Mimo Control Powered by Moki User's Manual

MCT-MC1-OPT / MCT-MC2-OPT / MCT-MC3-OPT

1 Year	2 Year	3 Year

Please keep this manual for future reference.

INTRODUCTION

OBJECTIVE

In addition to instructing Moki customers about how to perform administrative tasks, the primary purpose of this document is to educate them about how Moki works. This document is specifically tailored toward deployment, system and device managers and other administrators who have previously participated in an over-the-phone onboarding with a Moki representative. This call is typically a 1-2 hour session to welcome you and your organization to the Moki family and walk through most of the basics needed to get a deployment underway. If this introductory call has not taken place, please contact Moki's Customer Success Department.

ACCOUNT BASICS

HOW TO ACCESS MOKI

- https://app.moki.com
- Moki strongly recommends using **Google Chrome** as your web browser for working with Moki Control.

LOGGING IN

Before logging in to Moki for the first time, make sure you accept your Moki administrator invitation by following the link provided in your email. Every subsequent log in can be done at https://app.moki.com in your web browser. Once logged in, you will see several links aimed to help you manage your devices. Pages include:

- **Dashboard**: Provides a useful glance at account data and links to view your devices or deeper analytics for your device estate.
- **Devices**: This is your primary page for tracking and managing individual devices. You can perform actions such as restarts, take screenshots, and change applications app setting. View all device details as well as custom data, on-device inventory, action history, and device events.
- **Device Groups**: This is your Moki workhorse. Device groups allow you to perform mass changes and updates on your entire estate or on smaller subgroups of devices. This is where you build and schedule action sequences to send to your devices.
- **Action History**: Shows you both pending scheduled actions as well as your history of actions sent to devices. If you have two-person authorization configured and you are an approver, this is where you go to approve requested actions.
- **Enroll**: Create enrollment codes with installation instructions for devices upon first enrollment, including apps, profiles, and device tags.
- **Android Profiles**: Setup device configuration profiles including wifi, device settings, check in intervals, and app lock.
- **Apps**: Upload new apps or delete old apps.
- **Alerts**: Set up alerts for your account and devices.
- **Tags**: Create tags you can apply to devices to make grouping them easier.

DEVICE LIST

The device list gives you the ability to track individual devices in your estate. This section will help you understand the many ways you can look at your devices.

DEVICE INFORMATION

DETAILS

In this tab you can:

- **Rename Device**: Rename your device by clicking on the title and then clicking the "enter" key or

clicking on the check button.

- **Tags**: Apply tags to your device for easier tracking and grouping (see the section Tags for more information).
- **Notes**: Add plain text notes to your device. This is helpful for tracking issues on particular devices or making special notes for the use of others.
- **Device Information**: This section tells you the base information about the device including manufacturer's information, battery level, storage capacity, and operating system details.
- **Screenshots**: When you request a screenshot of your device that image will be available here.
- **Network Information**: Details about your device's network connection.
- **Custom Data**: Contains any custom data for your device generated by your Moki SDK enabled applications.

CUSTOM DETAILS

The custom details tab allows users to create a customized view of all details available to Moki about your devices. With this, you have quick access to those details that matter most to you. When you configure this page it carries over to all of the devices you view in your account. To edit these details:

1. Click on the select input box to review your data options. You can search for data or scroll through the elements to choose them.
2. Click the data elements to toggle them on and off in your view.

NOTE: In order to add custom data into columns, or search the values, you must first enable them on this tab.

ADVANCED

This tab shows you current alerts, specialized security information, and applied certificates.

INVENTORY

The inventory tab lists your device's managed apps, installed apps, and applied profiles. You can see details about your apps, including version and package name. You are able to delete managed applications from your device as well as applied profiles.

ACTION HISTORY

You can view any automated or manually requested actions on your device, including the time requested and completed. You can also see which actions may have failed.
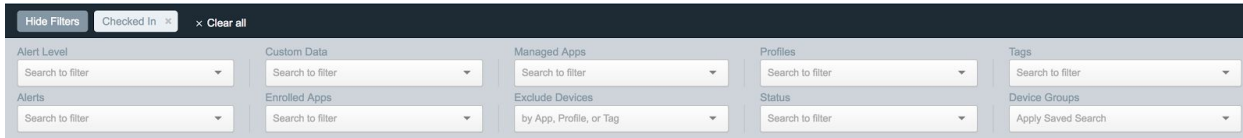
EVENTS

This tab allows you to view all events that have occurred on your device, including application changes and crashes, network connection changes, device or application restarts, and all changes to custom data. You can filter your events to see which events have occurred over time. You can customize your column layout and chose the event details that are the most useful to you. Like the Custom Details tab, customizations you make will carry over to all devices you view.

If you wish to view events for more than one device at a time you can view them in your device groups by clicking on the "Events" link.
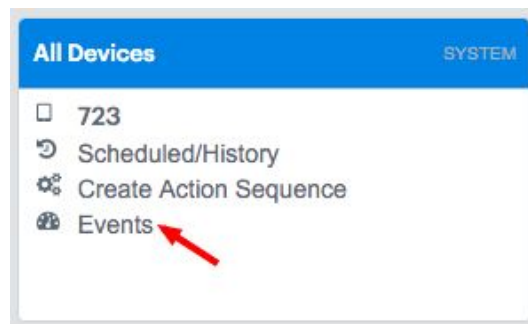
DEVICE SEARCH AND FILTERS

The device list contains a filter section to allow users to find devices that meet specific criteria. Filters can be exposed or hidden by clicking the "Show Filters" button. Applying filters is additive and you can apply more than one filter to your list. Doing so will further narrow your devices. To add more than one filter, click "Enter" on your keyboard to apply and select the next filter. Filter options include:

- **Alert level**: show all devices with alerts of the specified level
- **Alerts**: show all devices a specific alert type
- **Custom Data**: show all devices that have a current custom data value
  - Custom data is defined in apps using the Moki SDK. Custom data keys are established in the custom app schema, and when a data type is also specified, such as an integer, Moki can present operator controls for your searches
- **Enrolled Apps**: show all devices that have a specific Moki SDK enabled app installed
- **Managed Apps**: show all devices that have a particular version of an app installed
- **Exclude Devices**: excludes all devices on your list that meet certain criteria
- **Profiles**: shows all devices with a particular profile installed
- **Status**: shows all devices that are "Checked In" or "Checked Out"
- **Tags**: shows all devices with a particular tag applied
- **Device Groups**: shows all devices from a specific device group

When you would like to alter the applied filters, you can remove them individually by clicking the "X" in the applied filter or you can clear them all by clicking the "Clear all" button.

DEVICE ACTION BAR

The device action bar allows you to control your devices individually, as needed, rather than in a scheduled mode. There are three main controls in this bar: actions, profiles, and apps. Once you have selected a device, you may use these tools to perform actions or install profiles or applications. The next sections outline more specifically what is possible.

ACTIONS

Clicking the actions menu allows you to select and apply one of these predefined MDM actions. Some of these actions require a second step of configuration before completing.

- **Factory Reset**: sends a factory reset command to the device and unenrolls the device from Moki
- **File Management**: push files to your device or request download files from the device. These are files only available to the user. You cannot upload or download files in the system folder
- **Lock**: takes the device to the lock screen
- **Re-enroll**: migrate your device to another Moki account
- **Refresh**: requests all device logs as well as completes inventory on profiles, managed apps, and installed apps
- **Reset Password**: clears the password if one is set, forcing users to set a new one
- **Restart Android**: reboots the device

- **Take Screenshot**: take a screenshot of your device. Screen image is viewable on the details tab of the device
- **Wake Android**: wakes the device from the lock or sleep screen

APPS
Clicking this menu allows you to select available managed apps to push to your device. Managed apps are those apps that have been added to your account by administrators for installing on your devices. It is important to note that Android doesn't allow you to "downgrade" an application. You can only upgrade applications. If you wish to install an older version of an app, you must first delete the application from your device and then install the older version.

PROFILES
Clicking this menu allows you to choose from your configured Android profiles. These can be wifi settings, device settings, and application locks. Profiles are setup by administrators and can then be pushed and installed.

