CounterACT® MobileIron Plugin
Configuration Guide
Version 1.7.1
# Table of Contents

**About MobileIron Integration** ................................................................. 4

**Additional MobileIron Documentation** ................................................. 4

**About this Plugin** ................................................................................ 4
- How it Works ......................................................................................... 5
- Continuous Query Refresh .................................................................. 5
- Offsite Device Management ................................................................. 6
- Supported Network Infrastructures ..................................................... 6
- What to Do ......................................................................................... 6

**Requirements** ................................................................................... 6
- CounterACT Software Requirements .................................................... 7
- ForeScout Module License Requirements ............................................. 7
  - Requesting a License ...................................................................... 7
  - More License Information .............................................................. 8
- MobileIron Requirements ................................................................... 8
- Networking Requirements ................................................................. 8
- Endpoint Requirements ..................................................................... 8
- Supported Devices ............................................................................. 8
- Additional Deployment Recommendations ...................................... 9

**MDM Web Service Verification** ............................................................. 9

**Define a CounterACT User at the MobileIron Admin Portal** ................ 10

**Install the Plugin** ............................................................................... 10

**Configure and Test the Plugin** ............................................................ 11
- Configure the Plugin .......................................................................... 11
- Test Plugin Communication with the MobileIron Service .................. 13

**Run MobileIron Policy Templates** ....................................................... 13
- MobileIron Enrollment Policy Template ......................................... 14
  - Prerequisites ................................................................................ 14
- Multiple MDM Service Enrollment ............................................... 15
- Running the Template ..................................................................... 15
- Which Endpoints are Inspected - Policy Scope .............................. 17
- How Devices are Detected and Handled ......................................... 18
- MDM Classification Policy Template .............................................. 19
  - Prerequisites ............................................................................... 19
- Which Endpoints are Inspected - Policy Scope .............................. 20
- How Devices are Detected and Handled ......................................... 20
- MobileIron Device Compliance Policy Template ........................... 22
Prerequisites .................................................................................................................. 22
Running the Template .................................................................................................... 22
Which Endpoints are Inspected - Policy Scope ................................................................. 25
How Devices are Detected and Handled ........................................................................... 26
Adding Applications to the Unauthorized Application List ........................................... 28
Configuring Virtual Firewall Actions ............................................................................. 29

Mobile Device Enrollment ............................................................................................ 30

Display Inventory Data ................................................................................................. 33

Managing Offsite Devices .............................................................................................. 34

Create Custom MobileIron Policies .............................................................................. 34
  Detecting MobileIron Devices - Policy Properties ......................................................... 35
  MobileIron .................................................................................................................... 35
  MobileIron Apps .......................................................................................................... 35
  MobileIron Details ....................................................................................................... 36
  MobileIron Label Membership .................................................................................... 36
  MobileIron Policies ..................................................................................................... 37
  Asset Classification ..................................................................................................... 37
  Controlling MobileIron Devices - Policy Actions .......................................................... 37
  MobileIron Apply to Label ............................................................................................ 37
  MobileIron Force Device Check-In ............................................................................... 38
  MobileIron Remove From Label .................................................................................. 38
  MobileIron Wipe .......................................................................................................... 38

Additional CounterACT Documentation ........................................................................ 39
  Documentation Portal .................................................................................................. 39
  Customer Support Portal ............................................................................................... 39
  CounterACT Console Online Help Tools ....................................................................... 39
About MobileIron Integration

CounterACT/MobileIron integration helps IT administrators streamline the process to provision, manage and secure today’s expanding suite of smartphones and tablets, all from a single portal. CounterACT/MobileIron integration yields an easy to use platform that includes all of the essential functionality for end-to-end management of mobile devices. You can secure and manage apps, docs, and devices for global organizations, and support both corporate and individual owned devices.

MobileIron is available as both an on premise system and a cloud service. This means with a single unified security management and reporting system, you can ensure that your network is secured, regardless of the type of device a user may be carrying.

Instead of implementing new security silos that are limited to mobile devices, you can extend your PC and network security systems to encompass mobile devices.

CounterACT integration with MDM services provides a whole new level of centralized visibility and control for actionable insights into your entire computing landscape.

