group and the directory server cannot be removed, since the group's parent also has a relation to the entry DN.
16096	The group is already assigned to a free query, it may not be assigned an additional query.
16097	The query must start with SELECT.
16098	The query must contain the condition of the group type. For example, GroupTypeID=101 if the query is concerned with device groups.
16099	There are too many synchronization results to display them.

Error Code	Description
16100	The group or device is already assigned to the monitored object.
16110	An import is already running. Try again later.
16115	The object is already a member of the group.
16116	The object could not be found.
16117	This object type is not available for search actions.
16120	The device is already assigned a transfer window with the same Channel/Shareable settings.
16133	The applications list does not contain any applications.
16134	A Software Catalog update is in progress ({PercentComplete}% complete).nPlease wait before accessing the library.
16136	The licensed software does not contain any applications.
16150	The patch is already assigned to this group.
16151	The patch group is currently being assigned.
16160	Impossible to modify. Assignment is processing.
16161	The operational rule contains steps which are no longer available with the current license.
16162	The operational rule is dependent on other rules that are not assigned to the device.
16163	The device assignment could not be removed because it was effected via a device group. You must remove the device group assignment.
16164	The user assignment could not be removed because it was effected via a user group. You must remove the user group assignment.
16165	The operational rule was assigned to the device via a user. To unassign it you need to unassign the user from the operational rule.
16166	The operational rule associated with the package could not be deleted because it contains more than one step, that is it has at least one step in addition to the package installation step.
16167	This step is referenced by a "Go to step" parameter. Are you sure you want to remove the step?
16168	This operational rule has at least one step for which the parameter "Go to Step" is not defined.
16170	Error
16180	Unavailable functionality, a database update is in progress.
16182	Scanned Device
16183	Unavailable functionality, a database update is required.
16190	The object in the buffer is not compatible with the specified destination.
16191	The Clipboard is empty.
16200	A compliance rule is already assigned to this device group.
16201	The relation must be empty as the compliance rule does not have any criteria groups.
16202	The criteria group relation is empty.
16203	Some constants could not be deleted as they are used by compliance rules.

Error Code	Description
16204	The compliance rule is inactive and therefore may not be evaluated.
16205	This object is assigned to a dashboard on which you do not have write access.
16206	This alert name already exists.
16207	You have selected a compliance rule/device group combination that is already assigned to an alert.
16208	This object is used by a compliance rule and cannot be deleted.
16210	The administrator account is disabled.
16211	The administrator could not be found.
16220	The access token is invalid.
16221	External Integration is not enabled for the specified user name. Ensure that the user name you specified matches the login specified in BMC Client Management under Global Settings > External Integration.
16222	The operational rule is not available for external integration.
16224	The external interface version is older than the BMC Client Management interface version.
16225	The external interface version is newer than the BMC Client Management interface version.
16226	Operation impossible. This operational rule is in "additional workflow needed" in external integrations.
16227	Remote credentials are required
16240	Device not found
16241	Only one primary user can be assigned to a device.
16242	Agent version is prior to 11.5
16243	A conflict occurred during the device merge.
16246	The device cannot be deleted because it has children.
16304	The rollout server is currently in use.
16305	No user account is assigned to this rollout.
16306	No target is assigned to this rollout.
16307	This device was already added.
16308	You must enter a device name, not a list of devices.
16309	The rollout cannot be deleted as it is currently assigned to at least one rollout server.
16400	The indexation was never launched or is not finished.
16401	A memory error occurred.
16402	No results were found.
16500	The device is already attached to a parent
16501	The device is parent for other devices so it cannot be a child itself
16502	The device is attached to a parent so it cannot have children.
16503	The device cannot be a child of itself.

Error Code	Description
16504	One or more statuses have not been changed.
16505	This status cannot be removed, devices are using it.
16506	This status cannot be removed, it does not exist.
16507	This status cannot be removed, it is predefined and mandatory.
16550	If you disable the user, it will no longer be possible to assign him operational rules. Are you sure you want to continue?
16551 Device	Some operational rule assignments exist to this device via the selected users. By removing this user-device relation the rules will also be unassigned. Are you sure you want to continue?
16551 User	Some operational rule assignments exist to these devices via the selected user. By removing this user-device relation the rules will also be unassigned. Are you sure you want to continue?
16601	The SCAP package was already imported and you do not have the necessary access right on it. Select another package.
16602	The package validation failed.
16603	This SCAP rule is already added as an exception.
16700	The value must be greater than 100 or 0, if the attribute is not to be displayed.
16701	The data type is incorrect.
16800	The file does not contain any BCM object.
16830	This OSD agent already has a parent.
16831	You cannot modify the role of this repository, it has OSD agents as children.
16832	Impossible to remove this device, it is an image repository and it has OSD agents as children.
16833	You cannot remove this device, it is an OSD Manager and it has children.
16834	The OSD functionnality has undergone major changes. To be able to use the OSD Role you have to upgrade the BCM agent to the latest version.
16835	The OSD functionnality has undergone major changes. To be able to use the OSD Manager you have to upgrade the BCM agent to the latest version.
16836	Impossible to load the OS deployment module
16837	Impossible to unload the OS deployment module
16900	The device is not reachable.

Windows Device Management

Error Code	Description
65050	Command failed

File Store

Error Code	Description
44001	Operation is postponed, an operation is already in progress
44002	File has already been processed by this module, other modules may process it further.
44003	File has already been processed by this module and will be deleted, therefore no other module can process it.
44004	File cannot be managed by this module.
44005	File has a bad address.

HTTP Protocol Handler

Error Code	Description
27001	The device is not reachable.
27002	The server certificate is invalid.
27003	The server certificate key is invalid.
27004	The key does not match the server certificate.
27005	The intermediate authority certificate is invalid.
27006	The root authority certificate is invalid.
27007	Unable to rebuild the certificates chain.

LDAP

Error Code	Description
36001	Invalid LDAP Host Name.
36002	Invalid LDAP Port.
36003	Invalid LDAP Base DN.
36004	Invalid LDAP User DN.
36005	Invalid LDAP Password.
36010	Unable to connect to the LDAP server.
36011	Invalid authentication on the LDAP server.
36012	Bad parameter, the LDAP search could not be executed.
36013	Unable to count the entries in the LDAP search result.
36014	Unable to get DN.
36015	Unable to get the value from the specified DN.
36016	Unable to get DN, it does not exist.
36017	Unable to get DN, too many found.

Error Code	Description
36019	The synchronization failed. The entry could not be found. Make sure that it was not renamed, moved or deleted.
36050	LDAP pointer is null, there is no connection.

MSI Packages

Error Code	Description
35001	General error.
35002	The Chilli script contains errors and could not be compiled. (Pre and post install scripts)
35003	Error: The package was not renamed, even though the Force Rename parameter is activated.
35004	Impossible Operation: The package is under construction.

NT Event

Error Code	Description
62001	General error.

Operational Rules

Error Code	Description
32001	Failed to get the required function address.
32002	Dependency check during rule execution failed.
32003	The master could not be contacted.
32004	The operational rule module does not have the required master information.

Operational Rule Steps

Error Code	Description
43001	Succeed
43002	Failed
43100	Insufficient RAM installed.
43110	Insufficient free disk space left.
43120	No software name supplied.
43121	Software not found.
43130	Operating system name check failed using full match comparison.
43131	Provided string is not part of the operating system name.
43140	Service not found.
43150	No valid archive file found.

