Cimetrics Inc.

B3075 BACnet/IP to BACnet/IP Router User's Manual

Revised July 18, 2023
© 2018-2023, Cimetrics Inc.

Contents

Introduction: Who is this manual for?

This manual is written for engineers and technicians who are responsible for the design, installation, and configuration of BACnet-based building automation systems.

To successfully configure the B3075's core routing functionality, you will need to be familiar with the following terminology and concepts, at a minimum:

TCP/IP) terminology
IP address
IP subnet
Network mask
Default gateway
UDP port

BACnet terminology
BACnet Device Instance Number (a.k.a. "Device ID")
BACnet Device Name (a.k.a. "Device Name")
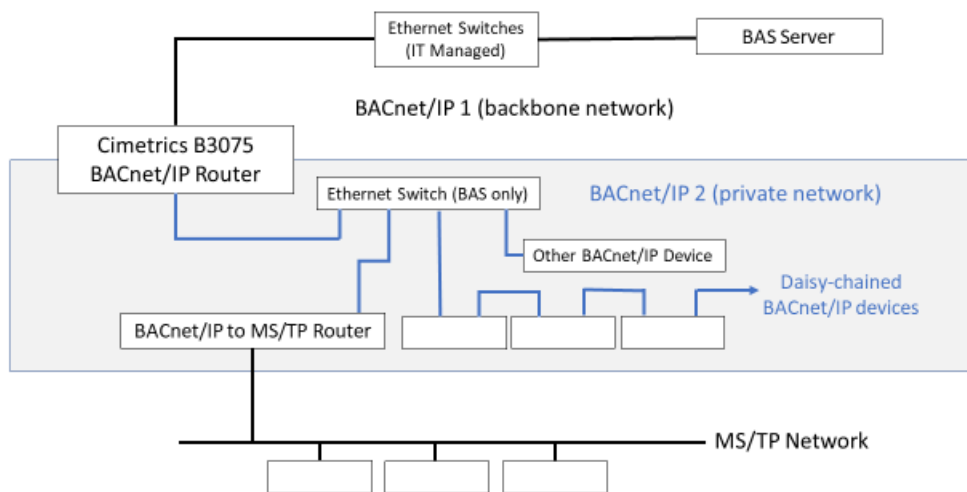BACnet Network
BACnet Network Number
BACnet Router
BBMD (BACnet Broadcast Management Device) – see **Appendix: What does a BBMD do?**

What does a BACnet/IP to BACnet/IP router do, and why is it used?

Many BACnet-based building automation system (BAS) installations contain more than one BACnet network. BACnet routers are used to selectively forward BACnet messages between BACnet networks, allowing the creation of a BACnet internetwork. BACnet/IP employs the UDP protocol (IETF RFC 768) to enable interoperable communication of BACnet messages over IP (Internet Protocol) networks, typically using twisted-pair Ethernet as the data link technology. Since the release of its specification in 1999, BACnet/IP has become increasingly popular even for relatively low-cost BAS devices.

In some facilities, BACnet/IP devices are connected to an IP network managed by the end customer's IT department to reduce the cost of BAS network construction and maintenance. However, there are situations in which it is desirable to create multiple BACnet/IP networks; for example, the BAS integrator might want to put most or all the BACnet/IP devices on one or more private IP networks (installed by the integrator) but use an IT-managed IP network for communication between the private networks or between buildings. The devices on the private network will have IP addresses that are assigned by the BAS integrator. The Cimetrics B3075 was designed for this situation, as shown in the following diagram.

BACnet/IP to BACnet/IP Routing to a Private Network

The B3075 has two Ethernet ports that are used for BACnet/IP communication, and each of those ports will be assigned an IP address appropriate for the directly connected IP network. The B3075 is not an IP router, so the IP addresses of devices connected to the backbone network will not appear on the private network, and the IP addresses of devices connected to the private network will not appear on the backbone network. BACnet/IP network packets originating from devices on the private network will contain the B3075's backbone network IP address when they are forwarded to the backbone network, and BACnet/IP network packets originating from devices on the backbone network will contain the B3075's private network IP address on the private network. The IP address of the originating BACnet/IP device is not lost when a message passes through a BACnet router; it is encoded within the BACnet NPDU by the B3075 in accordance with the requirements of the *BACnet Standard*.

B3075 Functionality Overview

The B3075 is a BACnet/IP to BACnet/IP router with two distinct Ethernet ports for BACnet/IP communication. In this document we refer to those two ports as the "Customer port" and the "Private port". Also, the B3075 has a third physical Ethernet port that is dedicated to local B3075 configuration, and that port is referred to as the "Configuration port" in this document.

The B3075 also has several features that supplement the core BACnet routing functionality. These features are summarized below, and there is additional information later in this document.

Additional BACnet Functionality

The B3075 is a BACnet Device, as defined in the *BACnet Standard*. The Device Object instance number (a.k.a. "Device ID") and the Device Object name (a.k.a. "Device Name") are configurable.

The B3075 can be configured to be a BBMD on the Customer port, with optional support for Foreign Devices.

BACnet packet capture is also supported on both BACnet/IP interfaces, and the packet capture files created by the B3075 can be imported into software tools such as Wireshark. This feature is disabled by default, but it can be enabled by the administrator.

Non-BACnet Functionality

The B3075 includes functionality that is designed to make it easier to manage, monitor, and secure the B3075, including the following:

1. An internal syslog client can forward logged events to an external syslog server.
2. An internal NTP client can retrieve the current date and time from an external NTP server.
3. An internal DHCP client can configure the IP address, network mask, default gateway address, and the DNS server's IP address used by the Customer port.
4. One or two OpenVPN virtual NICs can be enabled at IP addresses in the IP subnet connected to the Private port, permitting non-BACnet communication through the B3075 to devices connected to the Private network. OpenVPN Community Edition client software is required.
5. The factory default private key and operational certificate used by the built-in web server can be replaced.