- **Secure all Mobile Devices**: supports iOS and Android smartphone and tablet platforms - in both Exchange and Lotus Notes environments.
- **Manage Devices Outside the Corporate Network**: leverage integration with MDM services to manage devices even when they are not in the corporate network.
- **Embrace BYOD**: provides workflows to discover, enroll, manage and report on personally owned devices, in addition to corporate devices, as part of your mobile device operations.
- **Experience simple device enrollment and approval**: provides auto-quarantine for Exchange, and alerts IT personnel to approve all new devices. Additionally it provides for easy user self-enrollment via web, email or SMS.

Additional MobileIron Documentation

Refer to the documents linked from the following file for more technical information about the MobileIron solution:

https://www.mobileiron.com/en/resources/datasheets

About this Plugin

Integration with CounterACT lets you deliver a comprehensive solution that provides powerful monitoring and enforcement capabilities not available when working solely with the MobileIron solution. Use this plugin to complete the cycle of security by obtaining valuable capabilities:

- Automated real-time, continuous detection and compliance of mobile devices the moment they try to connect to your network, including unmanaged and unknown devices.
Policy-based unified NAC enforcement limits network access based on device type, device ownership, time of day, and policy compliance.
- Allow compliant and managed devices to join the network.
- Limit network access to a subset of applications and data, blocking access to more sensitive corporate resources.
- Block noncompliant devices or specific types of devices from your network.
- Tag devices at the MobileIron console, based on CounterACT detections.
- Enhance the CounterACT inventory by populating it with MobileIron Core information.

How it Works
The MobileIron MDM plugin queries the MobileIron Core Service for host device attributes, for example core attributes, security and compliance information, hardware inventory and network information. All MobileIron queries are performed by a single CounterACT Appliance that is designated for this purpose. This designated CounterACT device, the Connecting CounterACT Device, retrieves information from other CounterACT Appliances and the CounterACT Enterprise Manager and forwards the information to the MobileIron Core Service. Similarly, the Connecting CounterACT Device retrieves information from the MobileIron service and forwards it to other CounterACT Appliances and the CounterACT Enterprise Manager.

Continuous Query Refresh
MobileIron query mechanisms recheck endpoint attributes at a static frequency—approximately once a day. However, after plugin installation, querying of endpoint properties is based on CounterACT policy recheck definitions that define the conditions under which to recheck hosts that match a policy. Specifically, you can specify:
How often hosts are rechecked once they match a policy
Under what conditions to carry out the recheck

This ensures continuous, real-time endpoint evaluation that can be customized for each CounterACT policy.

Queries for device core attributes are initiated on the basis of the endpoint MAC address. Core attribute results return the device ID, which is used for further queries. As such, the plugin must learn endpoint MAC addresses in order to initiate the query process.

**Offsite Device Management**

The plugin leverages integration with MobileIron to manage devices even when they are not in the corporate network. The plugin retrieves updated host information for offsite devices through the MobileIron service platform. Offsite endpoints are identified and managed based on their MAC addresses.

For more information, see [Managing Offsite Devices](#).

**Supported Network Infrastructures**

- Devices connected to the network via a Wi-Fi connection
- MDM integration can be carried out with an on-premise MDM service or an MDM service in the cloud

**What to Do**

This section describes steps you should take to set up your system when integrating with the MobileIron:

1. Verify that you have met system requirements. See [Requirements](#).
2. [Define a CounterACT User at the MobileIron Admin Portal](#)
3. [Install the Plugin](#)
4. [Configure and Test the Plugin](#)
5. [Run MobileIron Policy Templates](#)

**Requirements**

This section describes system requirements and recommendations.

- [CounterACT Software Requirements](#)
- [ForeScout Module License Requirements](#)
- [MobileIron Requirements](#)
- [Networking Requirements](#)
- [Endpoint Requirements](#)
CounterACT® MobileIron Plugin Configuration Guide

Additional Deployment Recommendations

CounterACT Software Requirements

The following CounterACT releases can work with this plugin.

- CounterACT version 7.0.0
- Service Pack 2.3.1 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- A module license for either the MDM Integration Module or the MobileIron Module. See ForeScout Module License Requirements for details.
- An active Maintenance Contract for the module.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin you are provided with a 90-day demo module license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license.*

Demo license extension requests and permanent license requests are made from the CounterACT Console.

*This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the CounterACT Console User Manual for more information.*

Requesting a License

When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices you want the license to support. Licenses for this module are based on the number of mobile devices managed by CounterACT via the MDM service.

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.
More License Information
See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

MobileIron Requirements
This plugin supports MobileIron Core version 9.0, 9.1, 9.3, and 9.5 (on premise or Connected Cloud).