CUSTOMIZING YOUR VIEW
One convenient feature of the Moki user interface is that you can choose to arrange the columns in your device list view according to those elements that are most important to you. You can choose to:
- Resize columns
- Show/Hide columns (see image below)
- Arrange columns in your desired order
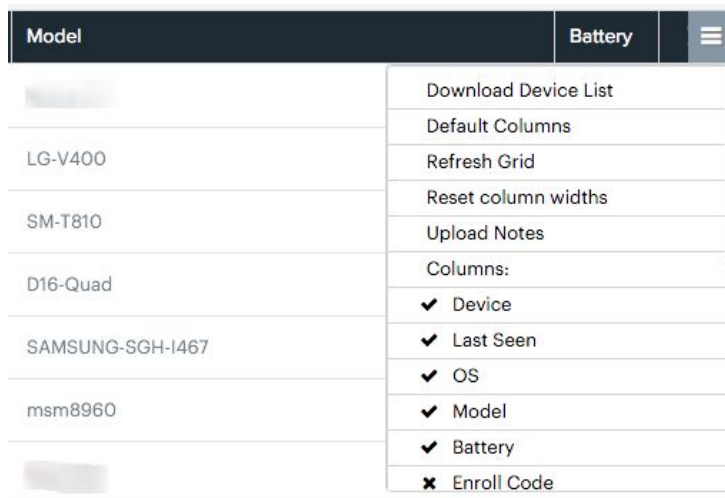
These configuration changes are saved as part of your user profile so they will be there for you no matter where you login. You can reset your view by clicking on the "Default Columns" option and by clicking "Reset column widths".

MANAGING DEVICE GROUPS
Device groups allow you to organize and manage your devices using a variety of criteria. They can speed up the process of managing your devices by allowing you to target specific groups to send commands and actions to.

There is one default device group for all of your devices.
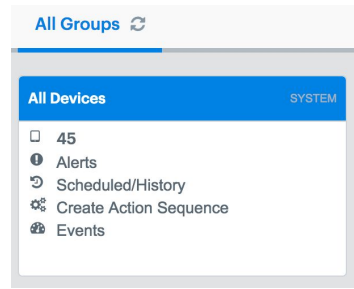
A Dynamic Device Group will allow devices that are added or removed from your account to join the group or leave the group automatically. A Dynamic Device group can be set to pull in devices based on a set of criteria. It is good practice to use Tags to label and organize your devices. The tags you apply will be very effective in creating and managing device groups. If devices are added in the future that match the criteria, they will automatically be added to the group.

A Static Device Group is a group of devices that you determine which devices to be included. Once the group is defined, it cannot be changed. This group can also be based on a variety of criteria to populate the group, but it will not automatically update and pull new devices that might meet that criteria in the future.

Let's look at a situation in which you might use device groups. For example, if you have deployed devices to a specific region, a "Region 1" tag might be appropriate. Creating a Device Group that pulls using the "Region 1" tag will allow you to quickly target those devices for sending commands like a Restart or Lock command. It will also allow for easier management of the Apps that are on those devices. You can schedule commands and actions like Installing an App or Profile for your Device Groups.

CREATING A DYNAMIC DEVICE GROUP

Dynamic device groups are groups of devices whose membership changes when new devices, which meet the group criteria you have defined, are added to your account or when devices are deleted or change their designation.

Firstly, you will need to go into the Device Groups tab within your Moki Control browser window. From there select the New Device Group button.
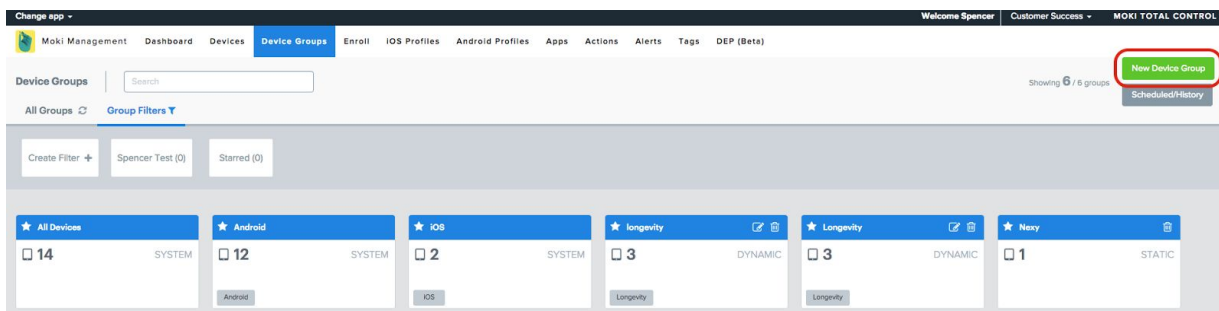
A dynamic list is a list of devices determined by search filters. You can select filters via the text fields on the left, such as OS, apps, and whether the device is checked in or not. When your list is refined to your requirements, give it a name and Save the group. Any new devices that fit the criteria to this group will be added automatically.

FILTERS

Moki has provided specialized operators for creating effective filters both in the device list view and in the device group configuration interface. There are operators for integer based data and string based data. This is particularly important if you are using a [Moki SDK](#) enabled application that passes data to and from devices.

- Integer operators
    - **=** : Matches all values equal to your value and returns those devices.
    - **<** : Matches all values less than to your value and returns those devices.
    - **<=** : Matches all values less than or equal to your value and returns those devices.
    - **>** : Matches all values greater than your value and returns those devices.
    - **>=** : Matches all values greater than or equal to your value and returns those devices.
    - **!=** : Matches all values not equal to your value and returns those devices.
    - **EXISTS**: provides boolean operations to test if a custom data element is present regardless of values.
    - **NOT EXISTS**: provides boolean operations to test if a custom data element is not present.
- Text operators
    - **=** : matches text exactly and returns devices with that text.
    - **EXISTS**: provides boolean operations to test if a custom data element is present regardless of values.
    - **NOT EXISTS**: provides boolean operations to test if a custom data element is not present.

CREATING A STATIC DEVICE GROUP

Static Device Groups are device groups whose member devices are selected at group creation. Once the group is created devices cannot be added to it.

Before you begin, you will need to go into the Device Groups tab within your Moki Control browser window. From there select the New Device Group button.
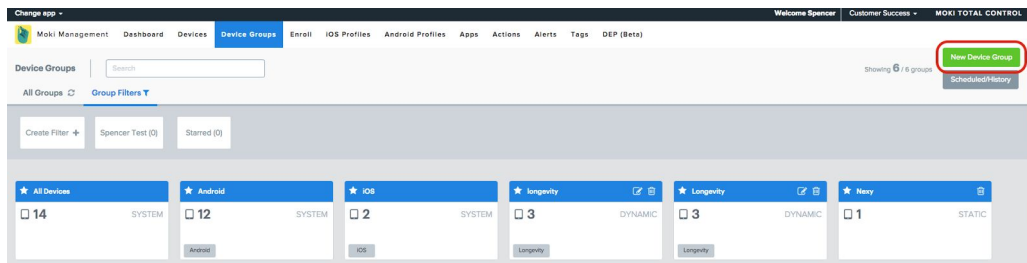
Select each device that will be part of your device group from the list provided. This list can be modified through the use of filters, allowing you to refine the list of devices that are selected. When you have completed your list, give it a name and select Save.

HOW TO SCHEDULE DEVICE ACTIONS

Once you have created your device group you can easily set up scheduled actions to manage your group of devices. To start creating actions click on the "Create Action Sequence" link:

In the next screen you choose your actions and order them in the sequence you would like them to run:

Drag each action into the command sequence space, in the example below there are two action tiles selected – "Install Android App" and "Restart Android". Note that some actions require further configuration and contain a link called "Click to finalize":
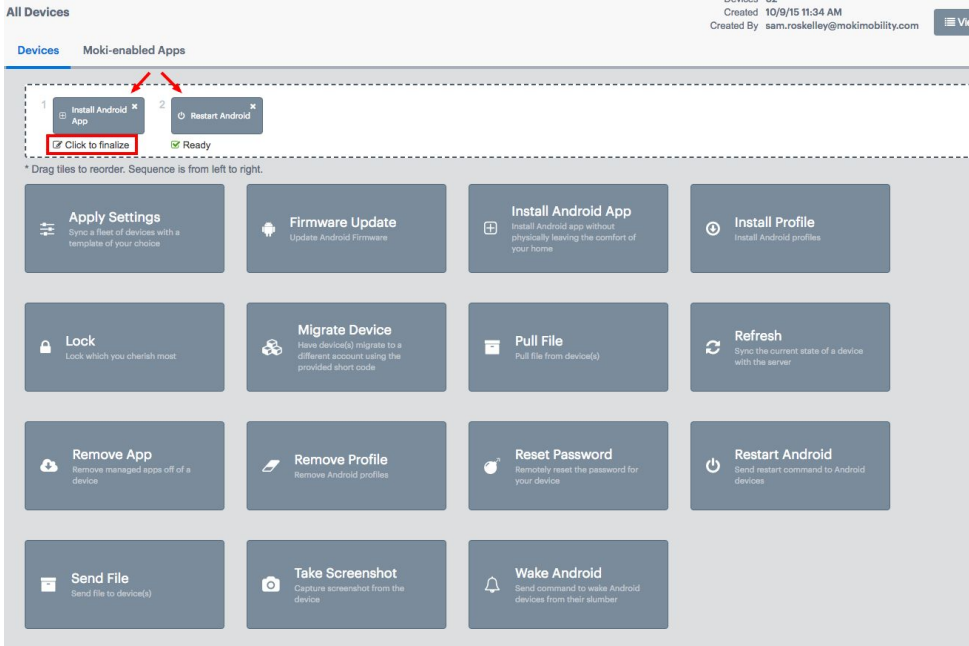
For app installation you need to select the app you wish to install:
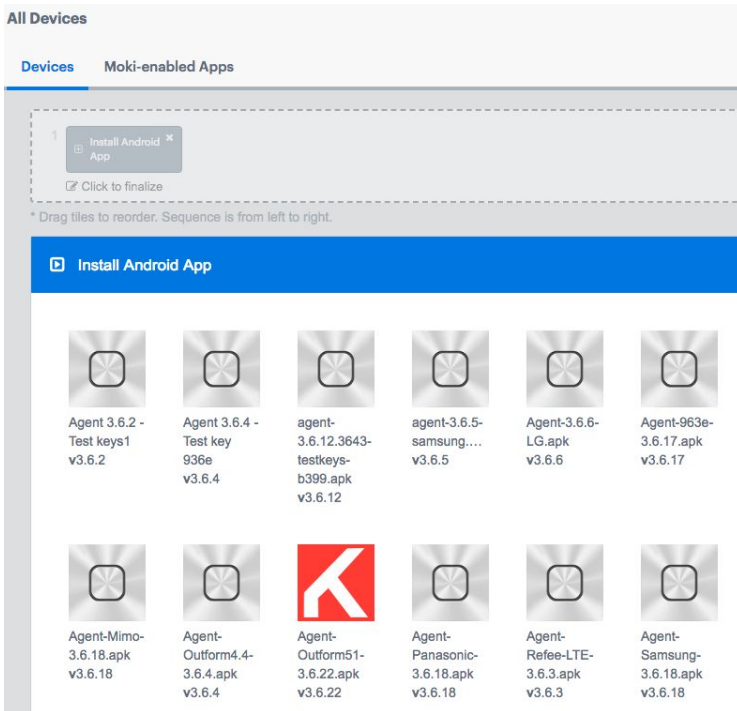
Once configured click the "Schedule" button:

Next you need to set your details for running the action:

The following options are available for setting schedules:
- Schedule Action Time
    - Set date and time
    - Determine if this is a one time or daily recurring action
- Select Timezone
    - Choose the timezone for the time you have set. This will kick the action of for all devices in the group at the same time. For example if you have devices in US Eastern, Central, and Pacific and you set the scheduled action timezone for 3AM Mountain time, the actions will be sent to all devices at that time (5AM Eastern, 4AM Central, and 2AM Pacific respectively).
- Scheduled Run Window (optional)
    - The start and end window will only allow the action to be run on the devices during that timeframe on the LOCAL TIME of the device. If for some reason your device is offline during the run window, the run window will prevent the action from running on that device until the next possible run window time.
- Sequence Expiration Time (optional)
    - Setting an expiration time clears the action from any devices where it is still waiting to be processed. This prevents action build up in devices that have been offline for an extended period. This setting is optional but recommended especially if your action contains a restart command.

Once you have determined your scheduled settings click "Next"

In the next screen you can optionally rename your sequence, then click "Confirm"

On the confirm screen you can click to "View Progress" to see status on your action:

AVAILABLE ACTIONS

- **Lock**: takes the device to the lock screen
- **File Management:** push files to your device
- **Re-enroll**: migrate your device to another Moki account
- **Take Screenshot**: take a screenshot of your device. Screen image is viewable on the details tab of the device
- **Reset Password**: clears the password if one is set, forcing them to set a new one
- **Wake Android**: wakes the device from the lock or sleep screen
- **Restart Android**: reboots the device
- **Install Profile**: installs profile
- **Remove Profile**: removes a profile
- **Install App**: select from the .apks listed in the Apps tab
- **Remove App**: remove a managed app from the device

ACTION HISTORY

Moki allows you to view action history in three ways. First, by clicking on the "Action History" navigation, you are able to view all scheduled actions in the system including those that are pending and those that are completed.

SCHEDULED ACTIONS (PENDING)

In the Scheduled tab, you can see all pending scheduled actions. If you have 2-Person Authorization enabled, this is where you can approve or reject requested scheduled actions.

SCHEDULED ACTIONS (HISTORY)

In the History tab you can view all actions that have been run in the account. You can track success rate for your devices and determine next steps, if needed.

DEVICE GROUPS

Each device group contains a link to view the Scheduled Action history filtered for actions applied to that device group.

DEVICE ACTION HISTORY

You can view all actions that have occurred on a specific device by clicking on the device in the Device List and then clicking on the action history tab. You can track all actions for the device, including automated actions such as those run on each heartbeat (Query Extended Information) and any manually run actions along with their current status; which can be one of the following:
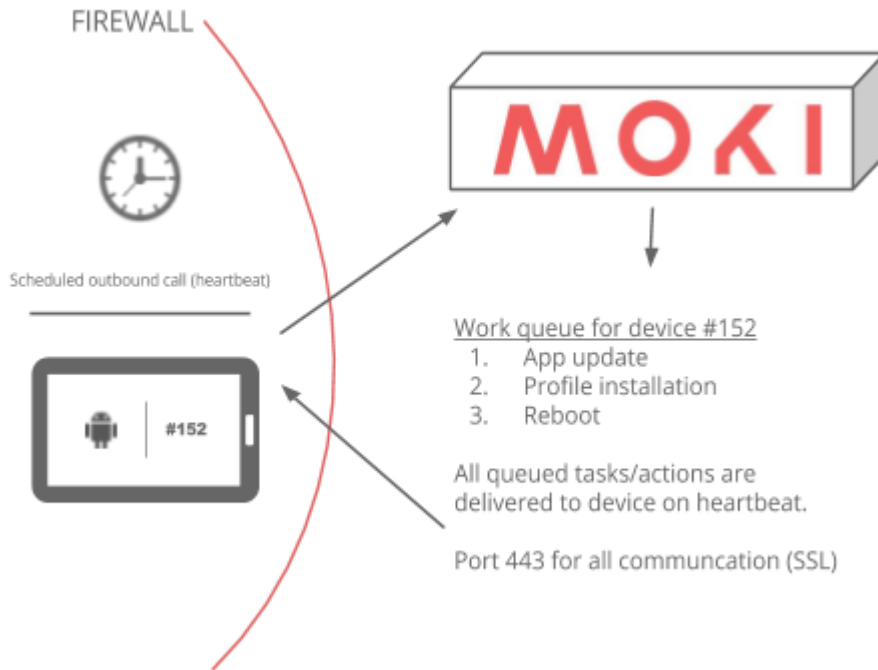
- **Created**: action is sitting in device queue
- **Scheduled**: action has been acknowledged by the device
- **Completed**: action has been completed by the device
- **Failed**: action failed to complete

| Actions ▼ | Profiles ▼ | Apps ▼ | 🗑 |

| Details | Custom Details | Advanced | Inventory | **Action History** | Events |

	↻ Refresh Data
Restart Android	Created 11/6 12:09 PM ▸
Restart Android	Created 11/6 11:07 AM ▸
Restart Android	Created 11/6 10:56 AM ▸
Query Extended Information	Completed 11/3 3:30 PM ▸
Query Extended Information	Scheduled 11/3 3:30 PM ▸
Query Extended Information	Completed 11/3 2:30 PM ▸
Query Extended Information	Completed 11/3 1:30 PM ▸
Query Extended Information	Completed 11/3 12:30 PM ▸
Query Extended Information	Completed 11/3 11:30 AM ▸
Query Extended Information	Completed 11/3 10:30 AM ▸
Query Profiles	Completed 11/3 9:43 AM ▸
Query Profiles	Scheduled 11/3 9:43 AM ▸

HOW MOKI WORKS

In many cases Moki's Android Agent is deployed on devices where the Google Cloud Messaging (GCM) service is not installed, the GCM inbound traffic is blocked at the firewall or the customer has requested that no inbound traffic be relied upon by the Moki systems. In these cases, the Moki Android Agent cannot be contacted proactively by Moki Control for management and monitoring activities.

The Moki Android Agent used in these scenarios runs in a 'GCM-less' model where all communication is done on a scheduled model. The Moki Android Agent is configured to call 'home' to Moki to check its work queue on a schedule. Once the Agent calls Moki Control for items in its work queue, it receives those items in the order they were given, executes each item in succession and reports back to Moki Control until all items in the work queue have been addressed.