Note that this additional functionality is optional. It can be enabled by the administrator using the B3075's web-based configuration interface.

The B3075 Hardware

The B3075 product consists of the following hardware:
- A small-form-factor computer with three Ethernet ports, two for BACnet communication and one dedicated for B3075 configuration.
- An AC-to-DC power adapter that converts the AC line (mains) voltage to 12 VDC.
- An AC power cord for the power adapter that is suitable for use in the U.S. and Canada.
- Hardware for mounting the B3075's computer on a flat surface or on a DIN rail.

Due to the changing availability of hardware components that can be used to construct the B3075, the B3075 that you obtained may differ in some respects from the photo shown above. For more detailed information about the hardware, please see the applicable B3075 data sheet.

Limited Warranty

Cimetrics warrants that the supplied B3075 hardware is free from defects in materials and workmanship, and that the B3075 will perform substantially in accordance with the applicable datasheet, under normal and proper use, for two (2) years from the date the B3075 is delivered to the Buyer. This warranty will be void if, in Cimetrics' reasonable opinion, the defect was caused by (a) improper handling, configuration, operation, or testing by anyone other than Cimetrics; (b) failure to install or maintain the B3075 in accordance with the current edition of any applicable safety code or Cimetrics' written instructions; (c) modification or alteration by anyone other than Cimetrics; (d) Force Majeure events or acts of vandalism, sabotage, or hacking; or (e) any other cause outside of normal usage in accordance with Cimetrics' written instructions and/or specifications. Cimetrics' liability for breach of this warranty will be limited to replacement, repair, or refund, in Cimetrics' sole discretion, of a defective B3075 that has been properly stored, configured, installed, used, and maintained by Buyer, and has not been damaged in transit. All terms hereof (except the limitation of liability in the preceding sentence) are subject to Buyer's return of the defective B3075 to Cimetrics without further damage, subject to confirmation of any claimed defect by Cimetrics' inspection. The B3075 that Buyer considers defective must be returned per Cimetrics' standard Return Material Authorization (RMA) procedures.

Basic B3075 Software Configuration

Before you start
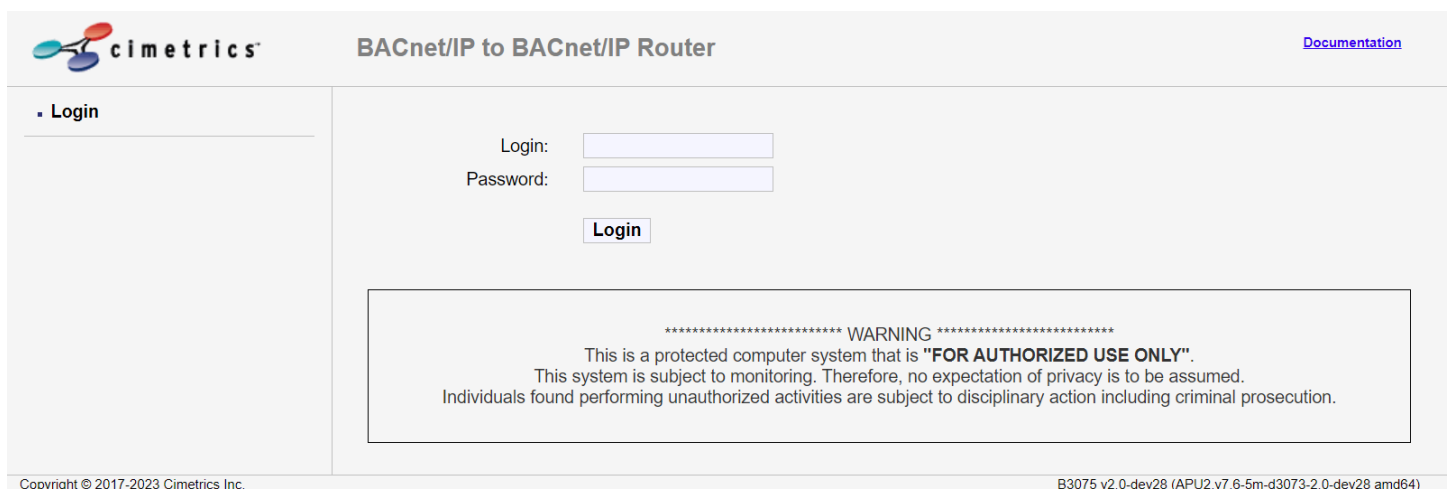
Before configuring and installing the B3075, please ensure that you have the following:

- The B3075 router box.
- The B3075's power adapter and an appropriate power cord.
- An Ethernet cable to connect your PC to the B3075's configuration port.
- The B3075 quick start document, which includes a basic configuration checklist.

You will need to gather the necessary data about your planned installation. Refer to the configuration checklist and to this User's Manual for information about configuring the B3075.

Configuration Interface Overview

Follow the instructions in the B3075 Quick Start document to set up your PC to communicate with the B3075's configuration port, and then connect the PC and the B3075's configuration port using an Ethernet cable. Enter the IP address of the B3075's configuration port in your web browser to access the login page, and if all is well then you should see a login screen like the following:

Enter the login "admin" and the factory default admin password that is written on the label affixed to the bottom of your B3075. Note that the "admin" account is always enabled. You will be required to change the password for the "admin" account upon first use, and the new password must meet the complexity requirement that is displayed. Note: The new password will not be saved until configuration changes are activated, so we recommend that you activate changes immediately after changing the password (see the section **Activate New Configuration**).