Networking Requirements
The following ports must be open on enterprise firewalls to support communication between CounterACT and the MobileIron service.
- 43261/TCP or the port used to communicate with the MobileIron web service.
- The port used to communicate with a proxy server, if one is used.
Specify these ports when you configure the plugin. See Configure and Test the Plugin.
- 443/TCP
In addition, define exceptions to the Virtual Firewall action for these ports. See Configuring Virtual Firewall Actions.

Endpoint Requirements
Queries to MDM services are based on endpoint MAC addresses. As such, CounterACT must learn endpoint MAC addresses in order to initiate the query process. MAC addresses can be learned from the following sources:
- Wireless plugin (Client table)
- Packet-Engine (ARP and DHCP traffic)
- L3 switches (ARP table)

Supported Devices
The following devices are supported by the MobileIron MDM Plugin. Vendor-supported OS versions are also supported by this plugin:
- iOS
- Android

For OS version support of the MobileIron service, refer to MobileIron documentation: http://www.mobileiron.com/en/resources/resources-overview/datasheets
Additional Deployment Recommendations

- Run the DHCP Classify Plugin (recommended to accelerate asset classification).
- Verify that HTTP Redirect actions, for example the *HTTP Notification* action, are working in your environment. Refer to the CounterACT Console online help for information about working with HTTP actions.

MDM Web Service Verification

This section describes how to verify that the Web Service is properly set up. To verify setup, test REST API calls on the MobileIron Server by verifying that the MobileIron console supports Web services.

1. Install the Firefox *RESTClient* plugin from the following URL:

2. Launch the *RESTClient* plugin by selecting **Tools -> RESTClient**.

3. In the REST client user interface, do the following:
   - Enter the URL of the REST API on the MobileIron server, as follows: https://<server name>/api/v1/dm/devices. Provide the same MobileIron server name that will be defined in Configure the Plugin.
   - Define the HTTP header Authorization (basic). Provide the same username and password that will be defined in Configure the Plugin.
   - Define the HTTP header Accept, as follows: application/xml.

4. Select **Send**.

   The REST client user interface displays the returned *Response* body; this information is provided in XML format.
Define a CounterACT User at the MobileIron Admin Portal

CounterACT logs in to the MobileIron Core Service as this user. The CounterACT user information is required during the plugin configuration.

To define a CounterACT user in the MobileIron Admin portal:
1. Define a user account for CounterACT in the MobileIron Admin administration portal.
2. Select Admin.
3. Select the CounterACT user, and then select Edit Roles.
4. In the Device Management area, select the following roles:
   - View dashboard, device page, device details
   - Manage devices
   - Wipe device
   - Add device
   - Manage device enrollment (iOS only)
5. In the Other Roles area, select the following roles:
   - Connector
   - API

Record user account settings. You will use them later in CounterACT configuration screens.

Install the Plugin

This section describes how to install the plugin.

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:
1. Navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log in to the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.

9. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.

10. Once the installation is complete, select Close. The plugin is listed in the Plugins pane. The Module Status column indicates the time remaining for the demo license. See ForeScout Module License Requirements or the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension.

11. Select Start to start the plugin. The Select Appliances dialog appears.

12. Select CounterACT Appliances on which the plugin should be started. The plugin must be running on every Appliance that may manage enrolled mobile devices. It is recommended to run the plugin on all Appliances in the environment.

13. Select OK. The plugin runs on the selected Appliances.

Once installed, the plugin automatically adds a HTTP Redirect exception to the CounterACT NAC Redirect Exception list. CounterACT NAC HTTP redirect exceptions are designed to ensure users can access business essential Internet sites or important files on the Internet while allowing required HTTP blocking and redirection. This exception ensures that devices can enroll with the MobileIron Core Service and still receive required HTTP notifications.

## Configure and Test the Plugin

This section describes how to configure and test the plugin.

### Configure the Plugin

The plugin is configured to communicate with the MobileIron Web Service.

**To configure the plugin:**

1. In the CounterACT Console, select Options from the Tools menu.
2. Select Plugins.
3. Select MobileIron MDM from the Options pane, and then select Configure.
4. Enter the following information about the MobileIron Web Service.
   - Username
   - Password
− **MobileIron Server Name** Verify that the MDM server is accessible to the CounterACT Appliance. To specify a port for communication with the server, use the format: 
<server_name>:<port>
For example:
de.mobileiron.net:8843

The Username is the user account defined on the MobileIron Administration Portal.