FIREWALL

Scheduled outbound call (heartbeat)

#152

MOKI

Work queue for device #152
1. App update
2. Profile installation
3. Reboot

All queued tasks/actions are delivered to device on heartbeat.

Port 443 for all communcation (SSL)

This is an overview of the communication process for devices not using GCM:
1. An action is initiated in Moki Control and is added to an action queue for the device
2. The device heartbeats into Moki and Moki sends the first action in the queue for processing
3. The device reports back to the server with the status of the first action
4. Steps 2 and 3 repeat until all actions in the queue have been received and processed

NOTE: Some actions that take longer to process when they are received by the device will send a received status to the server. The device will then attempt to perform the action. Upon success or failure, a status update is sent to the server. The current status of any action can be viewed at any given time from Moki Control.

There is little to no difference between actions on devices with GCM, as opposed to those without. The chief difference is that when devices with GCM have a new action added to the queue, they will receive a push message telling the device to heartbeat and process the action. Devices without GCM must wait until the device heartbeats before they can access and process the action queue. When the device heartbeats it will get an action from the queue, as described above.

This is expected behavior. Moki does not communicate instantaneously with devices unless they have Google Cloud Messaging (GCM). As a way to overcome this, Moki uses what we call an "action queue". This means that admin users submit actions to a device and they are stored, in order, in the action queue. Enrolled devices have a heartbeat, which means on a regular schedule they check in with Moki to find out if there are tasks in their action queue. At each check-in, the device sends logs to Moki and picks up actions from its queue. It then responds to each action, one by one, in order until all actions are completed. By default, Moki Agent has a 15-minute interval heartbeat. This can be changed by setting up an Android Profile for "Check-in Interval". Check in interval is set in terms of minutes. The shortest time you can set is a 1-minute interval, which means every 1-minute the device checks in with Moki to get actions. Typically, in production, we don't recommend using a check in interval of less than 15-minutes. In cases where you are working with a device (or a merchant customer with a device) and you want to troubleshoot issues or send actions quickly, we have introduced the function of "support mode" which checks in nearly constantly for new actions for a 2-minute period of time. Such frequent checkins are ok for shorter, defined periods, but if all devices were always running in this mode it

would be very costly in terms of both data consumption and hosting costs. It is rare that actions sent require immediate processing and usually those actions can wait until the next heartbeat.

HISTORY AND RESETTING

This is how Moki is designed to work. The system assumes that if you factory reset a device or unenroll it that you are removing the device from the system. We do not hang on to action history or action queue. This prevents any confusion of past actions with a device that has been reset and possibly repurposed.

MOKI SYSTEM ADMINISTRATION

MOKI USER MANAGEMENT

Moki uses Google Authentication for authentication into the service. This means that all user accounts must be either Google Accounts or setup using a business owned account and integrated with Active Directory. If you choose to connect Moki with Active Directory, you can follow the instructions found in section USING ACTIVE DIRECTORY below.

ADDING USERS

This is a very simple process consisting of the following steps:

1. Click on your account links in the upper right hand corner of Moki Control and then select Users.
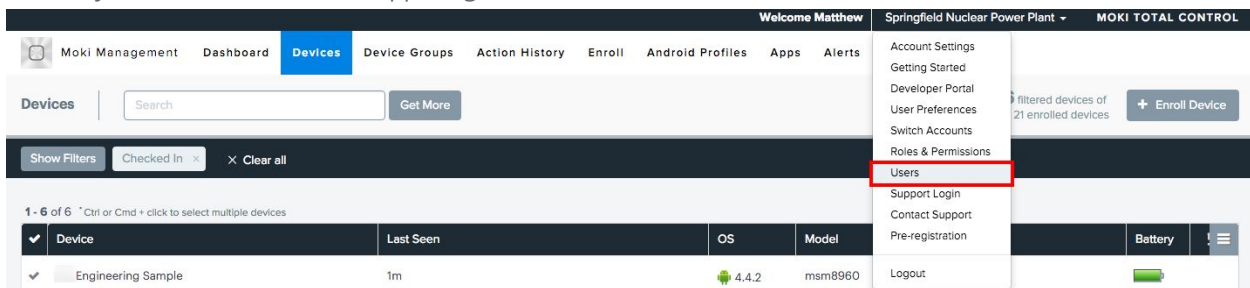
2. On the next page you can see the list of current users as well as users with pending invitations.
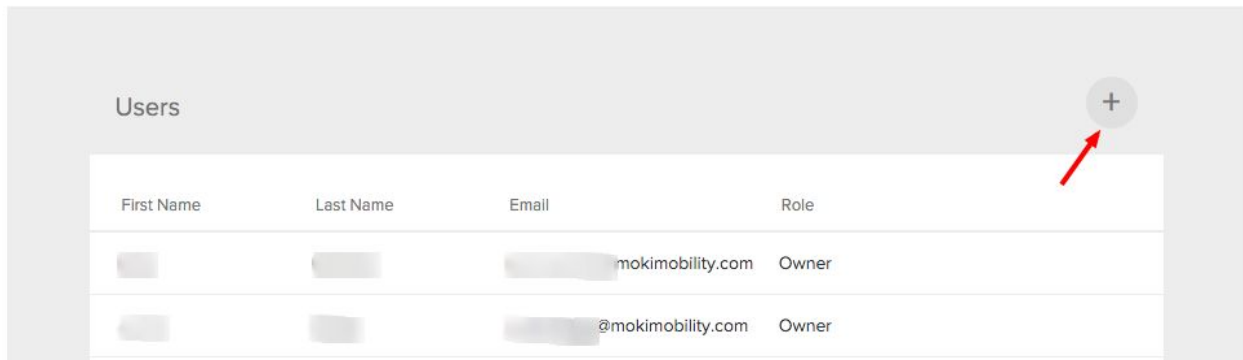
3. To create a new user, click on the plus button in the image above and fill out the form on the resulting page (see below):

4. Choose a user role from admin, standard, view only or any of your custom created roles.
5. Users will be activated once they have clicked on the link supplied in the invitation email.

MODIFYING USERS

If you need to modify or delete a user account do one of the following:

1. **Edit account:** Click on the pencil icon to bring up the user account editing interface, make needed changes, and save.
2. **Delete account:** Click on dust bin icon and confirm your choice.

USER ROLES

In Moki there are three different user roles by default. They are:

- **View Only**: This user has read-only access on the account. They can view device lists, apps, enrollment codes, etc., but are not able to issue commands or change settings on device.
- **Standard**: This user has all the privileges of the View Only type, as well as the ability to add devices, perform, update actions to apps and settings, and add new applications. This user has no delete

privileges.

- **Admin**: This user has full privileges for the account and can add and delete any items, perform all actions, and is also able to change account and device settings.
- **Custom roles:** Moki allows you to create roles to meet the custom needs of your organization. For instructions on how to do this go to XYZ.

APPLICATION MANAGEMENT

UPLOAD YOUR APP

If you are using MokiTouch 2, it is already in your account and you can skip to Step 4. If you are using another app, follow these steps.

1. In Moki Control, go to the Apps tab
2. Click the + icon on the left

3. Click the Android tab

4. Click the Upload Apk button and upload your APK file. Your file can't have any spaces in it, only dashes or periods
5. Select the options you need. If you upload an icon it will be displayed in Moki Control next to your app name

6. Click the Add App button and your app will be loaded into Moki Control for you to push to your device
7. If your app is on the Play Store and you don't have access to the APK, you'll need to install the app directly from the Play Store instead of through Moki Control

NOTE: Do not click on the "Install System App" option as this will soon be deprecated.

TAGS

If you want all your devices to come preconfigured with organizational Tags, follow the following steps. Otherwise, proceed to step 5.

1. Click the Tags tab in the top navigation
2. Click the + icon on the left side of the screen

3. Type in your tags and hit Enter (Tags can have spaces)

4. Click Save

ENROLLMENT CODE

Moki Control is intended to allow easy setup and management of your entire fleet of devices; therefore, we have created enrollment templates to allow maximum output from a minimal amount of steps.

1. Click on the Enroll tab in the top navigation
2. Click on the + icon and select Android
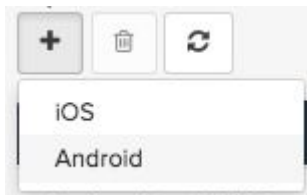
3. Give the enrollment a name to remember it later
4. Hit the Save button
5. Get the 7 character enrollment code or hit Done and your new template will show up in the list, along with the code

ANDROID PROFILES

Profiles provide a way to control certain settings and configurations on devices. There are different types of profiles that can be pushed to the devices. The following article will provide additional information on the types of profiles and the capabilities of each.