Even if you lose the "admin" password, you can reset the B3075 to factory default settings and recover the factory default admin password using the procedure described in section **How to reset to factory default settings if the admin password is unknown.**

Once you have successfully logged in you will see the home page which shows a little information about the B3075:
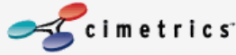
6

To select a specific web page, click on the corresponding menu item on the left side of the window below the Cimetrics logo. After you have finished modifying the configuration parameters on a page, click the "OK" button on the bottom of the page to accept your changes.

After you finish making changes to the B3075's configuration, select "Activate Configuration" to store your changes on the B3075's non-volatile memory and reboot. See the section **Activate New Configuration**.

BACnet Device Settings

The B3075 contains a basic BACnet Device that will respond to a few BACnet service requests. See the B3075's BACnet PICS document for details.

The default BACnet Device Instance Number is chosen at random over a specific range of values, and the default BACnet Device Name is derived from the default Device Instance Number. If you want to change these values, you can do so on the BACnet Device Settings web page, and please remember to click on the "OK" button to accept your changes before you move to a different web page.

Note that the *BACnet Standard* requires that each BACnet Device have a Device Instance Number and the Device Name that are unique across the entire BACnet internetwork to which the Device is connected. It is the responsibility of the system integrator to configure all the BACnet Devices accordingly.
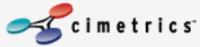
cimetrics

BACnet/IP to BACnet/IP Router

- Home
- BACnet Device Settings
- Customer Network Settings
- Private Network Settings
- OpenVPN Settings
- Network Services
- System Settings

- Network Packet Capture
- Status and Statistics

- Web Server Configuration
- Manage Configuration
- Activate Configuration

Changes are not activated yet

BACnet Device Settings

This page allows you to view/modify BACnet Device settings of the Router, or restore them to factory default.
Device Instance Number and Device Name should be unique across the whole BACnet internetwork.
The BACnet standard and BTL require Device discovery be turned on.

Parameter	Value	Description
☑ Enable discovery of this BACnet Device		Deselect this checkbox to disable sending I-Am/I-Have messages. Routing is not affected by this parameter. (default: enabled)
Device Instance Number	1457433	Instance Number of the Device Object (default: 1457433)
Device Name	B/IP to B/IP Router 1457433	Name of the Device Object (default: "B/IP to B/IP Router 1457433")

OK

Restore default

B3075 v2.0-dev28 (APU2.v7.6-5m-d3073-2.0-dev28 amd64)

Customer Network and Private Network Settings

The B3075 has two Ethernet ports that are used for BACnet/IP communication, referred to as the "Customer port" and the "Private port". Those two ports have different capabilities that correspond to the expected use of the B3075.

> Note: The Customer port is connected to the "Customer network," and the Private port is connected to the "Private network." In one common deployment scenario, the Customer network is configured and managed by the IT network team, whereas the Private network is configured and managed by the BAS integrator.

The B3075's ports used for BACnet/IP communication must be assigned a valid IP address and network mask that are appropriate for the IP networks to which the ports will be directly connected. Both the Private port and the Customer port can be configured with static IP protocol settings, and in most cases this will be appropriate. However, the Customer port can be configured to use DHCP to obtain certain network settings if the IP network to which it is connected has a DHCP server.

> Note: Although the B3075 can be configured to use DHCP to obtain an IP address and other network parameters, the product is a BACnet anchor point used to maintain the integrity of the building automation network. As such, the stability of this product in the IP network environment is critical. For reliable system operation, the B3075's BACnet ports need to be assigned *unchanging* IP addresses and (if required) unchanging DNS names. If DHCP is used, ask the administrator of the DHCP server for a "DHCP Reservation" for the B3075.

The Default Gateway parameter must be configured if a B3075 port is directly connected to a BACnet/IP network that consists of multiple IP subnets. If the BBMD function is enabled on the Customer port, then the Customer port's Default Gateway must be configured. The BACnet UDP Port typically has the value 47808 for both the Customer port and the Private port, but a different UDP port can be configured for each port if appropriate.

The system integrator is responsible for choosing unique BACnet Network Numbers for each of the BACnet networks in a system. A BACnet Network Number is chosen from the range 1 to 65,534. Each of the B3075's BACnet router ports must be configured with the BACnet Network Number that was chosen for the BACnet network to which the port is connected.

Please remember to click on the "OK" button to accept your changes before you move to a different web page.

cimetrics BACnet/IP to BACnet/IP Router   Documentation Logout

- Home
- BACnet Device Settings
- Customer Network Settings
- Private Network Settings
- OpenVPN Settings
- Network Services
- System Settings

- Network Packet Capture
- Status and Statistics

- Web Server Configuration
- Manage Configuration
- Activate Configuration

Changes are not activated yet

Customer Network Settings

[Network Settings] [BBMD Settings]

Network Settings

This page allows you to view/modify Customer network settings, or restore them to factory default.

[Enable DHCP]

Parameter	Value	Description
IP Address	10.14.72.185	IP address of the Router (default: 10.14.72.185)
Network Mask	255.255.0.0	Subnet mask (default: 255.255.0.0)
Default Gateway	10.14.0.1	IP address of default gateway. Leave empty if no default gateway (default: 10.14.0.1)
BACnet UDP Port	47808	BACnet/IP UDP port number (default: 47808)
BACnet Network Number	888	BACnet network number of the directly connected network (default: 888)

[OK]   [Restore default]

Copyright © 2017-2023 Cimetrics Inc.   B3075 v2.0-dev28 (APU2.v7.6-5m-d3073-2.0-dev28 amd64)

---

cimetrics BACnet/IP to BACnet/IP Router   Documentation Logout

- Home
- BACnet Device Settings
- Customer Network Settings
- Private Network Settings
- OpenVPN Settings
- Network Services
- System Settings

- Network Packet Capture
- Status and Statistics

- Web Server Configuration
- Manage Configuration
- Activate Configuration

Changes are not activated yet

Private Network Settings

This page allows you to view/modify Private network settings, or restore them to factory default.