− In the **Connecting CounterACT Device** drop-down list, select the name of an Appliance that will serve as a proxy between the MobileIron service and other CounterACT devices. The CounterACT device listed here is the only device that will communicate directly with the MobileIron Core Service.

5. Select the Advanced tab.
   − In the **MDM Query Threshold Interval (Seconds)** field, specify the frequency that the plugin should query the MobileIron Core Service.
   − In the **MDM Query Threshold** field, define the maximum number of query requests to the MobileIron Core Service per threshold interval (defined in the preceding field).
   − Select **Use a Proxy Server** if there is a proxy between the Connecting CounterACT Device and the MobileIron Core Service. Enter the IP address of the proxy server in the **DNS Name or IP Address of the Proxy Server** field. Enter the required proxy server port in the **Port Number** field.
   − To manage mobile devices not in the Internal Network Range of the network, select the **Support Offsite Devices** option. The plugin retrieves updated host information for off-site devices through the service platform.
6. Select **Apply** to save configuration changes.

**Test Plugin Communication with the MobileIron Service**

Test the plugin communication with the MobileIron service.

**To test communication:**

1. In the **MobileIron MDM** configuration pane, select the Test tab.

2. In the **Device MAC Address** field, type the MAC address of a mobile device that is registered with the MobileIron service. Do not enter colons. Use lower case alphanumeric characters only. Select **Apply**.

3. In the Options pane, select **Plugins**. Select the **MobileIron MDM** plugin and select **Test**. Using configured settings, CounterACT attempts to connect with the MobileIron service and to retrieve endpoint property values for the specified device.

**Run MobileIron Policy Templates**

This plugin provides the following policy templates to detect, manage and remediate mobile devices in a MobileIron environment:
MobileIron Enrollment Policy Template – generates a CounterACT policy that detects corporate hosts not enrolled with the MobileIron service and prompts host users to enroll.

MDM Classification Policy Template – generates a CounterACT policy that classifies all mobile devices into groups. All plugins in the MDM Integration Module use this policy. If another plugin of this module is already installed, this policy was probably already created, and the existing version of the policy is retained. If this policy does not already exist, the MobileIron Enrollment Policy Template creates this policy in addition to the MobileIron Enrollment policy.

MobileIron Device Compliance Policy Template – generates a CounterACT policy that detects and remediates non-compliant devices.

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

MobileIron Enrollment Policy Template

Use this policy to detect corporate devices that have not enrolled with the MobileIron portal and prompt users to enroll. Devices are redirected to an enrollment interaction when they browse in the corporate network. By default, users cannot browse the Internet until enrollment is complete. A restrictive action blocks corporate network access to users not enrolled. This action is disabled by default.

Prerequisites

Before you run a policy based on this template, run policies based on the Asset Classification, Mobile Classification, iOS Classification and Android Classification templates. Policies based on these templates create groups and classify devices into
Multiple MDM Service Enrollment

When additional MDM services are active in the network environment, other plugins of the MDM module may be installed. By default, this policy only checks whether endpoints were previously enrolled in the MobileIron service. It does not check for enrollment in other MDM services. When additional plugins of the MDM module are installed, edit this and other enrollment policies to omit endpoints that are already enrolled in another active MDM service.

- If MDM services are deployed by geographical region or network segment, see Which Endpoints are Inspected - Policy Scope.
- To add a general rule that checks for previously enrolled endpoints, see Detecting and Handling Devices Not Qualified for Enrollment.

Running the Template

This section describes how to run the template.

To run the template:

1. Select the Policy tab from the Console.
3. Select MobileIron and then select MobileIron Device Enrollment.
4. Select **Next**. The Name page opens. Define a unique name for the policy you are creating based on this template.

5. Select **Next**. The Scope page opens. Use the IP Address Range dialog box to define which endpoints will be inspected. The following options are available for defining a scope:
   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope page.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

Select **OK**. The added range appears in the Scope page.

In the Filter by Group area, the scope of the policy is limited to members of the **Mobile devices group**. You must run the Mobile Classification template to create and populate this group.