WI-FI

You can create a Wi-Fi profile to send to one or multiple devices. The profile will allow a device to connect to the Wi-Fi network specified in the profile, assuming the information for the network is accurate and up to date.

- **Profile Name**: Use your own desired naming practices for the profile name. Something easily identifiable will be beneficial if you plan on having multiple Wi-Fi profiles in your account
- **SSID**: The Service Set Identifier (SSID), commonly known as the network name, should be input here. Keep in mind that the SSID is case sensitive
- **Security Type**: Select either the WEP or the WPA/WPA2 security type from the list. If you are not sure, a quick Google search will help you learn how to identify which security type your network is running
- **Password**: Enter the network password here
- **Hidden**: If the network is setup as hidden, meaning the SSID is not broadcast, you will need to toggle this to Yes
- **Proxy Type**: Change this option from None if you connect to your network by proxy. If you select Automatic then you'll need to enter the proxy server URL that retrieves the proxy settings. If you select Manual then you'll need to enter the Hostname or IP address as well as the port and authentication required

After filling out the necessary information, click the Save button. The profile will be saved and can be pushed to devices from the Devices tab or via an action on the Actions tab.

DEVICE SETTINGS

- **Profile Name**: Use your own desired naming practices for the profile name. Something easily identifiable and specific regarding the devices you are targeting will be beneficial if you plan on having multiple profiles
- **Bluetooth**: Enable or disable the Bluetooth function on the device
- **Enable Screen Lock**: Enable or disable the device from Locking after inactivity or by the device being put to sleep via the power button or other method
- **Screen Sleep Timer**: Determine the time that the device must be inactive before sleeping. **NOTE**: This is not available on every device. It is recommended to test this feature before implementation
- **Disable Android Apps**: Allow/Disallow access and use of Android system apps including Google Docs, Photo Gallery, Google Quick Search, Google+, Google Talk, and Google Messaging
- **Enable Location Services**: Allows device to utilize GPS, Wi-Fi, and/or Cellular to log the location of the device. Enabling this can affect the battery life of the device. Be mindful that certain apps require use of Location services to function properly
- **Enable Android Email**: Allows device to utilize email services
- **Allow Apps from Unknown Sources**: Allows apps downloaded outside of the Google Play store to be installed on the device
- **Verify Apps**: Allows device to scan for potential threats from apps downloaded on the device
- **Volume Level**: Set the volume level of the device to desired level
- **Date Format**: Select from the three options for the date formatting on the device
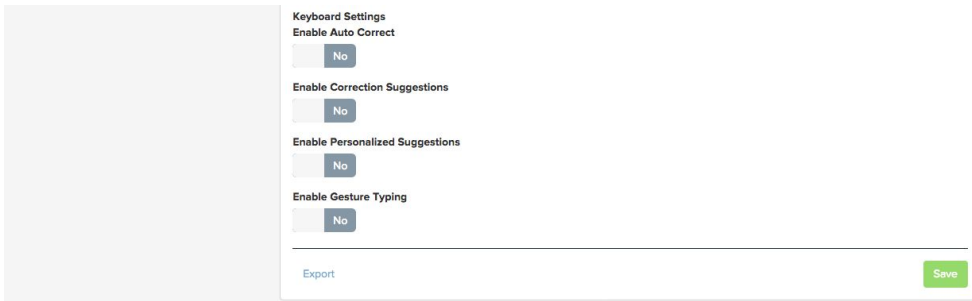
- Keyboard Settings
    - **Enable Auto Correct**: Allows device to auto correct inputs
    - **Enable Correction Suggestions**: Allows device to offer suggested corrections to input values
    - **Enable Personalized Suggestion**: Allows the device to analyze inputs over time and customize suggested words when typing
    - **Enable Gesture Typing**: Allows user to type via gesture/swiping on the keyboard

After configuring the device settings as desired, click the Save button. The profile will be saved and can be pushed to devices from the Devices tab or via an action on the Actions tab.

CHECK IN INTERVAL

- **Profile Name**: Use your own desired naming practices for the profile name. Something easily identifiable and specific regarding the devices you are targeting will be beneficial if you plan on having multiple profiles.
- **Heartbeat Interval**: Numerical values represented as minutes.

ISSUES UPDATING CUSTOM APPS

When a custom Application that you or your client has created fails to update, this could be due to a number of reasons. The first thing you should do is compare the old and the new VersionCode in the .apk files. This is not the same as the version number of the app. If the VersionCode has not been updated then Android will not replace the existing .apk.

Your app also has a key that acts as an identifier for the App. If a new version of the app has a different key but the same name, Android will not install it because of the conflicting key signatures. Make sure that both versions are signed with the same key signature.

One way to diagnose this is to look in the MokiMDM folder of your device's local file directory. If your new app file is in there, it means that Moki successfully pushed the app to the device but wasn't able to install it likely because of one of these two issues. The file name cannot contain any special characters outside of "_",', or "-".

DELETING DEVICES

Deleting a single device requires that you go to the Devices Tab, select your device, and verify that it is the correct device that you wish to delete. Select the trash button and the device will be removed from your Managed account. If you wish to recover your device, you will need to enroll it again.
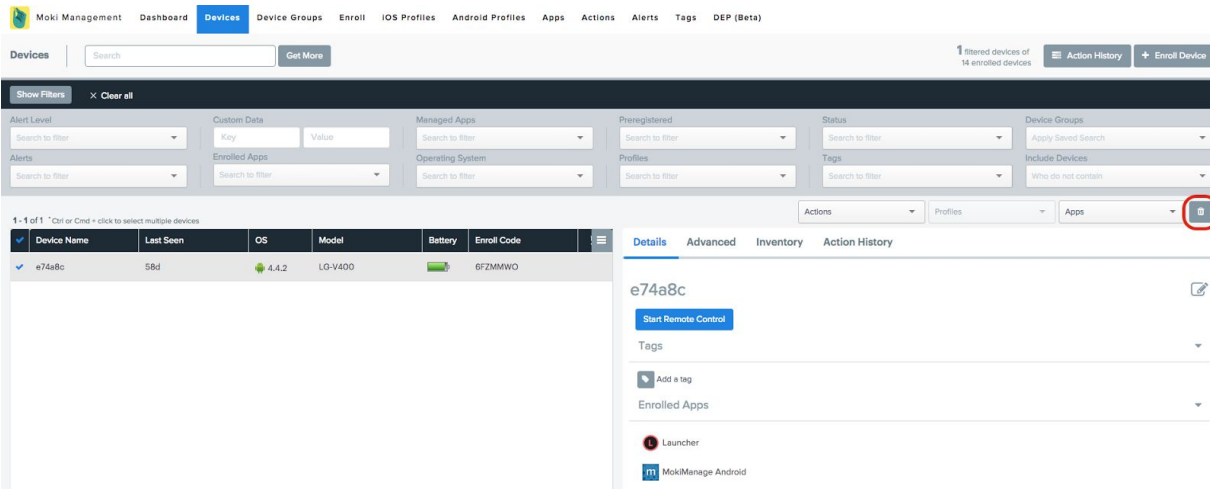
Deleting multiple devices from your account simply involves selecting more than one.
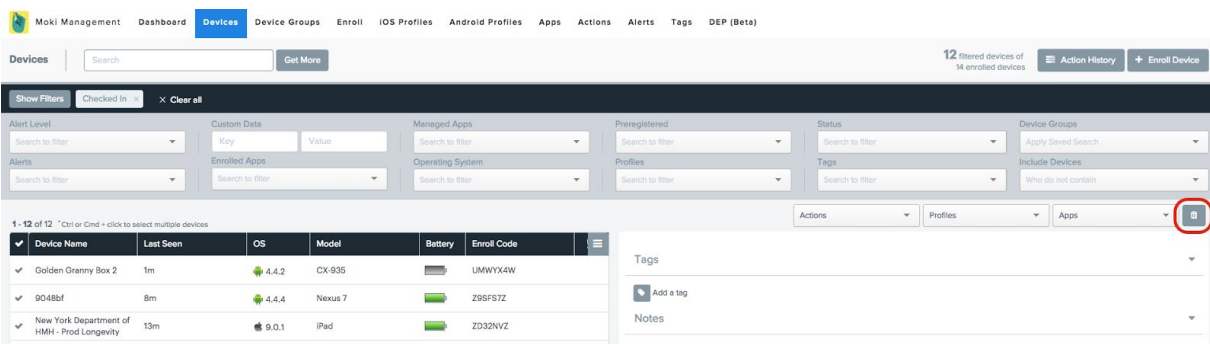
Deleting devices doesn't change the state of the device, it just takes it out of Moki. If your device is locked down, make sure to unlock it before removing it from Moki.