Parameter	Value	Description
IP Address	192.168.0.24	IP address of the Router (default: 192.168.0.24)
Network Mask	255.255.255.0	Subnet mask (default: 255.255.255.0)
Default Gateway		IP address of default gateway. Leave empty if no default gateway (default:)
BACnet UDP Port	47808	BACnet/IP UDP port number (default: 47808)
BACnet Network Number	14617	Directly connected BACnet/IP network number (default: 14617)

[OK]   [Restore default]

Copyright © 2017-2023 Cimetrics Inc.   B3075 v2.0-dev28 (APU2.v7.6-5m-d3073-2.0-dev28 amd64)

BBMD Settings

The BBMD function can be enabled on the Customer port, but not on the Private port. For general information about how BBMDs work, see the **Appendix: What does a BBMD do?.**

The most complex configuration parameter in a BBMD is the Broadcast Distribution Table ("BDT"), which contains the list of BBMDs (identified by each BBMD's IP addresses and UDP port) that will receive forwarded BACnet/IP broadcasts from this BBMD. In most cases (if the netmask is 255.255.255.255 and the target BBMD's UDP port used for BACnet/IP is 47808) you will only need to type in the target BBMD's IP address. If the target BBMD uses a port other than 47808 then you will need to include that port as well as the target BBMD's IP address; for example, "10.14.1.15:47809" indicates that the BBMD at IP

address 10.14.1.15 is using UDP port 47809 for BACnet/IP. It is rare that a netmask other than 255.255.255.255 would be used today, so accepting that default value is almost always correct.

> Note: It is <u>not</u> necessary for you to include the B3075's own IP address in the BDT Entries table. If you do include the IP address of the B3075 in that table, then on the Activate Configuration web page you may see a spurious warning message such as the following: "Some BDT addresses are inside of Customer network with same port."

The Enable Foreign Device Registration option should only be enabled if Foreign Devices need to use this BBMD to relay broadcast messages on their behalf. If enabled, the BBMD will accept a BACnet/IP Foreign Device Registration request from <u>any</u> device.

> Note: Connecting a B3075 so that it is accessible from the Internet or from an untrusted network is <u>not</u> recommended unless appropriate cybersecurity precautions are in place, and this is especially true if the Foreign Device Registration option is enabled.

Please remember to click on the "OK" button to accept your changes before you move to a different web page.

Advanced BBMD Configuration Parameters

Advanced BBMD configuration parameters can be accessed by clicking on "Advanced" near the bottom of the BBMD Settings web page. These advanced parameters rarely need to be modified.

<u>Reject Write-BDT requests</u>

The *BACnet Standard* defines an interoperable method for modifying the Broadcast Distribution Table of a BBMD over the network using a specific BACnet/IP message, Write-Broadcast-Distribution-Table. For

security or reliability, it may be desirable to disable the processing of that message, thus preventing other BACnet devices from modifying the B3075's Broadcast Distribution Table using this message, although disabling such processing is not in conformance with the *BACnet Standard*. To disable processing of the BACnet/IP Write-Broadcast-Distribution-Table message, select "Reject Write-BDT requests"; processing is enabled by default.
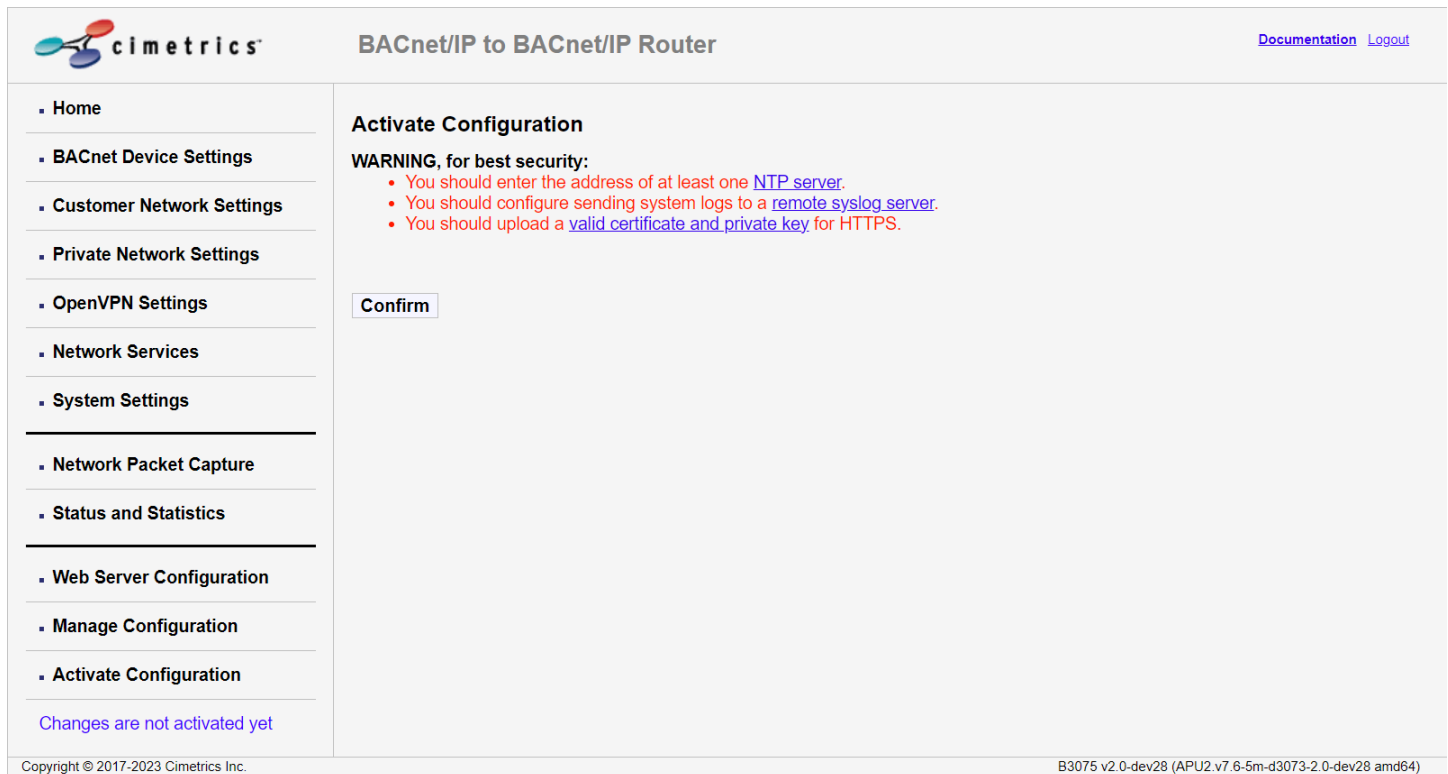
Parameters for BACnet NAT traversal