6. The Offsite Hosts page opens. If you selected the **Support off-site devices** option when you configured the plugin, select the **Include offsite hosts** option. Endpoints without a known IP address are added to the scope of the policy. This is equivalent to selecting the **Unknown IP addresses** option in the Scope page of the wizard.
7. Select **Next**. The Summary page opens and lists the policies generated by the template.
   - If the **MDM Classification** policy did not already exist, it is also created.
8. Select **Finish**. The policy is created.

Which Endpoints are Inspected - Policy Scope

By default, MobileIron service enrollment is only invoked when devices are in the corporate network. Devices without an IP address are not in the corporate network. Do not include the **Unknown IP Address** option when you define the range for
policies based on this template, because policy rules filter out these endpoints even if they are included in the scope.

**How Devices are Detected and Handled**

This section describes the rules and sub-rules of the policy created by the MobileIron Enrollment Policy template.

**Main Rule**

The main rule of the policy does not filter hosts, but it specifies recheck behavior for the policy. By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

**Sub-Rules**

Sub-rules of the policy filter situations and endpoints for which MobileIron enrollment is not applicable. The final sub-rules enroll qualified mobile devices in the MobileIron service.

*Detecting and Handling Devices Not Qualified for Enrollment*

Initial sub-rules of the policy detect and bypass devices that are not candidates for enrollment, for example devices that are not part of the corporate domain, or devices listed in the MobileIron Exceptions group. When a device matches one of these rules, the policy evaluation of the device ends. No actions are applied, with the exception of already enrolled devices, which are placed in the MobileIron Enrolled Devices group.

1. **Unknown MAC** – CounterACT queries MobileIron for host information based on the MAC Address of the device. If no MAC Address is known for an endpoint, the MobileIron service cannot be used to manage the device.

2. **Cloud Disconnected** – this rule tests for CounterACT connectivity with the MobileIron cloud, which is necessary for enrollment. This rule suspends evaluation of the policy if there is no connectivity with the MobileIron cloud.

3. **Enrolled Device** – this rule detects devices already enrolled in the MobileIron service.

   🌟 The Add to Group action adds devices that match this rule to the MobileIron Enrolled Devices group.

   No further enrollment action is necessary for these endpoints, and their evaluation ends at this rule.

4. **Unknown IP Address** – enrollment is only invoked when devices are in the corporate network. Devices without an IP address are not in the corporate network.

5. **Offline** – Enrollment cannot be implemented if the device has gone offline.

6. **Non-Corporate Users** – by default, only corporate user devices are enrolled in the MobileIron service.

7. **MobileIron Exceptions** - devices listed in the MobileIron Exceptions group are excluded from enrollment.
Detecting and Handling Devices Qualified for Enrollment

The following two sub-rules detect devices that are qualified for enrollment in the MobileIron service, and prompt device users to enroll in the service.

8. Devices Not Enrolled – iOS – if a device has been classified into the iOS group but is not a member of the MobileIron Enrolled Devices group, it is a candidate for enrollment.

9. Devices Not Enrolled – Android – if a device has been classified into the Android group but is not a member of the MobileIron Enrolled Devices group, it is a candidate for enrollment.

The following actions are applied when a device matches one of these rules:

- An HTTP Notification action redirects users to an enrollment interaction. See Mobile Device Enrollment for typical enrollment interaction.
- An optional Virtual Firewall action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See Configuring Virtual Firewall Actions for information about enabling this action.

Newly enrolled endpoints are not immediately added to the MobileIron Enrolled Devices group. If the enrollment interaction completed successfully, the Enrolled Device sub-rule assigns them to the group the next time this policy runs.

MDM Classification Policy Template

Use this template to create a policy that classifies all mobile devices into groups. Devices are sorted by operating system, and by their corporate/guest status.

All plugins in the MDM Integration Module use this policy. If another plugin of the module is already installed, this policy was probably already created, and the existing version of the policy is retained.

If this policy does not already exist, the MobileIron Enrollment Policy template creates this policy in addition to the MobileIron Enrollment policy.

Prerequisites

This policy sorts endpoints based on previous classification by the Asset Classification and Mobile Classification policies, and corporate/guest status as determined by Corporate/Guest Control policies. Run these policies before you run this policy.
Which Endpoints are Inspected - Policy Scope

To classify all mobile devices, including devices not currently in the corporate network, include the **Unknown IP Address** option when you define the range for policies based on this template. This option is active in the default template.

How Devices are Detected and Handled

This section describes the rules and sub-rules of the MDM Classification policy as it is created by MDM plugin templates.