Error Code	Description
43151	Could not find install script in the archive file.
43152	Failed to extract the install script from the archive.
43153	Too many environment variables currently in use.
43170	At least one file failed to install.
43171	Run command failed.
43172	A file required to be present is absent.
43173	A file required to be absent is present.
43174	Failed to extract files.
43190	Succeeded.
43191	Insufficient disk space.
43192	At least one file does not satisfy the installation rules.
43193	The contents of the package are not suitable for this system.
43194	Failed to create a directory.
43195	Failed to delete a directory.
43196	The archive file is not valid.
43198	Failed to create registry key.
43199	Failed to delete registry key.
43200	Failed to create registry value.
43201	Failed to delete registry value.
43203	Failed to delete file.
43220	Operation cancelled by user.
43221	Operation cancelled due to timeout.
43222	Operation cancelled: no user logged on to the device.
43223	Operation cancelled as the device was in screen saver mode.
43240	Failed to end process.
43241	Process not found.

OS Deployment

Error Code	Description
63001	The OS deployment module is not properly configured. Modify your parameters and run the configuration check.
63002	The OS deployment module initialization process is currently running. This may take several minutes. Try again later.
63003	No running build to cancel.

Error Code	Description
63004	A build is already running for this project.
63005	Invalid object ID.
63008	A USB support creation is in progress, retry later.
63010	The database insertion of the object failed.
63011	The database update of the object failed.
63012	The database selection of the object failed.
63013	The database deletion of the object failed.
63014	Another target with the same MAC address already exists in this target list.
63015	The Windows edition to be deployed was not specified in the Parameters tab of the target.
63016	The target device list is empty. At least one device is required to proceed.
63020	FAT32 partition bigger than 32 GB.
63021	Total partition size bigger than disk.
63022	Physical partition index found twice.
63023	"Extend" partition field found active twice.
63024	Partition label found twice.
63025	Partition letter found twice.
63026	Partition order number found twice.
63027	"Active" flag found set twice.
63030	The Windows AIK toolkit or one of its required element could not be found.
63031	The Trivial FTP server check failed.
63032	Access to the root driver cache path failed.
63033	The DHCP server check failed.
63034	The status update failed.
63035	The TFTP local path and the TFTP UNC path do not match.
63036	Could not find a share for the local TFTP path. The share may be missing or the path is invalid.
63037	The internal TFTP server failed to start. Check that no other application use the UDP port 69.
63038	The internal DHCP gateway failed to start. Check that no other application use the UDP port 67.
63039	The Windows ADK toolkit or one of its required elements could not be found.
63040	Incorrect .inf file.
63041	File .inf not found.
63042	Driver root directory not found in the database.
63043	Driver root directory creation failed.

Error Code	Description
63044	Previous file deletion failed.
63045	Storage folder creation failed.
63046	Source folder opening failed.
63047	Too many files around the .inf file.
63048	Driver copy failed. Insufficient credentials or disk space.
63049	The INF file path contains the driver cache path.
63050	The write access test failed for the specified UNC path. Please check the access rights.
63051	The connection to the specified UNC path failed. Please check the path and access rights.
63052	The impersonation required to check UNC path and credentials failed.
63053	The specified UNC does not follow the standard UNC path format (for example: servershare).
63054	The share name is missing from the specified UNC path (for example: servershare).
63055	The UNC path could not be found. Please check the path.
63057	The specified UNC path failed the check for unknown reasons.
63058	The WIM image file could not be found at the specified location.
63059	The static IP address was not entered for at least one target device!
63060	The static IP addresses of the targets are identical!
63061	Impossible to apply driver!
63062	Impossible to remove the driver!
63063	Impossible to clear drivers!
63065	The image path is not valid for a Vista setup, but is valid for an XP Setup.
63066	The image path is not valid for an XP setup, but is valid for a Vista Setup.
63067	The image path does not end with a .wim extension.
63068	The image path must point to the folder containing an I386 or AMD64 subfolder. Please select the parent folder to solve this problem.
63069	The driver already exists in the database.
63070	The project build failed because it conflicts with the active project \{ProjectId\} on the MAC address or PXE Mask \{MacAddress\}. nPlease disable the project or target responsible for this conflict to continue.
63071	Another PXE menu is already active with this scope. Deactivate it, then try again.
63072	Proxy not found.
63073	Unknown network interface.
63074	Session not found.
63075	BIOS type mismatch, UEFI only and Legacy only are not compatible.
63078	

Error Code	Description
	The project is configured as Legacy but no Legacy compatible disk configuration is assigned to the target list. Please assign a Legacy compatible disk configuration (MBR) to the target list.
63079	The project is configured as UEFI but no UEFI compatible disk configuration is assigned to the target list. Please assign an UEFI compatible disk configuration (GPT) to the target list.
85001	Failed to erase existing export
85002	Disk read error of file not found
85003	Disk write error
85004	Source data read error
85005	Metadata file not found
85006	Metadata file has bad format
85007	Update from reference failed
85008	Bad checksum

Patch Management

Error Code	Description
53001	The missing patch/service pack scan failed.
53003	Wrong MS XML version.
53004	The patch manager database update is in progress.
53005	The Patch Manager could not retrieve the information from the server. Please check your settings.

Performance Counter

Error Code	Description
48001	General error.

Power Management

Error Code	Description
58001	Initiation failed.
58002	Unsupported OS.
58003	Not enough memory.
58004	No user logged.

Privacy

Error Code	Description
8001	A session identifier is required.
8002	Invalid session ID.
8003	The session has expired.

Relay

Error Code	Description
33001	Device unreachable

Rollout

Error Code	Description
32	Failed to normalize the directory
33	Failed to create the temporary directory
34	Failed to change the directory
35	Failed to get the directory
36	Unknown archive header
37	Unexpected end of archive
38	Failed to read the archive
39	Failed to decompress the archive
40	Unexpected archive header
41	Failed to open the file
42	Memory allocation failed
43	Failed to initialize the ZLib
44	Failed to detect the marker
45	The directory could not be created
46	The file could not be created
47	Impossible to write to the file
48	The process could not be created
49	Command was canceled
61	Failed to detect a remote share to connect to
62	Memory allocation error
63	Unsupported system

Error Code	Description
64	Missing parameter
65	Missing system variable
66	Agent version could not be detected
67	Agent build number could not be detected
68	Agent installation directory could not be detected
69	Agent service could not be detected
70	Windows directory could not be detected
71	Agent cannot be upgraded
72	A Master agent has been detected
73	More than one agent detected
74	More than one operation requested
75	No operation requested
76	Agent is already installed
77	Failed to compare versions
78	Directory could not be deleted
79	Directory could not be created
80	The file does not exist
81	Failed to open the file
82	Failed to read the file
83	Failed to decrypt the file
84	Insufficient access rights
85	Extraction impossible
86	Failed to create the event (progress bar)
87	Failed to create the thread (progress bar)
88	Failed to treat the key
89	Impossible to create the process
90	Impossible to treat the version
91	Failed to delete the driver
92	Failed to create the auto-extractible file
93	Failed to initialize OpenSSL
94	Process timeout
95	Process error
96	An agent is already installed with a different version