A B3075 with the BBMD function enabled on the Customer port can be configured to communicate through a network address translation (NAT) router, but this requires careful network design and configuration of the B3075. Please refer to clause J.7.5, "BBMD Operation with Network Address Translation," in the *BACnet Standard* for details.

Activate New Configuration

Once changes are made to any configuration parameter on the B3075, the changes get saved and applied only after the new configuration is activated from the Activate Configuration page. Activation is needed if you see the text "Changes are not activated yet" below the menu, shown in blue letters in the lower left part of the screen shot below. One or more configuration warnings may be displayed. If the B3075 does not detect any configuration errors, clicking on the "Confirm" button will initiate a reboot of the device after the configuration changes have been saved in the B3075's non-volatile memory.

Note that if the B3075 is disconnected from its power source or a logout occurs (manually by the user or automatically due to a timeout), all configuration changes that have not been activated will be discarded.

Within the screenshot:

c i m e t r i c s

BACnet/IP to BACnet/IP Router   Documentation Logout

- Home
- BACnet Device Settings
- Customer Network Settings
- Private Network Settings
- OpenVPN Settings
- Network Services
- System Settings
- Network Packet Capture
- Status and Statistics
- Web Server Configuration
- Manage Configuration
- Activate Configuration

Changes are not activated yet

Activate Configuration

WARNING, for best security:
- You should enter the address of at least one NTP server.
- You should configure sending system logs to a remote syslog server.
- You should upload a valid certificate and private key for HTTPS.

Confirm

Copyright © 2017-2023 Cimetrics Inc.   B3075 v2.0-dev28 (APU2.v7.6-5m-d3073-2.0-dev28 amd64)

Additional Features
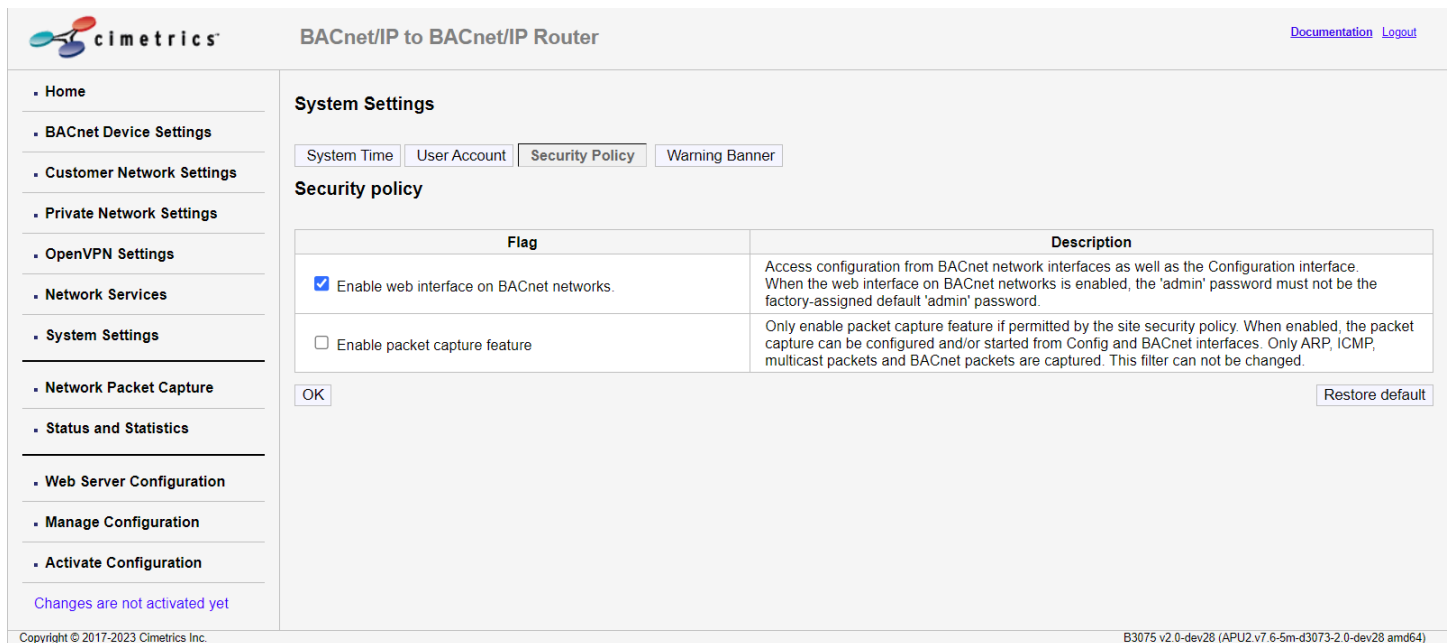
In addition to the core BACnet routing functionality and the local configuration interface, the B3075 provides additional functionality that can be selectively enabled by the user.