Main Rule

The main rule of the policy does not filter hosts, but it specifies recheck behavior for the policy. By default, the policy is evaluated every 30 minutes, and is applied to newly discovered endpoints.

Sub-Rules

Sub-rules of the policy perform the following:

- Filter endpoints that cannot be evaluated
- Sort corporate user mobile devices into groups by their operating system
- Evaluate mobile devices that have not logged in as corporate users.

Conditions Preventing MDM Evaluation

This rule excludes endpoints based on the following filter conditions.

1. **Unknown MAC** – If no MAC Address is known for an endpoint, CounterACT cannot evaluate whether the device is managed by an MDM service. No actions are applied, and policy evaluation of the endpoint ends.

Corporate Devices Already Enrolled in an MDM Service

The following rules detect corporate mobile devices that are already enrolled in an MDM service based on the **MDM Network Function** host property. Because this
property receives values from MDM services, a valid value indicates that the endpoint is managed by an MDM service.

2. **Corporate iOS Mobile Devices**

3. **Corporate Android Mobile Devices**

4. **Other Corporate Mobile Devices**

The Add to Group action is used to assign all endpoints that match one of these rules to the following groups:

- **Mobile Devices** group
- **Corporate Hosts** group - devices with any CounterACT management components installed are assumed to be corporate user devices.

In addition, devices are assigned to the following groups based on their operating system:

- **iOS** group
- **Android** group

**Conditions Preventing Further Evaluation**

The final rules of the policy will sort corporate/guest users. The following rules of the policy exclude endpoints that cannot be classified as corporate/guest users. When an endpoint matches one of these rules, no actions are applied, and policy evaluation of the endpoint ends.

5. **Unknown IP Address** – Corporate/guest evaluation is irrelevant for the remaining endpoints without an IP address. (Corporate devices that are already enrolled in an MDM service were detected by the previous rules - even if they are currently outside the corporate network.)

6. **Not a Mobile Device** – this policy focuses on mobile endpoints. Endpoints that were not classified into the *Mobile Devices* group are excluded from further evaluation.

**Corporate/Guest User Evaluation for Mobile Devices**

The remaining rules sort unmanaged mobile devices into groups using standard corporate/guest authentication criteria.

7. **Corporate Users** - if at least one of the following criteria is met, a device is evaluated as a **Corporate Host**.
   - The device recently authenticated via the **HTTP Login** action
   - The device is enrolled in an MDM service

The Add to Group action assigns endpoints that match the rule to the **Corporate Hosts** group.

8. **Signed-in Guest Users** - if the user authenticated as a guest via the **HTTP Login** action the endpoint is evaluated as a **Signed-In Guest**.

   The Add to Group action assigns endpoints that match the rule to the **Signed-In Guests** group.

9. **Unregistered Guest Users** – if the user was not authenticated as a corporate host or signed-in guest, the following actions are applied:
The **Add to Group** action assigns the endpoint to the *Guest Hosts* group.

The **HTTP Login** action redirects the endpoint to an interaction for authentication.

An optional **Virtual Firewall** action prevents users from accessing the corporate network until they complete enrollment. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.

**MobileIron Device Compliance Policy Template**

Use this template to create a policy that verifies device compliance with CounterACT network requirements and MobileIron service requirements. When a non-compliant device browses in the corporate network, an **HTTP Notification** action redirects the user to a notification that indicates:

- Why the device is not-compliant
- Network access limitations
- Steps for remediation

By default, non-compliant users cannot browse the Internet but can access the corporate network. An optional restrictive action blocks corporate network access to users not enrolled. This action is disabled by default.

**Prerequisites**

To detect unauthorized applications you must add unauthorized applications to the Unauthorized Mobile Application list. An empty list is automatically created when the plugin is installed. See [Adding Applications to the Unauthorized Application List](#).

You must create and run a policy based on the MobileIron Device Enrollment template **before** you use this template to create policies. This template uses groups and other information created by the MobileIron Device Enrollment policy.

**Running the Template**

This section describes how to run the template.

**To run the template:**

1. Select the Policy tab from the Console.

![CounterACT Enterprise Manager Console - admin connected to 10.37.2.200 - Licensed for 650](image)

2. Select **Add**. The Policy Wizard opens.

3. Select **MobileIron** and then select **MobileIron Device Compliance**.
4. Select **Next**. The Name page opens. Define a unique name for the policy you are creating based on this template.