MOKI AGENT

Moki Agent is installed on the device at the Factory level. Thus, all devices are shipped with Moki Agent already on them. Moki Agent handles the enrollment of Moki enabled apps and devices into the Moki administrator portal. Enrollment means that the device and its Moki enabled apps (apps with the Moki SDK integrated into them) show up in the Moki administrator portal where Admins can control the device.

As explained earlier, many aspects of the device can be controlled - such as app updates, app settings updates, and a host of other things relative to managing devices. However, these actions can only be applied to devices that are enrolled, or Checked-In. A device can become unenrolled, or Checked-Out, if either Moki Agent has been deleted from the device or if someone factory resets from the device. If a user removes enrollment using Moki Agent it should not show as Checked-Out. Likewise, if the device is either deleted or factory reset from Moki it will not show as Checked-Out but will just be gone from the system. There is a filter for Checked-Out devices so that Admins can review these devices, determine what has happened to cause this change, and enroll the device again, if necessary, or delete the device from the account.

ADDING APPS

Manager allows you to upload apps so you can send them to devices at any time. Android apps only have the

option to upload the .apk file because Google doesn't have APIs that allow MDM providers to connect to the app on the Play Store.
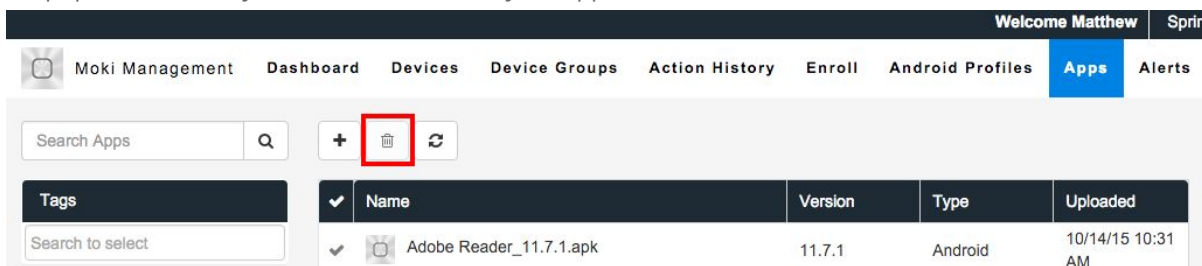
UPLOADING APPS
1. Select the Apps tab in the top navigation
2. Click the + icon on the left
3. Click the Android tab
4. Click the Upload APK button and upload your APK file.
5. Click the Add App button and your app will be loaded into Manager for you to push to your device
6. If your app is on the Play Store and you don't have access to the APK then you'll need to install the app directly from the Play Store instead of through Manager

SENDING APPS TO A DEVICE
1. Go to the Devices tab
2. Select your device(s)
3. Click the Apps drop down and select your app
4. Confirm you want to send it to the device
5. If installing an iTunes app, you'll need to follow the prompts on the device. Android users should be good. If the app doesn't install, here is an article on troubleshooting android app installation

DELETING APPS

To remove unwanted or unneeded Apps from your account, go to the Apps tab. From there, your list of Apps will populate. You may select one or more of your apps and then select the trash can button.

ENROLLED APPS

An enrolled app is a mobile application that has been developed to incorporate the Moki SDK for advanced remote management functionality. When installed on your device, enrolled apps will appear with a link to manage your application settings (as below) with the "Manage Settings" button to the right. Once you have settings applied for one device, you can then create a settings template that can be applied to your other devices - either directly on one or via a scheduled action.
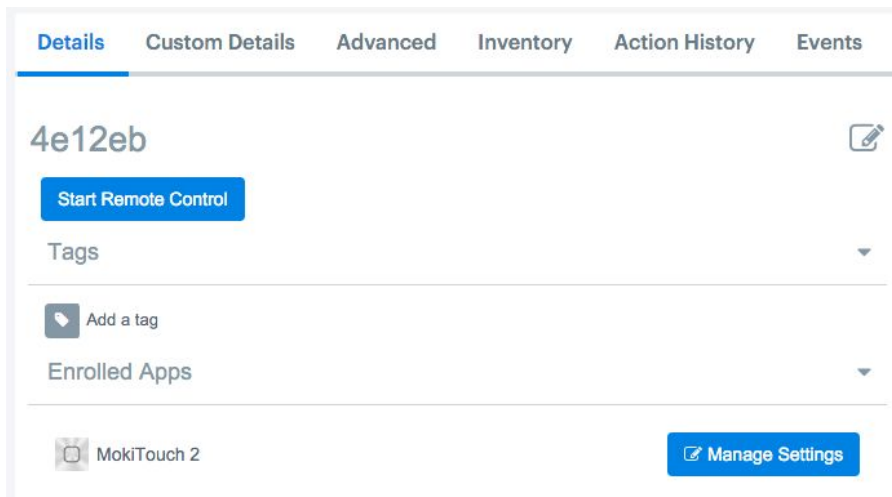
POST ENROLLMENT ACTIVITIES

STEPS TO UNENROLL PROPERLY

If you have the need to reset an Android device, for either testing or repurposing a device, there are two possible ways to accomplish this. Which method you choose depends on the state of your device and its connection to Moki at the time of performing the reset.

- If your Android device is communicating with Moki and is responding to commands, it is best to perform a factory reset through Moki. The reason for this is that Moki will also reset its relationship to that device ensuring that it will get apps pushed properly when it enrolls again. To do this:
    1. Go to the device list
    2. Find and select the device with which you are working
    3. Go to the Actions menu and select 'Factory Reset'
    4. You will be asked a basic maths question which needs to be answered before you can send the reset command. This helps prevent accidental resets
    5. After the device has received the reset command and is processing it, you may delete the device from your device list by selecting it and clicking on the trash can icon next to the action bar
- If your device has lost communication with Moki, follow these steps:
    1. Open Moki Agent on your device
    2. Click on the ". . ." menu in the bottom right corner
    3. Select "Remove Device Enrollment" and then exit Moki Agent
    4. Open device settings
    5. Go to "Backup & reset"
    6. Click on "Factory data reset"
    7. Click on "Reset tablet"
    8. Go to Moki Control and click the Device list
    9. Find the device from that list
   10. Select the device and delete the device

RE-ENROLLING

You may have a need to move a device from one account to another without factory resetting the device. In this case you have two options available to you. The first, and definitely the easiest method, is to use Moki's "Re-enroll" action. The second method is to do it all at the device level.
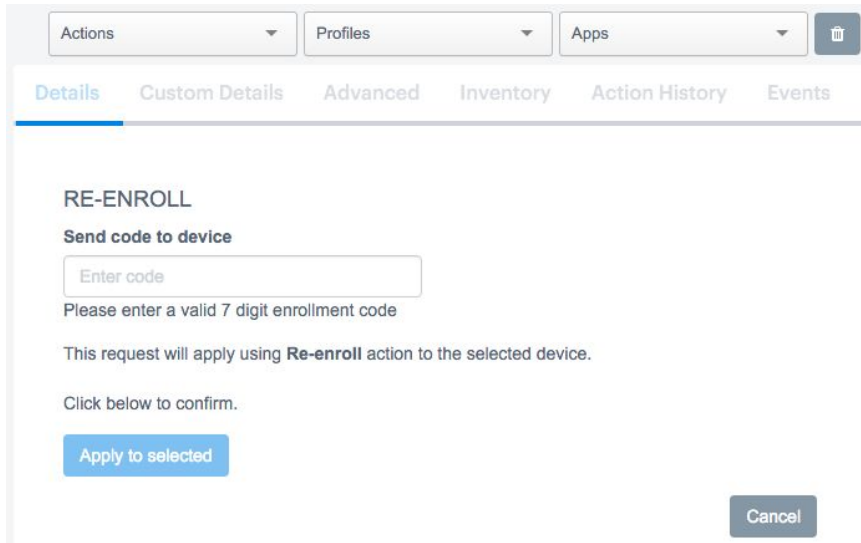
- Using Re-enroll action
    1. Via device list