Error Code	Description
97	An error occurred while opening the service
98	An error occurred while stopping the service
99	An error occurred while starting the service
100	An error occurred while deleting the service
101	An error occurred while creating the service
102	Failed to start msiexec
103	It is not authorized to install an older version
104	Invalid archive
105	Registry key could not be found
106	Registry key could not be deleted
107	Registry key value could not be deleted
108	Registry key could not be enumerated
109	Registry key could not be created
110	Registry key value could not be created
111	No agent found
112	Failed to rename the file
113	Failed to compile the Chilli script
114	Failed to execute the Chilli script
115	No system directory was found
116	Failed to delete the file
117	The directory does not exist
118	Failed to create the file
119	RPM Package not found
120	Binary RPM not found
121	RPM error
122	Service not registered
123	An error occurred during the service registration
124	The installers do not match
125	The operating system is not supported.
127	Failed to execute self-extractible file.
30001	The device cannot be reached
30002	Failed to connect to the remote service controller
30003	Maintenance operation found

Error Code	Description
30004	Failed to create the remote service
30005	Failed to start the remote service
30006	File copy error
30007	Rolling out a Windows agent requires a Windows Rollout server.
30008	Failed to modify the file rights
30009	Execution error
30010	Access denied
30011	Invalid network address

RPM Packager

Error Code	Description
52001	General error.
52002	Error: The package was not renamed, even though the Force Rename parameter is activated.
52003	The package is empty.
52004	Impossible Operation: The package is under construction.
52005	Error: The package was not renamed, even though the Force Rename parameter is activated.
52009	A reboot is needed.

Security Products Management

Error Code	Description
81001	Browser not found
81002	Browser is not the default one
81003	No antivirus product found
81004	Firewall not enabled
81005	File date signature is older than the chosen number of days
81006	Installed Product with chosen regex has not been found
81007	Real-time protection is inactive.
81008	No product was found.
81009	No option is selected.
81010	No files are selected.
81501	General Opswat Framework error.
81502	This action is currently not available for this product.

Error Code	Description
81503	Invalid arguments
81504	Object/Component is in invalid state
81505	Object/component cannot be created, since it already exists
81506	The object or component could not be found.
81507	OESIS dll signatures failed checksum verification
81510	Failure in core API call
81511	Maximum amount of objects has been reached
81512	Object/component has already been initialized
81513	Invalid local path
81514	Cannot initialize OESIS database
81515	OESISCore was not initialized
81516	OESIS database access failure
81517	License is not valid for current method call
81530	Method cannot be performed due to the state of the integrated software product. Product or some of its components may not be installed
81531	DB integrity failure
81533	Access violation
81534	IO error
81535	Input parameters sent to method invocation do not match the expected signature
81536	Output parameters returned from method invocation do not match the expected signature
81537	Insufficient privileges
81538	The operation has timed out
81540	A critical error has occurred
81541	The network location was not accessible
81542	The product requires a reboot before it can continue
81550	The product requires a reboot before it can continue
81551	User attempts to use callback functionality without initializing the callback
81552	Failed to create a new callback thread
81553	Error in connecting to 32-Bit Proxy
81554	Error in communicating with 32-Bit Proxy

Snapshot Packager

Error Code	Description
34001	The Chilli script contains errors and could not be compiled. (Pre and post install scripts)
34009	A reboot is needed.

Virtual Infrastructure Management

Error Code	Description
50001	The virtual machine was not found.
50002	Failed to change state.
50003	Wrong MS XML version.

Web API

Error Code	Description
82001	A session identifier is required.
82002	Invalid session ID.
82003	The session has expired.

Windows Services

Error Code	Description
38001	Unknown system error
38002	The specified database does not exist
38003	The service handle is invalid
38004	Invalid parameter
38005	Invalid service name
38006	The service does not exist
38007	The service binary file could not be found
38008	An instance of the service is already running
38009	The database is locked
38010	The service depends on a service that does not exist or has been marked for deletion
38011	The service depends on another service that has failed to start
38012	The service has been disabled
38013	The service did not start due to a login failure
38014	The service has been marked for deletion

Error Code	Description
38015	A thread could not be created for the service
38016	Request timeout
38017	The service cannot be stopped because other running services are dependent on it
38018	The requested control code is not valid, or it is unacceptable to the service
38019	The requested control code cannot be sent to the service
38020	The service has not been started
38021	The system is shutting down
38022	A circular service dependency was specified
38023	The name already exists in the services database
38024	The account name is invalid

Best practices for mobile device manager

The mobile device manager is a computer (virtual or physical) that is used for managing enrollment, notifications, and other communication with the managed mobile devices. For seamless communication between the managed mobile devices and BMC Client Management, the IT administrators should consider the following recommended best practices when defining and configuring mobile device manager:

- Prerequisites
- Hardware recommendations
- Setting up two or more mobile device managers without load balancing
- Setting up two or more mobile device managers with load balancer

Prerequisites

The following are the prerequisites for the mobile device manager:

- Must be connected to internet uninterruptedly.
- Must be able to handle both the outbound and inbound requests.

Hardware recommendations

BMC recommends using only one mobile device manager. However, the number of mobile device managers you may need depend on the following factors:

- Number of mobile devices to be managed
- Specifications of the mobile device manager

The following test results should help the IT administrators to make an informed decision about the hardware configuration and number of mobile device managers required:

Test description

The test included sending six different mobile commands to the managed mobile devices. The mobile devices sent the inventory information back to the mobile device manager using web services.

Test hardware specifications

CPU	Intel® Xeon® CPU E3-1240 V2 @ 3.40GHz - 8 Cores
Platform	DELL PowerEdge T110 II
Memory	24 GB
Hard Drive	3 x 500 GB 7200tr/s SATA
Operating System	• Linux Debian 7 64 bit • Windows Server 2012
Network	1 GB/s

Test criteria and results

Processing time for 30,000 mobile devices with one mobile device manager on Windows server:

	Web Service Count	Throughput (WS/Sec)	Processing Time (Sec)	Transfer Time to Master
6 Web services	180,000	296	609	15h 00m

Processing time for 30,000 mobile devices with one mobile device manager on Linux server:

	Web Service Count	Throughput (WS/Sec)	Processing Time (Sec)	Transfer Time to Master
6 Web services	180,000	648	278	2h 40m

Processing time for 30,000 mobile devices with three mobile device managers on Windows Server via load balancer:

	Web Service Count	Throughput (WS/Sec)	Processing Time (Sec)	Transfer Time to Master
6 Web services	180,000	416	432	9h 00m