Access to the Configuration Interface from a BACnet Network

By default, access to the web-based configuration interface of the B3075 is only possible by connecting a PC to the B3075's configuration port, as described in the *B3075 Quick Start*. However, you have the option of enabling access to the configuration interface through the B3075's Customer port and Private port as well. To enable access, select the security policy "Enable web interface on BACnet networks" from the Security Policy tab of the System Settings web page. Click on the "OK" button to accept your changes before you move to a different web page.

Please note that not all configuration parameters are modifiable when the web-based configuration interface is accessed from a PC connected to the Customer network or the Private network.

When this feature is enabled, the B3075's configuration interface can be accessed at the IP address of the B3075's Customer port from the Customer network or at the IP address of the B3075's Private port from the Private network.

Internal Diagnostics

The Status and Statistics page shows the output of various internal tools that, in aggregate, provide a technically dense view of the health of the B3075 since its last reboot. If you suspect that the B3075 is malfunctioning or that it might not be correctly configured, you can click the "Save Internal Diagnostic Info" button to save diagnostic information in a file that you can send to [Cimetrics technical support.](#) You should also download and send the B3075's current configuration file (see **Managing B3075 Configuration**) with the internal diagnostic file.

Network Packet Capture

The B3075 can be configured to capture BACnet/IP packets that are sent or received on either BACnet port. A few other types of packets are also captured. The files containing the captured packets can be downloaded using the configuration interface and then viewed using applications such as Wireshark.

Network packet capture is off by default and must first be enabled through the configuration interface using the checkbox "Enable packet capture feature" on the System Settings web page, Security Policy tab.

Click on the "OK" button to accept your changes before proceeding.

When you enable network packet capture, you should also set the B3075's system time from the System Settings web page System Time tab. This will ensure that the packet timestamps will be reasonably accurate, assuming that the connected PC's clock is accurate. (This is not necessary if NTP is being used for time synchronization.)

Navigate to the "Activate Configuration" web page to save the new configuration and reboot. You should now be able to start capturing network packets.

The simplest way to capture packets is to use the B3075's internal RAM for temporary packet storage. Click the "Start" button to begin the capture. You can click on the "Stop" button to terminate a running packet capture, and then click "Download files" to download the compressed packet capture file(s). The packet capture files created by the B3075 are managed as a ring buffer: When the last file is full, the oldest file is removed, and the resulting free space is reused to create a new file. Under normal conditions, packet capture continues until explicitly stopped by the user.

> Note: The packet capture files stored in the B3075's internal RAM are not persistent, so they will be erased when the B3075 is rebooted.

16

If you want to do a packet capture that is expected to require a considerable amount of memory, you can use a USB memory stick to store the files containing the captured packets. Insert a formatted memory stick into one of the B3075's USB ports, and then navigate to (or refresh) the Network Packet Capture web page. If the memory stick is recognized by the B3075, you should now see something like the following:

Select the "USB disk" as the location for the captured packets, select the number of packet capture files and the maximum size of each file, then click on the "Start" button to begin capturing packets. You should click on the "Stop" button to terminate a running packet capture.

<mark>Be sure to click on "Eject" before you physically remove the memory stick from the B3075.</mark>

Configuring and Using the VPN Functionality

By default, the B3075 will only forward BACnet/IP messages. However, there are situations in which it is desirable to permit client devices connected to the Customer network to communicate with devices connected to the Private network using a different network protocol, such as HTTPS. When this is functionality is needed, the B3075 may be configured to allow the use of OpenVPN community edition client software on a PC that is connected to the Customer network. TAP mode is used, allowing the use of both IP-based and non-IP protocols.

> Note: Consult with your customer's IT department before enabling the B3075's VPN functionality.

To configure the B3075's VPN server functionality, login as admin then navigate to the OpenVPN Settings web page. You can choose from two modes of VPN operation:

1. "Insecure OpenVPN" mode: The VPN client configuration file can be freely downloaded from the B3075's login web page. The VPN will be automatically disabled after a certain period (configurable by the admin user). We sometimes refer to this as "construction mode" because it is particularly useful while the automation system is being configured and commissioned.
2. "OpenVPN" mode: The VPN client configuration file can only be downloaded by the admin user. There is no time limit in this mode.

Both modes may be used simultaneously, with a limit of one active client per mode. In both modes, the B3075's built-in VPN server is present on the Customer port. For each mode, select an unused IP address on the Private network for use by the VPN's virtual interface.

Replacing the Web Server's Private Key and Certificates

The B3075's web server uses the HTTPS protocol for communication with web browsers. The B3075 ships with a pre-assigned private key and a self-signed operational certificate that are used by the B3075's web server.

> Note: Modern web browsers will display security warnings when they navigate to a web server that uses a self-signed certificate. For example, Google Chrome says that the B3075's web pages are "not secure" and that the "certificate is not valid".