i. Select your device in the device list
ii. Select "Re-enroll" from the action menu
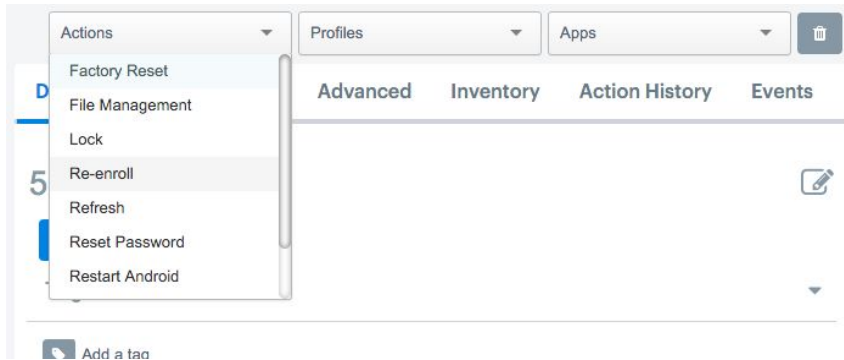
iii. In the text input enter a valid enrollment code for your account and click "Apply to selected"

iv. The device will receive the command at next heartbeat and will move itself to the new account along with any enrolled applications using the SDK.
v. **NOTE**: If there are additional apps applied to the new enrollment code, they will be installed on the device upon re-enrollment and all existing apps will stay installed on the device.
2. If you have more than a few devices to you will want to do this via device groups scheduled action
i. Go to Device Groups and either create a new group for your needs or use an existing group
ii. Click on "Create Action Sequence"
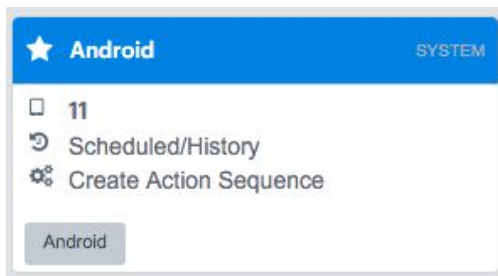
iii. Create a new sequence with a "Re-enrollment" action containing a proper enrollment

code
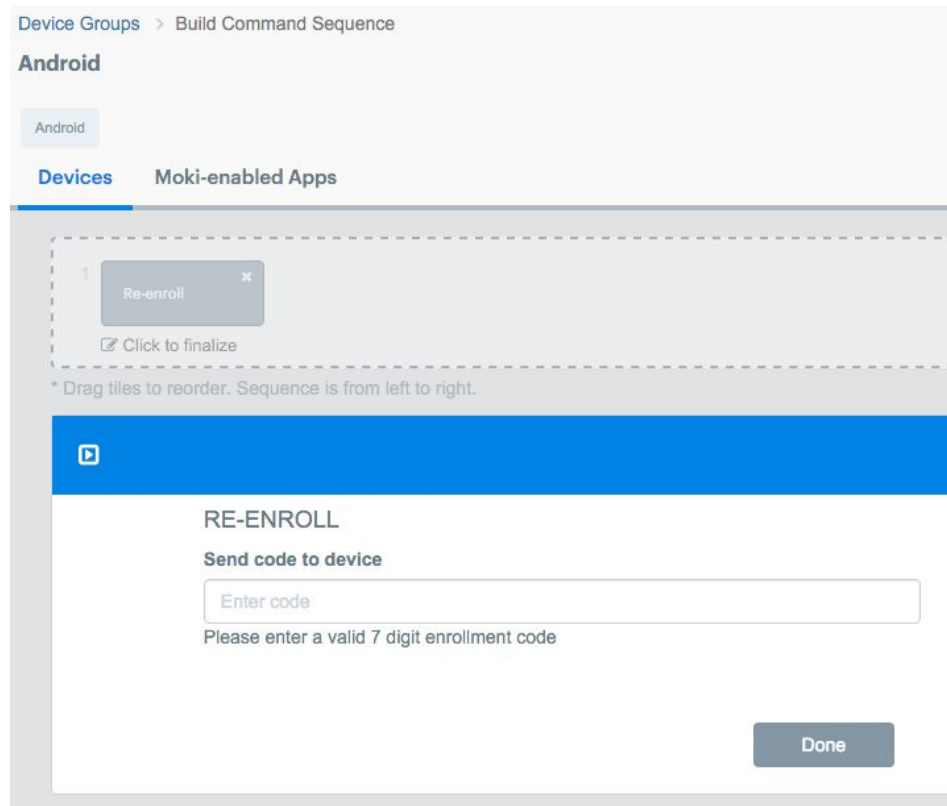
iv. Schedule your action and if you have 2-person authorization enabled, be sure to have your sequence approved

v. The devices will be enrolled to the new code upon next heartbeat

- Re-enrolling using device
    1. On your device open Moki Agent
    2. Click on the ". . ." menu
    3. Click on "Remove Device Enrollment"
    4. On the next screen enter the valid enrollment code for your new enrollment and submit that form
    5. Your device will enroll to the new account

ADVANCED MOKI

ROLES AND PERMISSIONS

Moki Control allows you to assign user roles with associated permissions to your users. As mentioned in the [Moki User Management](#) section there are three system level user roles: View Only, Standard, and Admin. These each come with their own set of unique permissions. In some cases customers may have need to create more specific roles and permissions variation to accommodate their needs.

There are a multitude of configuration options for your Moki user roles. To access the "Roles and Permissions" working area, click on the account settings menu in the upper right corner and click on the link for "Roles and Permissions".
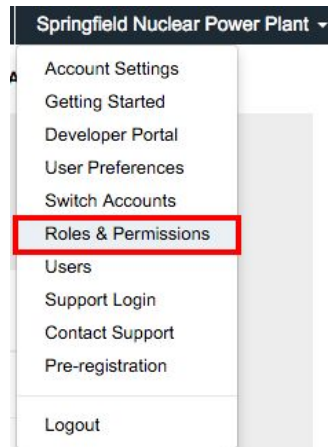
You will see the list of system roles that come standard for all Moki accounts. These system roles cannot be edited but can be duplicated if needed. Click on the role title to see the role capabilities. To create a new role, you can either duplicate and alter an system role or click the + button to open up the role creator interface.

As mentioned your roles are highly configurable. The configuration interface allows you to set a role name and then you can select permissions in any of these main functional groupings by selecting or deselecting the check marks next to them:
- **Account Administration**: limit access to account settings
- **Alerts:** Create, edit, delete
- **Android Profiles:** Create, edit, delete
- **Apps:** Create, edit, delete
- **Device Groups:** Create, edit, delete

- **Enrollments:** Create, edit, delete, enroll
- **Tags:** Create, edit, delete
- **Designated Groups:** Determine which device groups users can manage
- **Schedule Action Sequences:** Enables user to request selected scheduled actions
- **Approve Action Sequences:** Enables users to approve requested scheduled actions
- **Single Device:** Enables interactions with individual devices
- **Multiple Devices:** Enables limited interactions with bulk selected devices

Once you have created your necessary roles you can apply them to your users.

TWO-PERSON AUTHORIZATION

Moki has a highly configurable authorization system. This includes the ability to create custom roles as well as define which actions within Moki require a second person to authorize them. To enable advanced user roles and two-person authorization, go to "Account Settings" for your account and then scroll to the bottom of the settings tab to enable "Action Authorization".

APPROVAL QUEUE

If users are approvers, they will be notified of any actions requiring approval. This queue of pending actions can be seen in two locations in Moki: the dashboard and the action history tabs.

In cases when a requested action is "PENDING" (see above), approver users will be notified of the need to review the action. If approval is not received before the scheduled time, the scheduled action goes into a "LAPSED" state and requires the action to be rescheduled.

DEVICE PRE-REGISTRATION

For customers working with ODMs for custom device builds or where they are purchasing large lots of devices we have a simplified enrollment process we call pre-registration. Pre-registration allows Moki customers to upload a CSV file with 2 columns:

- Device serial number or wifi mac address
- Enrollment code

Most device manufacturers are able to provide an electronic file list of the serial number or wifi mac address to their customers. Moki customers can use this list as the basis of their pre-registration file, by creating a new file with the serial or mac address then they add the enrollment code they wish to use for each device. Typically this is the same enrollment code for all devices, but not necessarily so. Once you have the file prepared, go to the account management menu in the upper right corner and select "Pre-Registration".
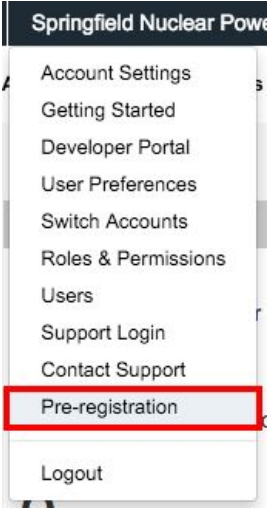
On the page you will see a button to "Import Pre-Registration". When clicked you will be presented with a file upload interface.
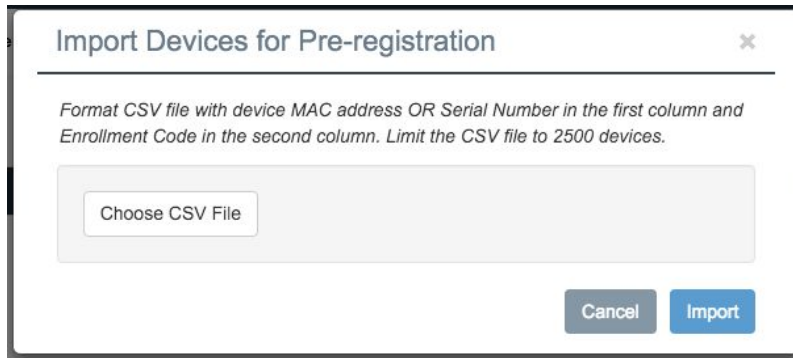
Once your list is uploaded you will see them in the Pre-Registration page. All that is now needed to enroll these devices to Moki is to:

1. Power the device on
2. Connect to a network
3. Ensure Moki Agent (3.6 or greater) is installed
4. Open Agent

HOW IT WORKS

Once you have completed the , you can open Moki and enroll the device without the need to enter an enrollment code. All Moki Agent version 3.6 or higher will automatically call home to Moki when first opened. If Moki has the serial number or wifi mac address stored as a pre-registered device, it will enroll to the account/code added in the upload file. Once that is underway, all of the expected software, profiles, and tags will be installed to the device without any further interaction from the user.

DEVICE LIST EXPORT

Moki gives users the ability to download the list of enrolled devices. Users can request a link to be sent via email that contains a link to a CSV file for downloading.
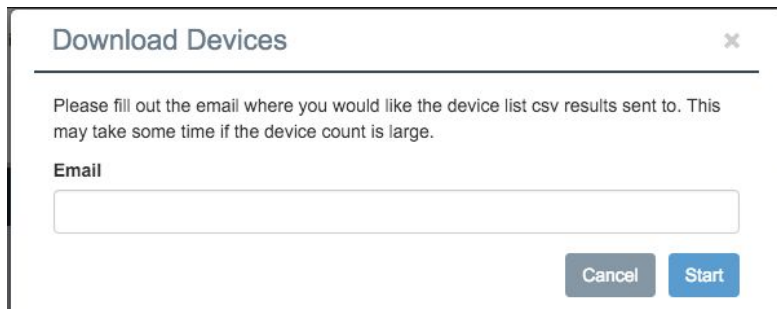
EMAIL LINK TO LIST

1. Go to the device list
2. Click on menu icon in upper right corner of the list
3. Click on "Download Device List"
4. Enter your email in the input box
5. Get email with link to CSV file
6. Click on link to CSV file and save
7. Open CSV file and confirm your device list

DEEP LINKED FILTERING

Moki provides the ability to create links using query string parameters to quickly filter devices based on custom

data. Here is an example URL for :

```
https://<environment url>/aem?tenantid=<tenant
ID>#/layout/mdm/devices?custom=true&<custom key>=<value>
```

There are 3 variable elements of the URL:
1. `<environment url>` will be the domain name for your target environment
2. `<tenant ID>` is the account identifier for your devices
    ○ This is important if you will be going between accounts
3. `<custom key>=<value>` is the name and value pair for the custom data on which you wish to filter
    ○ To find the correct format of your custom variable key, simply select it in the filter in the UI and the actual key will be displayed in the light grey filter box above. Use that for your custom key
4. **Note**: it is required to have the `custom=true` parameter somewhere in the query string

DEVELOPER RESOURCES

MOKI APIs

Moki has a developer portal where customers can access our system APIs. Visit https://moki-api.3scale.net/docs to request an account and for complete documentation of available APIs. There is also a test interface built in so you can test parameters and get results to ensure your code is sound.

GOOGLE APIs

For instructions accessing Google App Engine APIs, visit https://cloud.google.com/appengine/docs. This will tell you what you need to know to access Google backend data and information.

MOKI SDK

Moki provides a Java SDK for developers to make them work seamlessly with Moki's leading management tools for remote settings updates, alerts, custom data, and analytics. For documentation and downloads go to http://mokimobility.github.io/v2/.

APPENDIX A

GLOSSARY OF TERMS

Account: Moki is what is referred to as a multitenant app. Your account equates to a single tenant in the environment.

Agent: The software client from Moki, called Moki Agent, allows Android devices to connect to Moki and communicate by receiving commands and sending logs and other communication.

Checked-In: The device is enrolled and available to receive commands if network connections are live.

Checked-Out: The device has had enrollment removed. This is likely to be a factory reset from the device or deletion of Moki Agent. If the user removes enrollment, it should not show as Checked-Out. Likewise, if the device is deleted or factory reset from Moki it will not show as Checked-Out but will just be gone from the system.

Device Group: A collection of devices meant to ease management operations. Moki has two types of device groups: dynamic and static. Dynamic device groups can be grouped based on many different criteria, and membership to the group depends on the device current state. Static groups can be any random collection of devices, and group membership never changes unless the group is edited. Device groups are where managers create and schedule action sequences for managing more than one device simultaneously.

Enrollment Template: A defined set of instructions for devices that are enrolled. Instructions can include installation of applications and profiles as well as adding tags to the device. Moki assigns an "enrollment code" to each enrollment template. That code can be input into Moki Agent to enroll into an account. Once Agent is enrolled, all other apps containing the latest SDK will also auto-enroll.

Filters: Controls found on the device list page as well as on device groups that allow a manager within Moki to show devices that contain the same characteristics such as operating system, tags, status, managed apps, etc.

Heartbeat: This is the defined interval that a device communicates with Moki Control and sends back logs and collects actions. By default, Moki Agent heartbeats every 15 minutes. The heartbeat interval can be set via Android Profile. Moki recommends setting devices to a 60 minute heartbeat when devices are in production and strongly discourages setting heartbeat below 15 minutes.

Impression: Analytics event when someone looks at the screen but doesn't linger longer than 2 seconds.

Interaction: Analytics event when someone touches the screen to interact.

Queue: Each device registered within Moki has a queue endpoint. The queue contains all instructions that are sent by administrators using Moki Control to devices. These instructions can be actions, application installations or deletions, profile installations or deletions, or remote control session requests. If the device communicates directly with Moki using GCM then the queue clears itself almost instantaneously. If the device is GCM-less, the actions from the queue are picked up at the next heartbeat. It is critical to understand how actions are queued when managing GCM-less devices.

Push: The action of sending an "action" to a device.

Silent Enrollment: This is a version of Moki Agent that comes with a pre-programmed enrollment code. Moki Agent enrolls automatically as soon as it is opened.

Session: The singular analytics event of a single person interacting with the device. A session begins at the first point of interaction and is completed upon 30 seconds after inactivity.

Standard Enrollment: This is a version of Moki Agent that doesn't come with an attached enrollment code and allows administrators to choose which enrollment code is to be used and entered into the enrollment input.

Support Mode: This feature of Moki Agent is helpful in GCM-less deployments when a device needs support and more real-time communication. A device user must start support mode within Moki Agent, which begins a series of rapid heartbeats for a short burst of time. This allows logs and commands to be sent more frequently.

Support User: A special Moki user type that is granted access to all accounts in an environment.

Tag: A management feature of Moki Control that allows you to apply text labels to devices, which can be used for device list filtering and building device groups.

View: Analytics event when someone looks at the screen longer than 2 seconds.

ACRONYMS

AD: Active Directory
AEM: Application Environment Management
APN: Access Point Name
ASM: Application Settings Management
CSV: Comma Separated Values
GCM: Google Cloud Messaging. Google's messaging service layer, which is part of Google Play's services, that allows Moki to actively communicate to devices
GCM-less: A device that that doesn't utilize GCM. These devices can only accept actions when they heartbeat
MDM: Mobile Device Management
ODM: Original Device Manufacturers
OS: Operating System
VPN: Virtual Private Network

CHANGE HISTORY

Version	Date	Change Description
1.5	09 Nov 2017	*Updates:* Device group scheduled action details
1.4	22 Mar 2017	*Updates:* Corrected outdated references.
1.3	03 Mar 2016	*Updates:* Corrected link to Moki API and Moki SDK documentation.
1.2	10 Feb 2016	*New sections*: Introduction, Switching Between Accounts, Creating Support Users, Roles and Permissions, Device Preregistration, Filters *Updated sections*: Google Auth Adding Users, Active Directory Adding Users, Two-Person Authorization, Events *Other changes*: added browser support statement, slight modifications to "Logging In" section, device list export changes, updated link to API portal, removed references to Moki Total Control to Moki Control for branding consistency, added term to glossary, modified some wording in glossary definitions.
1.1	7 Jan 2016	Moved section "How Moki Works" from the beginning of the document to the end of the first main section.