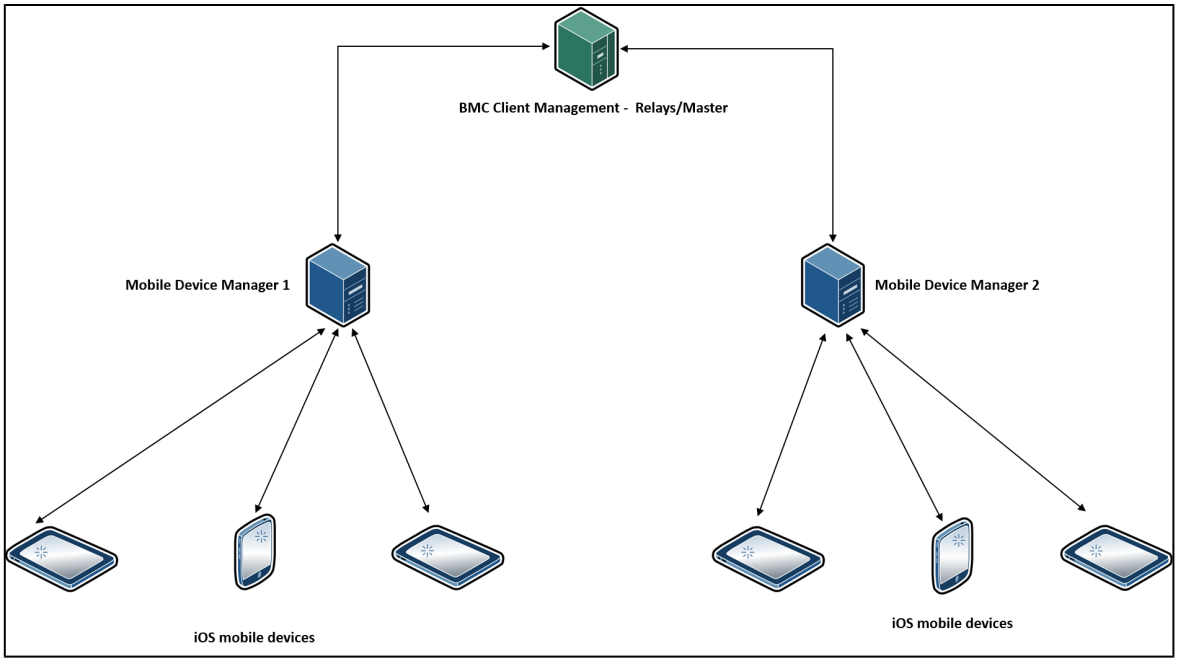
Processing time for 30,000 mobile devices with three mobile device managers on Linux server via load balancer:

	Web Service Count	Throughput (WS/Sec)	Processing Time (Sec)	Transfer Time to Master
6 Web services	180,000	723	249	1h 00m

Setting up two or more mobile device managers without load balancing

The following guidelines should be considered if you are defining and configuring more than one mobile device manager without using a load balancer. The figure 1 indicates the general architecture of two or more independent mobile device manager without load balancer:

Fig 1: Multiple mobile device managers without load balancer

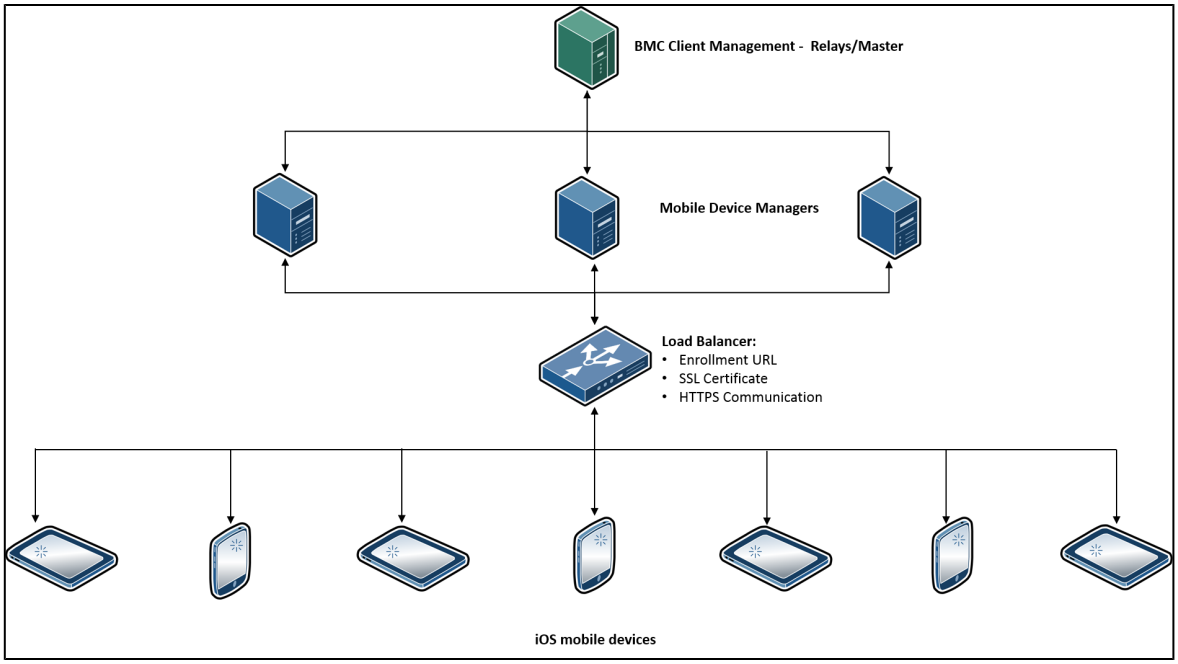


- The mobile device manager 1 is independent from the mobile device manager 2.
- The mobile device manager 1 and the mobile device manager 2 have their own enrollment URLs. The mobile devices enrolled on the mobile device manager 1 communicates with the mobile device manager 1 only.
- The mobile devices enrolled on the mobile device manager 1 cannot communicate with the mobile device managers 2 even if the mobile device manager 1 is down (not available).
- If a mobile device enrolled with mobile device manager 1 needs to be managed by mobile device manager 2, the mobile device first needs to cancel enrollment with the mobile device manager 1 and then enroll again using the enrollment URL of the mobile device manager 2.

Setting up two or more mobile device managers with load balancer

The following guidelines should be considered if you are defining and configuring more than one mobile device manager with a load balancer. The figure 2 indicates the general architecture of two or more mobile device manager with a load balancer:

Fig 2: Multiple mobile device managers with a load balancer



- The load balancer shares load with all the mobile device managers.
- There is only one enrollment URL, using which all mobile devices are enrolled.
- A mobile device connects with the load balancer and the load balancer connects the mobile device to an available mobile device manager.
- If one mobile manager is down (not available), the load balancer automatically transfer the mobile device connection to other available mobile device manager.
- IT administrator can add or remove mobile device managers as required.

PDFs and videos

This topic describes and links to PDFs and other documents that support this product release. If the ready-made PDFs of this space do not satisfy your requirements, you can export a custom PDF.

- Ready-made PDFs in English
- Translated content
- Videos

Note:

When you export a custom PDF, you can select the topics to include. For information about how you can export a custom PDF from this space, see Exporting to PDF and other formats.

Ready-made PDFs in English

Title	Date	File size
BMC Client Management version 12.5	August 11, 2016	14.9 MB
BMC Client Management - WebAPI Operations for Integrating with BMC Client Management **Note** There is no change in the BMC Client Management - web API operations manual from previous version.	June 10, 2016	3.1 MB

Translated content

Most of the product guide PDFs are also available as a translated version to our supported languages. Select your language to access the translated versions.

Note

The user documentation is not translated for BMC Client Management version 12.5. You can refer the following translated manuals from the BMC Client Management version 12.1 release. For the latest updates in BMC Client Management 12.5 release, see the 12.6 enhancements page to get started.

- PDFs in deutscher Sprache
- PDFs em brasileiro
- PDFs en français
- PDFs en español
- 日本語版PDF

Videos

The following topics contain videos that supplement or replace the text-based documentation:

- Configuring mobile device management
- Performing remote operations on managed mobile devices
- Managing configuration profiles for managed mobile devices
- Managing mobile applications
- Enrolling mobile devices

- Integrating Footprints Service Core 12 with BCM en français
- Prerequisites to rollout BCM agents on MACs

Restricted PDFs

This topic describes and links to PDFs and other documents that support this product release. If the ready-made PDFs of this space do not satisfy your requirements, you can export a custom PDF.