5. Select **Next**. The Scope page opens. Use the IP Address Range dialog box to define which endpoints will be inspected. The following options are available for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope page.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

Select **OK**. The added range appears in the Scope page.

In the Filter by Group area, the scope of the policy is limited to members of the **MobileIron Enrolled Devices** group. You must run the MobileIron Enrollment template to create and populate this group.
6. The Offsite Hosts page opens. If you selected the **Support off-site devices** option when you configured the plugin, select the **Include offsite hosts** option. Endpoints without a known IP address are added to the scope of the policy. This is equivalent to selecting the **Unknown IP addresses** option in the Scope page of the wizard.

7. Select **Next**. The Sub-Rules page lists the rules of the policy.
8. (Optional) Modify the sub-rules of the policy. You can also edit the policy after it is created.

9. Select **Finish**. The policy is created.

**Which Endpoints are Inspected - Policy Scope**

Policies based on this template only inspect devices previously enrolled in the MobileIron service. The *MobileIron Enrolled Devices* group is used to filter the scope of this policy.
Because notification and enrollment use HTTP redirection actions, do not include the **Unknown IP Address** option when you define the range for policies based on this template.

**How Devices are Detected and Handled**

This section describes the rules and sub-rules of the MDM Classification policy as it is created by MDM plugin templates.

**Main Rule**

The main rule of the policy does not filter hosts, but it specifies recheck behavior for the policy. By default, the policy is evaluated every 8 hours, and is applied to newly discovered endpoints.

**Sub-Rules**

Sub-rules of the policy perform compliance evaluations, and apply various remediation actions.

**Detect Endpoints with Unauthorized Applications**

The following rule detects and remediates devices with unauthorized applications:

1. **Unauthorized Application Installed** – this rule checks the applications listed in the **MobileIron Software Inventory** host property against the MobileIron Unauthorized Mobile Applications list. See [Adding Applications to the Unauthorized Application List](#) for information about creating this list.

   A device matches this rule when an unauthorized application is found. In this case the following actions are applied to the endpoint:

   - An **HTTP Notification** action informs the user that an unauthorized application is installed on the device.
   - The **Add to Group** action assigned the device to the **MobileIron Unauthorized Application Installed** group.
   - An optional **Virtual Firewall** action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.

**Detect Endpoints that Removed the MobileIron Service App**

The following rules examine applications listed in the **MobileIron Software Inventory** host property to identify previously enrolled devices that do not have the MobileIron service enrollment package installed.

2. **MobileIron App Not Installed – iOS**

3. **MobileIron App Not Installed – Android**

   When a device matches one of these rules:

   - An **HTTP Notification** action redirects users to a service enrollment interaction. See [Mobile Device Enrollment](#) for typical enrollment interaction.
The **Add to Group** action assigns the device to the *MobileIron App Not Installed – iOS* or the *MobileIron App Not installed – Android* group.

An optional **Virtual Firewall** action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.

**Detect Jailbroken or Rooted Endpoints**

4. **Device Jailbroken/Rooted** – this rule tests the *MobileIron Jailbroken/Rooted* host property to detect jailbroken iOS devices or rooted Android devices. When a device matches this rule:

   - An **HTTP Notification** action informs the user that the device is jailbroken/rooted, and its access to the corporate network is restricted.
   - The **Add to Group** action assigns the device to the *MobileIron Device Jailbroken/Rooted* group.

   An optional Virtual Firewall action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.

**Detect Devices Out of MobileIron Service Compliance**

5. **MobileIron Out of Compliance** – this rule tests the *MobileIron Compliance Status* host property to detect devices that do not meet compliance criteria of the MobileIron service. When a device matches one of these rules:

   - An **HTTP Notification** action informs the user that the device does not meet MobileIron service compliance criteria, and its access to the corporate network is restricted.
   - The **Add to Group** action assigned the device to the *MobileIron Out of Compliance* group.

   An optional **Virtual Firewall** action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.

6. **MobileIron Compliant** – Endpoints that did not match previous rules are considered to be compliant. When a device matches one of these rules:

   - An **HTTP Notification** action informs the user that the device is compliant, and prompts the user to continue browsing in the corporate network.
   - The **Add to Group** action assigns the device to the *MobileIron Compliant Devices* group.
Adding Applications to the Unauthorized Application List

In order to work with the MobileIron Device Compliance Policy template, you must compile a list of applications that you want to prohibit on your network.