It is possible to replace the B3075's pre-assigned private key and the self-signed operational certificate. You can generate these using a software tool such as contained in OpenSSL. The use of such tools is outside of the scope of this document. Once you have created the private key file and the corresponding operational certificate files (PEM format), navigate to the System Settings page, and choose the Web Server tab, as shown below. To replace and existing file, click on "Choose a file" and then select a file on your PC to upload to the B3075.
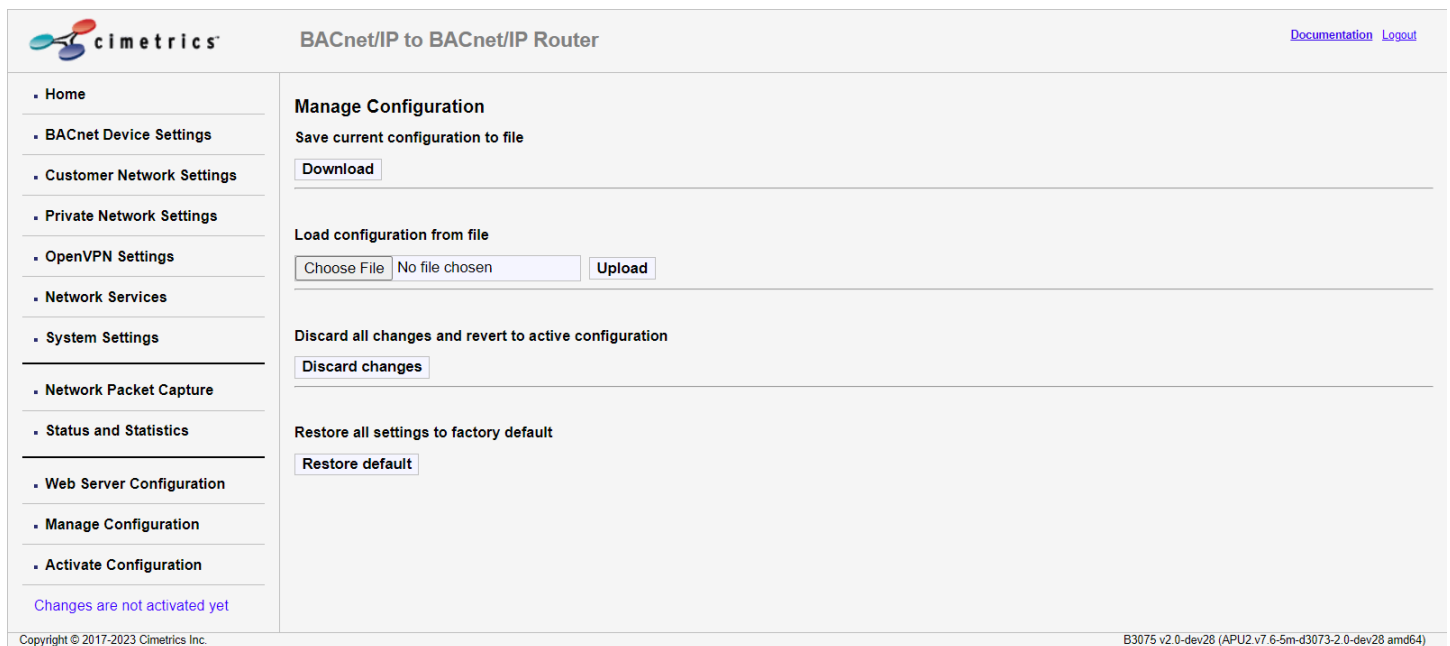
Managing B3075 Configuration

You may save the B3075's configuration in a file, and later load the configuration file into the same B3075 or into a different B3075 that is running compatible firmware. After you load a configuration file you may make additional configuration changes if desired. Configuration changes that are made by any method do not take effect until the new configuration is activated (see **Activate New Configuration**).

The B3075's account passwords, HTTPS-related configuration files, and OpenVPN client configuration files are <u>not</u> contained in the B3075 configuration file for security reasons. These sensitive data will <u>not</u> be restored when you load a B3075 configuration file.
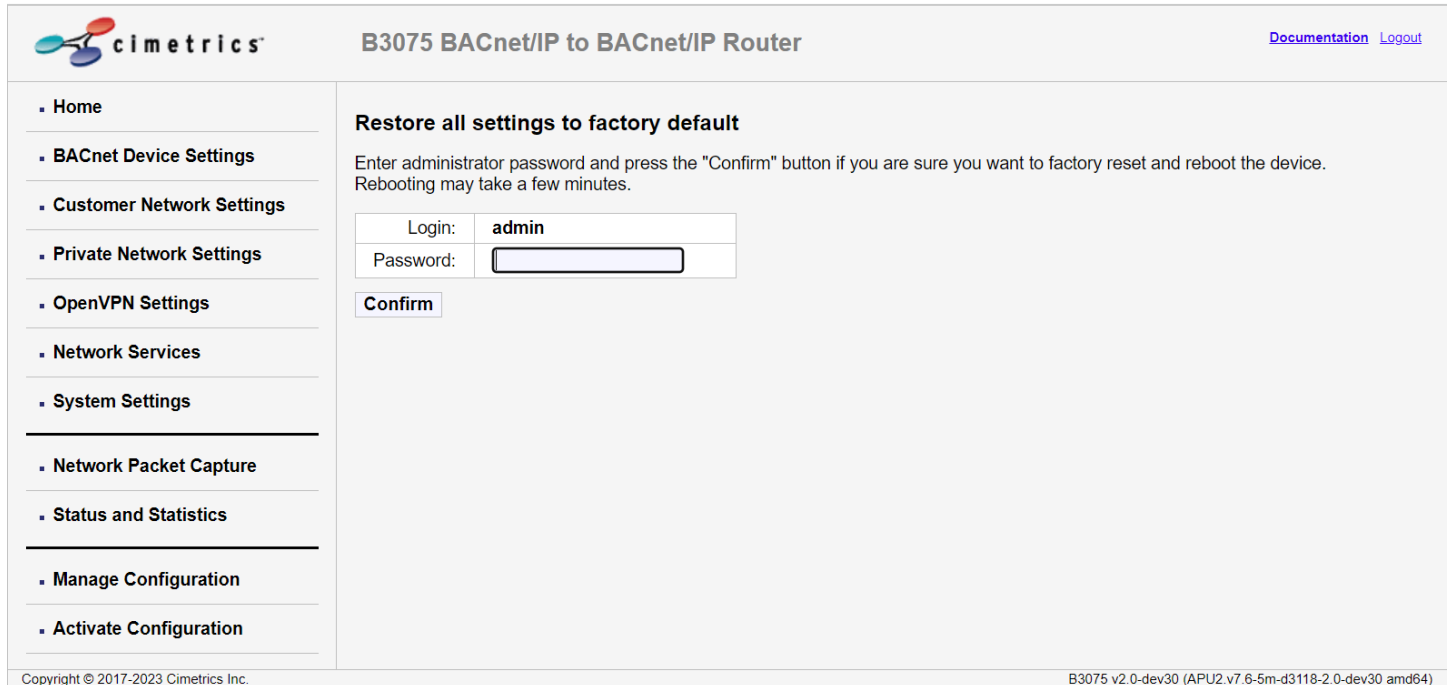
Note that directly editing a saved configuration file is not recommended. All configuration changes should be done via the B3075's web interface.