- Ready-made PDFs in English
- Translated content
- Videos

> **Note:**
>
> When you export a custom PDF, you can select the topics to include. For information about how you can export a custom PDF from this space, see Exporting to PDF and other formats.

Ready-made PDFs in English

Title	Date	File size
BMC Client Management version 12.5	August 11, 2016	14.9 MB
BMC Client Management - WebAPI Operations for Integrating with BMC Client Management **Note** There is no change in the BMC Client Management - web API operations manual from previous version.	June 10, 2016	3.1 MB

Translated content

Most of the product guide PDFs are also available as a translated version to our supported languages. Select your language to access the translated versions.

> **Note**

> The user documentation is not translated for BMC Client Management version 12.5. You can refer the following translated manuals from the BMC Client Management version 12.1 release. For the latest updates in BMC Client Management 12.5 release, see the 12.6 enhancements page to get started.

- PDFs in deutscher Sprache
- PDFs em brasileiro
- PDFs en français
- PDFs en español
- 日本語版PDF

Videos

The following topics contain videos that supplement or replace the text-based documentation:

- Configuring mobile device management
- Performing remote operations on managed mobile devices
- Managing configuration profiles for managed mobile devices
- Managing mobile applications
- Enrolling mobile devices

- Integrating Footprints Service Core 12 with BCM en français
- Prerequisites to rollout BCM agents on MACs

PDFs in deutscher Sprache

Auf dieser Seite finden Sie die Liste aller PDFs der BMC Client Management Produktdokumentation:

Titel	Beschreibung	Datum	Dateigröße
BMC Client Management - Technische Spezifikationen	Dieses Dokument liefert Ihnen erste technische Daten, die Sie kennen müssen, bevor Sie mit der Installation von Client Management beginnen können. Es verweist Sie auf weiterführende Dokumente, in welchen Sie detailiertere Angaben zu dem im Dokument angesprochenen Themen finden können.	22. Okt. 2015	0,2 MB
BMC Client Management - Windows-Installation	Dieses Handbuch leitet Sie durch die erste Installation aller Client Management-Komponenten auf einem Windows-System für einen lokale Installation.	23. Okt. 2015	2,0 MB
BMC Client Management - Linux-Installation	Dieses Handbuch leitet Sie durch die erste Installation aller Client Management-Komponenten auf einem Linux-System für einen lokale Installation.	23. Okt. 2015	0,5 MB
BMC Client Management - Aktualisierung auf Windows	Diese Handbuch leitet Sie durch die Aktualisierung aller Client Management-Komponenten auf einem Windows-System.	23. Okt. 2015	0,2 MB

Titel	Beschreibung	Datum	Dateigröße
BMC Client Management - Aktualisierung auf Linux	Diese Handbuch leitet Sie durch die Aktualisierung aller Client Management-Komponenten auf einem Linux-System.	23. Okt. 2015	0,2 MB
BMC Client Management - Agentferninstallation	Dieses Handbuch leitet Sie durch Ihre ersten Ferninstallationen für Client- und Relayagenten in Ihrem Netzwerk.	22. Okt. 2015	0,4 MB
BMC Client Management - Betriebsregeln	Betriebsregeln sind eines der Grundobjekte von Client Management und immer verfügbar. Sie werden hier separat erläutert, mit Prozessvorschlägen und einer Referenz aller verfügbaren Komponenten.	22. Okt. 2015	2,2 MB
BMC Client Management - Patchverwaltung	Diese Handbuch leitet Sie durch alle erforderlichen Schritte ,um Ihr Netzwerk vollständig gepatched zu halten. Es erläutert die unterschiedlichen Arten der Patchverwaltung, und wie Sie mittels der Patchinventarisierung einen Überblick über Ihre Patchsituation erhalten können um dann die Systeme entsprechend zu patchen.	22. Okt. 2015	1,0 MB
BMC Client Management - Parameterreferenz	Dieses Handbuch ist eine Ergänzung zu den anderen und erläutert alle in Client Management verfügbaren Module, ihre Parameter sowie die Fehlermeldungen der Software.	22. Okt. 2015	0,6 MB
Gesamte Dokumentation	Diese Zip-Datei enthält alle Handbücher, die in deutscher Sprache verfügbar sind.	23. Okt. 2015	6,7 MB

PDFs em brasileiro

Aqui é o achar toda a documentação do produto em formato PDF.

Documento	Descrição	Data	Tamanho do arquivo
BMC Client Management - Especificações técnicas	Este documento apresenta as informações técnicas iniciais que você precisa saber para começar a instalar o Client Management. Também serão indicados os locais onde você encontrará informações mais detalhadas sobre cada tópico.	20 outubro 2015	0,2 MB
BMC Client Management - Instalação no Windows	Este manual o orienta na primeira instalação local de todos os componentes do Client Management em sistemas Windows.	23 outubro 2015	2,0 MB
BMC Client Management - Instalação no Linux	Este manual o orienta na primeira instalação local de todos os componentes do Client Management em sistemas Linux.	23 outubro 2015	0,5 MB
BMC Client Management - Introdução	O manual de Introdução é um guia abrangente sobre todos os aspectos do software. Ele foi elaborado para o administrador de sistemas e fornece informações gerais do usuário e algumas explicações minuciosas sobre o funcionamento interno do Console e dos objetos do Client Management.	27 outubro 2015	4,4 MB
	Este documento o orienta ao longo do processo de upgrade de todos os componentes do Client Management em sistemas Windows.		0,2 MB

Documento	Descrição	Data	Tamanho do arquivo
BMC Client Management - Atualizaçao no Windows		24 outubro 2015	
BMC Client Management - Atualizaçao no Linux	Este documento o orienta ao longo do processo de upgrade de todos os componentes do Client Management em sistemas Linux.	29 outubro 2015	0,2 MB
BMC Client Management - Detecção de recursos	Este manual o orienta na detecção de sua rede, assim que o master e o console estiverem instalados, como preparação para a distribuição do agente.	20 outubro 2015	0,4 MB
BMC Client Management - Distribuição do agente do cliente	Este manual o orienta nas distribuições do primeiro cliente e agente de relay em sua infraestrutura.	22 outubro 2015	0,4 MB
BMC Client Management - Regras operacionais	As regras operacionais também são um objeto básico e estão sempre disponíveis. Elas são explicadas em um manual separado, que contém não apenas procedimentos de casos de uso, bem como uma referência de todas as etapas de regras operacionais.	20 outubro 2015	2,2 MB
BMC Client Management - Gerenciamento de inventários	Este manual fornece informações abrangentes sobre todos os tipos de inventários disponíveis no Client Management, como gerenciá-los e o que você pode fazer com eles.	20 outubro 2015	0,5 MB
BMC Client Management - Gerenciamento de aplicativos	Este manual fornece informações abrangentes sobre o monitoramento, proibição e recuperação de aplicativos, assim como gerenciamento de licenças de software. Ele ensina a administrar seus aplicativos e licenças e tudo o que é possível fazer com eles.	20 outubro 2015	0,8 MB
BMC Client Management - Gestao de recursos financeiros	Este manual explica como gerenciar os dados financeiros disponíveis de seu ambiente.	20 outubro 2015	0,3 MB
BMC Client Management - Distribuição de software	Este manual orienta em todas as etapas de distribuição de software dentro de sua infraestrutura. Ele explica em detalhes os diversos tipos de pacotes disponíveis, como criar e distribuí-los para os destinos.	20 outubro 2015	3,1 MB
BMC Client Management - Implantação do sistema operacional	Este manual orienta em todas as etapas da implantação de sistemas operacionais nos dispositivos existentes em sua rede. Ele explica os diversos tipos de implantação e todas as opções disponíveis.	20 outubro 2015	1,6 MB
	Este manual o orienta em todas as etapas para manter seu ambiente totalmente corrigido. Ele explica os vários tipos de gerenciamento de patches disponíveis e como inventariar a situação dos patches e aplicá-los em seus sistemas.	20 outubro 2015	2,3 MB

Documento	Descrição	Data	Tamanho do arquivo
BMC Client Management - Gerenciamento de patches			
BMC Client Management - Gerenciamento de conformidade	Este manual explica os dois diferentes modelos de conformidade disponíveis no Client Management - conformidade personalizada e conformidade SCAP. Ele descreve em detalhes todos os diferentes objetos e opções, e orienta ao longo do processo para manter a infraestrutura compatível com as regras e regulamentos de sua organização.	22 outubro 2015	1,0 MB
BMC Client Management - Gerenciamento de energia	Este manual explica a implementação das funções de gerenciamento de energia nos sistemas cliente.	20 outubro 2015	0,4 MB
BMC Client Management - Gerenciamento de dispositivos	Este manual explica como gerenciar os dispositivos periféricos no Client Management.	20 outubro 2015	0,3 MB
BMC Client Management - Controle remoto	Este manual explica as diversas opções disponíveis para acessar remotamente os dispositivos existentes em sua rede e as operações que você pode executar.	20 outubro 2015	0,3 MB
BMC Client Management - Integração Externa	Este manual explica a configuração do Client Management para a integração com o BMC Remedyforce and BMC FootPrints Service Core.	20 outubro 2015	0,3 MB
BMC Client Management - Diagnósticos	Este manual fornece ao administrador do Client Management controles e verificações para investigar se algo não está funcionando corretamente, bem como algumas verificações de sanidade geral. Ele também oferece operações automáticas de reparo, onde for possível.	20 outubro 2015	0,2 MB
BMC Client Management - Referência de parâmetros	Este manual acompanha os outros manuais e explica os módulos disponíveis do software, os respectivos parâmetros e os códigos de erro do software.	20 outubro 2015	0,6 MB
BMC Client Management - Referência técnica	Neste manual, você encontrará informações sobre como se conectar ao Client Management, além de algumas informações técnicas aprofundadas sobre assuntos mais avançados, como SSL, gerenciamento de largura de banda ou descoberta automática.	20 outubro 2015	0,8 MB
BMC Client Management - Referência de banco de dados	Este manual contém instruções específicas de instalação e ajuste do banco de dados, para uso com o Client Management. Se existir um administrador dedicado ao banco de dados, indique a ele este manual, antes de instalar o Client Management.	20 outubro 2015	2,3 MB
Documentação completa	Este arquivo zip contém o conjunto completo dos manuais dos produtos listados acima.	29 outubro 2015	24,1 MB

PDFs en français

Voici vous trouvez toute la documentation du produit en format PDF.

Titre du PDF	Description	Date	Taille du fichier
BMC Client Management - Spécifications techniques	Ce document présente des données techniques préalables que vous devez connaître de lancer l'installation Client Management. Il indique également l'emplacement d'informations plus détaillées sur des domaines spécifiques.	29 octobre 2015	0,2 Mo
BMC Client Management - Installation sous Windows	Ce manuel présente la procédure d'installation initiale de tous les composants Client Management sur des systèmes Windows sur site.	29 octobre 2015	2,0 Mo
BMC Client Management - Installation sous Linux	Ce manuel présente la procédure d'installation initiale de tous les composants Client Management sur des systèmes Linux sur site.	29 octobre 2015	0,5 Mo
BMC Client Management - Mise à jour sous Windows			
BMC Client Management - Mise à jour sous Linux			
BMC Client Management - Introduction	Le manuel d'introduction à Client Management est un guide complet qui présente tous les aspects du logiciel. Il présente à la fois des informations générales sur l'utilisation, et quelques notions de pointe sur le fonctionnement interne de la Console et des objets Client Management.		
BMC Client Management - Découverte réseau	Ce manuel présente la découverte de votre réseau après l'installation du master et de la console en vue de préparer le déploiement de l'agent.	22 octobre 2015	0,4 Mo
BMC Client Management - Déploiement des agents client	Ce manuel présente les premiers déploiements de clients et d'agents relais dans votre infrastructure.	22 octobre 2015	0,4 Mo
BMC Client Management - Règles opérationnelles	Les règles opérationnelles correspondent également à un objet de base, toujours disponible. Elles sont présentées dans un manuel séparé qui présente les procédures de cas d'utilisation et toutes les étapes des règles opérationnelles.	22 octobre 2015	2,2 Mo
BMC Client Management - Inventaires	Ce manuel présente des informations complètes sur tous les types d'inventaire disponibles dans Client Management, ainsi que leur gestion et leur utilisation.	22 octobre 2015	0,5 Mo

Titre du PDF	Description	Date	Taille du fichier
BMC Client Management - Gestion des application	Ce manuel présente des informations complètes sur la surveillance des applications, les interdictions et la résolution, ainsi que la gestion des licences d'application. Il montre comment gérer vos applications et vos licences, et comment les utiliser.		
BMC Client Management - Gestion financière	Ce manuel présente comment gérer les données financières disponibles dans votre environnement.	22 octobre 2015	0,3 Mo
BMC Client Management - Télédistribution	Ce manuel présente toutes les étapes de la distribution de logiciels au sein de votre infrastructure. Il montre en détail les différents types de package disponibles, leur création et leur distribution vers les cibles.	23 octobre 2015	3,4 Mo
BMC Client Management - Déploiement de systèmes d'exploitation	Ce manuel présente toutes les étapes de déploiement de systèmes d'exploitation sur les postes de votre réseau. Il montre les différents types de déploiement, ainsi que les options disponibles.		
BMC Client Management - Gestion de patchs	Ce manuel présente toutes les étapes d'application de correctifs à votre environnement. Il montre les différents types de gestion des correctifs disponibles, comment évaluer la situation de vos systèmes et installer les correctifs manquants.	22 octobre 2015	2,7 Mo
BMC Client Management - Gestion de conformité	Ce manuel présente les deux modèles de conformité disponibles avec Client Management, la conformité personnalisée et la conformité SCAP. Il explique en détail les différents objets et les options, et montre comment appliquer les règles et la stratégie de conformité de votre organisation à votre infrastructure.	22 octobre 2015	0,5 Mo
BMC Client Management - Gestion de l'énergie	Ce manuel présente la mise en oeuvre des fonctionnalités de gestion de l'alimentation sur les systèmes clients.	22 octobre 2015	0,4 Mo
BMC Client Management - Gestion des périphériques	Ce manuel présente la gestion des périphériques dans Client Management.	22 octobre 2015	0,2 Mo
BMC Client Management - Contrôle à distance	Ce manuel présente les différentes les options disponibles pour accéder à distance aux postes de votre réseau, ainsi que les opérations que vous pouvez exécuter.	22 octobre 2015	0,3 Mo
BMC Client Management - Intégration externe	Ce manuel présente la configuration de Client Management pour l'intégration à BMC Remedyforce et à BMC FootPrints Service Core.	22 octobre 2015	0,3 Mo
BMC Client Management - Diagnostics	Ce manuel fournit à l'administrateur Client Management des outils de contrôle et de vérification qui permettent de détecter les éléments défaillants et d'exécuter des contrôles d'intégrité générale. Il fournit également des opérations de réparation automatique, si possible.	22 octobre 2015	0,2 Mo
BMC Client Management - Référence des paramètres	Ce manuel complète les autres manuels et présente les modules disponibles pour le logiciel, leurs paramètres et les codes d'erreur du logiciel.	22 octobre 2015	0,6 Mo

Titre du PDF	Description	Date	Taille du fichier
BMC Client Management - Référence de bases de données		29 octobre 2015	3,2 Mo
BMC Client Management - Référence technique	Ce manuel présente des informations sur la consignation dans Client Management, ainsi que des informations techniques complètes sur des domaines plus avancés tels que le SSL, la gestion de la bande passante et la découverte automatique.	22 octobre 2015	1,3 Mo

PDFs en español

Aquí usted encuentra toda la documentación del producto en formato PDF.