Resetting the B3075 to Factory Default Settings

If you know the password for the admin account, you can easily restore the factory default settings. Navigate to the "Manage Configuration" web page. After you click on the "Restore default" button, you will see the following password challenge:

Once you enter the current admin password and then click on the "Confirm" button, the B3075's current configuration will be replaced by the factory default configuration, and the B3075 will reboot. You can then reconfigure the B3075 as required after you login using the factory default admin password.

How to reset to factory default settings if the admin password is unknown

Even if you don't know the current password for the admin account, it is still possible to restore all factory default settings and to recover the factory default admin password. To do this, you will need a USB mouse, a PC, an Ethernet cable, and physical access to the B3075. The recommended procedure is as follows:

1. Connect a USB mouse to one of the B3075's USB ports, and then power cycle the B3075 by disconnecting its external power adapter from AC power for several seconds. It will take a couple of minutes for the B3075 to reboot after the power is restored.
2. Connect a PC to the B3075's configuration port using an Ethernet cable, and then using the PC's web browser connect to the B3075's built-in web server as described in the B3075 Quick Start document.

3. After you see a web page like the one above that instructs you to unplug the USB mouse from the router, please do that. This must be done before the next step.
4. Click on the "Reset configuration" button. If all is well, you should see a web page like the following:

You can reconfigure the B3075 as required after you login using the factory default admin password, which is shown on the web page.

Appendix: What does a BBMD do?

BBMDs forward BACnet broadcast messages within BACnet/IP networks that span multiple IP subnetworks. The BACnet protocol utilizes broadcast messages for certain functions, such as the discovery of BACnet devices and for time synchronization. Also, BACnet networks and BACnet routers are discovered using BACnet broadcast messages. See the *BACnet Standard* for more information about BACnet broadcast messages.

IP routers (also referred to as "IP gateways") join IP networks together so messages from devices connected to one network can be sent to devices connected to another network. If your BACnet devices' networks are interconnected via IP routers, then BACnet/IP broadcast messages that are transmitted as UDP broadcasts will normally be blocked by an IP router. To solve this problem the *BACnet Standard* defines the behavior of the BBMD (BACnet/IP Broadcast Management Device) in Annex J.

BBMDs typically use UDP unicast messages to forward BACnet/IP broadcast messages. A BBMD directly forwards a BACnet broadcast message initiated by a BACnet/IP device on the BBMD's subnet to other BBMDs and to its registered Foreign Devices in accordance with its configuration. Upon arrival at a destination BBMD, the message is then transmitted (as a UDP broadcast) on that subnet by the destination BBMD and is also sent to the destination BBMD's registered Foreign Devices.

A BACnet/IP device can register with a BBMD as a Foreign Device if that configuration option is enabled. A registered Foreign Device becomes a member of the BACnet/IP broadcast domain, and it will receive forwarded BACnet/IP broadcast messages from the BBMD. A Foreign Device can also request that messages be broadcasted by the BBMD on the Foreign Device's behalf. Foreign Devices are typically connected to an IP subnetwork that does not have a connected BBMD.

Here are some other important characteristics of BBMDs that should be noted.

> 1. BBMDs only forward BACnet/IP broadcast messages, not unicast messages. BACnet/IP unicast messages are sent directly by the originating device to the destination device.
>
> 2. There is no standard method for a BBMD to discover other BBMDs that it should communicate with, so each BBMD must be configured with a list of the addresses of the other BBMDs to which it should forward BACnet/IP broadcast messages.
>
> 3. A BBMD that receives a forwarded BACnet/IP broadcast message from another BBMD will <u>not</u> forward that message to any other BBMDs.
>
> 4. To ensure that BACnet/IP broadcast messages flow in both directions between two BBMDs and between devices connected to their respective IP subnets, each BBMD must be configured to forward broadcasts to the other BBMD.
>
> 5. In almost all situations, there should be at most one BBMD attached to an IP subnetwork containing BACnet/IP devices.

To find out more about BACnet broadcast management and how to build a wide area network with BACnet you may refer to the classic article "Building Wide-Area Networks with BACnet" written by Bill Swan.