Título	Descripción	Fecha	Tamaño
BMC Client Management - Especificaciones técnicas	El presente documento proporciona los datos técnicos iniciales a tener en cuenta antes de empezar a instalar Client Management. También indica dónde se puede encontrar información más detallada sobre temas concretos.	22 de octubre de2015	0,2 MB
BMC Client Management - Instalación en Windows	Este manual sirve de guía para la primera instalación de todos los componentes Client Management en sistemas Windows con una instalación in situ.	28 de octubre de 2015	2,0 MB
BMC Client Management - Instalación en Linux	Este manual sirve de guía para la primera instalación de todos los componentes Client Management en sistemas Linux con una instalación in situ.	28 de octubre de 2015	0,5 MB
BMC Client Management - Actualización en Windows	Este manual sirve de guía para la actualización de todos los componentes Client Management en sistemas Windows.	28 de octubre de 2015	0,2 MB
BMC Client Management - Actualización en Linux	Este manual sirve de guía para la actualización de todos los componentes Client Management en sistemas Linux.	28 de octubre de 2015	0,2 MB
BMC Client Management - Descubrimiento de red	Este manual sirve de guía para el análisis de la red una vez el máster y la consola están instalados como preparación del despliegue del agente.	22 de octubre de 2015	0,4 MB
BMC Client Management - Despliegue de Agentes	Este manual sirve de guía en los primeros despliegues de agentes de relé y cliente en una infraestructura.	22 de octubre de 2015	0,4 MB
BMC Client Management - Introducción	Este manual contiene una introducción del producto y una presentación de todos sus componentes y los principales tipos de objetos.		4,5 MB

Título	Descripción	Fecha	Tamaño
		22 de octubre de 2015	
BMC Client Management - Reglas operativas	Las reglas operativas también son un objeto básico y siempre están disponibles. Se explican en un manual diferente que, además de abarcar los procedimientos de casos de uso también incluye material de consulta relacionado con todas las acciones de las reglas operativas.	22 de octubre de 2015	2,1 MB
BMC Client Management - Gerenciamento de inventários	Este manual ofrece información exhaustiva sobre todos los tipos de inventarios disponibles en Client Management, cómo gestionarlos y lo que se puede hacer con ellos.	22 de octubre de 2015	0,5 MB
BMC Client Management - Administración de aplicaciones	Este manual ofrece información exhaustiva sobre la supervisión, prohibición y recuperación de aplicaciones, así como la administración de licencias de software. Muestra cómo administrar las aplicaciones y licencias y todo lo que se puede hacer con ellas.	28 de octubre de 2015	0,6 MB
BMC Client Management - Financial Asset Management	Este manual explica cómo administrar los datos financieros disponibles sobre un entorno.	22 de octubre de 2015	0,3 MB
BMC Client Management - Distribución de software	Este manual guía a lo largo de todos los pasos de la distribución de software en una infraestructura. Explica detalladamente los distintos tipos de paquetes disponibles, cómo crearlos y distribuirlos a los destinos.	23 de octubre de 2015	3,4 MB
BMC Client Management - Distribución de sistemas operativas	Este manual sirve de guía a lo largo de todos los pasos de la implementación de sistemas operativos en los dispositivos de una red. Explica los distintos tipos de implementaciones así como todas las opciones disponibles.	22 de octubre de 2015	1,5 MB
BMC Client Management - Administración de parches	Este manual guía a lo largo de todos los pasos necesarios para la correcta administración de los parches en un entorno. Explica los distintos tipos de administración de parches disponibles y cómo analizar la situación de los parches e implementarlos en los sistemas.	22 de octubre de 2015	2,8 MB
BMC Client Management - Controlo remoto	Este manual explica las distintas opciones disponibles para el acceso remoto a dispositivos de la red y todas las operaciones que se pueden ejecutar.	22 de octubre de 2015	0,3 MB
BMC Client Management - Administración de conformidad	Este manual explica los dos modelos de conformidad disponibles en Client Management: conformidad personalizada y conformidad SCAP. Detalla los distintos objetos y opciones, y orienta a lo largo del proceso de mantenimiento de la conformidad de la infraestructura respecto a las normas y reglamentos de la organización.	22 de octubre de 2015	1,0 MB
BMC Client Management - Administración de dispositivos	Este manual explica la administración de los dispositivos periféricos en Client Management.	22 de octubre de 2015	0,2 MB
	Este manual explica la implementación de las funcionalidades de administración de energía en los sistemas cliente.		0,4 MB

Título	Descripción	Fecha	Tamaño
BMC Client Management - Administración de energia		22 de octubre de 2015	
BMC Client Management - Integración Externa	Este manual explica la configuración de Client Management para su integración con BMC Remedyforce y BMC FootPrints Service Core.	22 de octubre de 2015	0,4 MB
BMC Client Management - Diagnósticos	Este manual presenta los controles y comprobaciones para que el administrador de Client Management pueda investigar cuando algo no funciona correctamente, así como algunas comprobaciones generales. También explica operaciones de reparación automática cuando sea posible.	22 de octubre de 2015	0,2 MB
BMC Client Management - Referencia de parámetros	Este manual acompaña a los otros manuales y explica los módulos disponibles para el software, sus parámetros y los códigos de error del software.	22 de octubre de 2015	0,6 MB
BMC Client Management - Referencia de bases de datos	Este manual ofrece recomendaciones generales de hardware para la base de datos y directrices técnicas sobre el tamaño del hardware para su configuración.	22 de octubre de 2015	3,2 MB
BMC Client Management - Referencia técnica	Este manual contiene información sobre el inicio de sesión en Client Management así como información técnica detallada sobre temas más avanzados, como SSL, la gestión del ancho de banda o la detección automática.	22 de octubre de 2015	0,6 MB
Documentación completa		28 de octubre de 2015	23,5 MB

日本語版PDF

e以下は日本語版 PDF として入手可能な製品ドキュメントの一覧です:

ファイル名	説明	日付	サイズ
BMC Client Management - 本バージョンの新機能	このドキュメントは、新しいバージョンの改良点や新機能の概要について説明します。		
BMC Client Management - 技術仕様	このドキュメントは、Client Managementのインストールを開始する前に知っておくべき初期の技術データを提供します。また、各トピックについての詳細情報の参照先も記載されています。	2015年10月29日	0.3 MB
BMC Client Management - Windowsインストール	このマニュアルは、オンサイトインストールにおける、全Client Managementコンポーネントのシステムへの初回インストールについて説明します。	2015年10月30日	1.9 MB

ファイル名	説明	日付	サイズ
BMC Client Management - Linuxインストール	このマニュアルは、オンサイトインストールにおける、全Client Managementコンポーネントのlinuxシステムへの初回インストールについて説明します。	2015年10月30日	0.6 MB
BMC Client Management - Windows上でのアップグレード		2015年10月30日	0.3 MB
BMC Client Management - Linux上でのアップグレード		2015年10月30日	0.3 MB
BMC Client Management - クライアントエージェントのロールアウト	このマニュアルは、インフラストラクチャにおけるクライアントと中継エージェントの初回ロールアウトについて説明します。	2015年10月30日	0.5 MB
BMC Client Management - 操作ルール	操作ルールも基本オブジェクトであり、常に利用可能です。これらについては別のマニュアルで解説されており、手順の例や、すべての操作ルールのステップについてのリファレンスなども一緒に記載されています。	2015年10月30日	1.2 MB
BMC Client Management - パッチ管理	このマニュアルでは、ご使用の環境を常に全パッチが適用された状態に保つための手順を説明しています。利用できる色々なタイプのパッチ管理や、パッチ状況のインベントリ作成、システムへのパッチ適用などが詳しく解説されています。	2015年10月30日	0.7 MB
BMC Client Management - パラメータ リファレンス	このマニュアルには、ソフトウェアで利用可能なモジュールやそのパラメータ、ソフトウェアのエラーコードなどを解説した他のマニュアルも付属しています。		

Support Information

This topic contains information about how to contact Customer Support and the support status for this and other releases.

Contacting Customer Support

If you have problems with or questions about a BMC product, or for the latest support policies, see the Customer Support website at http://www.bmc.com/support. You can access product documents, search the Knowledge Base for help with an issue, and download products and maintenance. If you do not have access to the web and you are in the United States or Canada, contact Customer Support at800 537 1813 . Outside the United States or Canada, contact your local BMC office or agent.

Support status

As stated in the current BMC Product Support Policy, BMC provides technical support for a product based on time rather than number of releases. To view the support status for this release, see the BMC Client Management support status page.

Help for BMC Client Management Online Documentation

The BMC Client Management online documentation is wiki-based. You can provide feedback in the form of comments or "Likes", you can subscribe to pages and get email notifications, and you can export pages to PDF or Microsoft Word.

The following topics are provided:

- Exporting Help topics
- Providing feedback
- Searching BMC Client Management Help
- Subscribing to Help topics

Exporting Help topics

You can export Help topics to Word (one page at a time) or to PDF (a page and its child pages).

To export a single topic to Word

From the page you want to export, click **Tools** at the top of the window and select **Export to Word**.

The Word document appears in your browser's **Downloads** folder.

To export one or more topics to PDF format

1. From the page you want to export, click **Tools** at the top of the window and select **Export to PDF**.
   The **Export to PDF** dialog box appears.
2. To export the current page and its child pages using a predefined template:
   a. Double-click a template (such as **BMC Client Management Documentation**).
   b. Proceed to step 7.
3. To customize the exported PDF:
   a. select which pages to export, click the **Customize settings** link at the bottom left.
      - Selecting **This page and its children** will export the current page and all descendant pages in that branch. If you are on the **Home** page, all pages listed under that page are exported.

- Selecting **Only this page** will export only the current page.
- Selecting **This page and all children with label** will export all pages in that branch that contain a given label. If you are on the **Home** page, all pages in the space which contain the label are exported.

b. *(Optional)* Select from the other available options on this tab:
- **TOC macros** refers to **Tables of Contents** that list headings on some longer pages.
- **Children macros** refers to lists of links to descendant pages on some top-level pages.
- **Thumbnails** refers to images that are shown in a small size on the page. When thumbnails are clicked, the full-size image displays.

c. *(Optional)* To add a title and other information to the exported PDF, click the **PDF Properties** tab and fill in the fields.

d. *Optional)* Choose how you want exported links to behave in the **Linking** tab.

4. Click **Start Export** to begin the export process.
   An **Open/Save** dialog box appears.
5. Select the appropriate option and click **OK**.
   A confirmation message appears that the PDF was created or the PDF opens in a new window.

Related topics

Providing feedback

Subscribing to Help topics

Searching BMC Client Management Help

Help for BMC Client Management Online Documentation

Providing feedback

You can add comments at the bottom of any **Help** topic page. You can also "Like" a page or share it.

To add a comment

1. At the bottom of the page, enter your comment, using the **Rich Text** editor in the **Write a comment** text box.
2. Click **Save**.
   By default, the **Watch this page** check box is selected, which will enable email notifications.

To reply to a comment

You can reply to any comment.

1. Beneath the comment to which you want to respond, click **Reply**.
2. Enter your comment, then click **Save**.

To edit a comment

You can edit your own comments.

1. Beneath your comment, click **Edit**.
2. Edit the comment, then click **Save**.

To "Like" a comment

Click **Like** below a comment.

To "Like" a page

Click **Like** above the **Comments** section.

Related topics

Exporting Help topics

Searching BMC Client Management Help

Subscribing to Help topics

Help for BMC Client Management Online Documentation

Searching BMC Client Management Help

You can search for words and phrases or by page tags (known as "labels"). To limit the search results, you can use standard query operators such as AND or use double quotes to search for an exact phrase.

Basic searching

1. In the left pane, enter your search terms in the **Searching BMC Client Management 12** search box, then click **Go**.
   The advanced search page appears, showing the topics that match your criteria.
2. Click a topic title in the search results to jump to that page.
3. To search using different criteria, repeat steps 1 and 2 on the current page or follow the instructions in Advanced Searching.

Advanced searching

By default, when you enter a search phrase, the wiki searches for either term as an "OR" search (for example, *"password reset* OR reset*") So if you search for *password reset*, results will include pages with either the term *password* or the term *reset*.

To search for an exact phrase , from the advanced search page, enclose the terms in quotes, such as *"password reset"*.

Searching by labels

Labels are "tags" for content, similar to index keywords. Each page can have any number of labels to describe its content. You can find labels at the bottom of pages or by simply searching for a label in the **Search** field.

When you click on a label, a list of all pages that have been tagged with that label appears. By clicking another label in the **Related Labels** section of those results, a list of pages that are tagged with *both* of those labels appears. For example, by clicking an *installing* label, then clicking *Windows* in the results, you can see a list of the pages that contain content that pertains to that specific content.

Related topics

Exporting Help topics

Providing feedback

Subscribing to Help topics

Help for BMC FootPrints Service Core Online Documentation

Subscribing to Help topics

You can be automatically notified via email of updates to page content or of new comments.

To subscribe to a page that you want to watch, select **Tools > Watch**.

Whenever changes are made to the page or its comments, an email will be sent to you.

To cancel your subscription, select **Tools > Unwatch**.

Related topics

Exporting Help topics

Searching BMC Client Management Help

Providing feedback

Help for BMC Client Management Online Documentation

BMC contributor topics

There are currently no BMC contributor topics for BMC Client Management Version 12.1.

Index

BMC Software Inc.
2103 CityWest Blvd, Houston TX 77042-2828, USA
713 918 8800
Customer Support:800 537 1813 (United States and Canada) or contact your local support center