The Unauthorized Mobile Application list is automatically created when the plugin is installed. You must add the applications that you want to prohibit to this list. The list is automatically incorporated into the Unauthorized Applications Installed sub-rule.

To add an application to the list:

1. Select Options from the Tools menu and then select Lists.

2. Select the Unauthorized Mobile Application entry for MobileIron.


5. Enter the name of an application that you want to prohibit and then select OK.

6. Repeat steps 4 and 5 for other prohibited applications.

7. (Optional) Type a description of the list in the **Description** field of the Edit List dialog box.

8. Select **Ok**. The unauthorized applications that you added appear in the Values column.

---

**Configuring Virtual Firewall Actions**

Policy templates include optional **Virtual Firewall** actions that block user access to the corporate network. These actions are disabled by default in policy templates. If you enable the **Virtual Firewall** action, edit action settings to permit MDM service communication with the device.

**To configure virtual firewall actions:**

1. Open a rule of the policy. Select the **Virtual Firewall** action, and select **Edit**. The Virtual Firewall action dialog box opens.

2. In the Blocking Exceptions table of the Parameters tab, select the exception that uses port 443/TCP. Select **Edit**:
3. In the Blocking Exceptions dialog, make the following selections:
   - Allow traffic from the host
   - All IPs
   - Select the port used to communicate with the MDM service.

![Blocking Exceptions dialog]

4. Select **OK** to save changes to the exception. Select **OK** to finish editing the action.

5. Repeat this procedure for all the ports required by the plugin. See Networking Requirements.

### Mobile Device Enrollment

The MobileIron Enrollment policy template provided with this plugin creates policies that are used to guide corporate users through enrollment. These policies detect corporate devices that have not enrolled and prompt them with the enrollment pages shown below. See MobileIron Enrollment Policy Template for information about the policy template.

Default MobileIron policies are designed to enroll corporate users only. The policies do not redirect guest users to MobileIron enrollment. By default, users can browse the Internet, but cannot access the corporate network.

This section describes user interaction on the mobile device during enrollment. The process shown below reflects iOS enrollment. Interaction may vary slightly on devices running Android mobile operating systems.
To enroll:

1. CounterACT detects new mobile endpoints when they enter the network, and redirects users to the login page shown below. Corporate users log in to the network. Other users can register as guests to enter the corporate network.

2. CounterACT authenticates corporate users and redirects them to the following page.


4. In a new window, the MobileIron Mobile@Work Client download page opens. Users download and install the application. The ForeScout redirection window contains information needed for enrollment. Users should not close this window.
5. When profile installation is complete, users must return to the ForeScout redirection page and select **Recheck my computer**.

6. CounterACT identifies the device as enrolled in MobileIron, and applies MobileIron-based compliance policies. Enrolled users select **Continue** to access the corporate network.
Display Inventory Data

Use the CounterACT Inventory to view a real-time display of MobileIron device network activity at multiple levels, for example, software installed, core attributes or hardware information.

The inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific
- View MobileIron devices that have been detected with specific attributes
- Easily track MobileIron device activity
- Incorporate inventory detections into policies

To access the inventory:

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the MobileIron entries.
The following information is available:

- MobileIron Apps: Software Installed
- MobileIron Details: MobileIron Manufacturer, Model, Platform

Refer to the section about working with inventory detections in the CounterACT Console User's Manual or the Console, Online Help for information about how to work with the CounterACT Inventory.

Managing Offsite Devices

When devices are not in the corporate network, the plugin uses the MobileIron service platform to retrieve updated host information and implement CounterACT policy actions.

To configure support for management of offsite devices:

- Select the **Support Offsite Devices** option when you configure the plugin. See Configure the Plugin.
- Select the **Include Offsite Hosts** option when you create policies based on MobileIron templates. See Run MobileIron Policy Templates.

Consider the following when you create CounterACT policy conditions and actions that apply to offsite endpoints:

- CounterACT identifies offsite devices by their MAC address. To manage offsite devices, policies must include endpoints without a known IP address in their scope.
- All host properties can be evaluated for offsite devices.
- All MobileIron-specific actions provided by this plugin are supported on offsite devices. See Controlling MobileIron Devices - Policy Actions.
- Not all general CounterACT actions can be applied to offsite devices. The following CounterACT actions can be applied to offsite devices:
  - **Manage**: Add to Group / Classify / Delete Host
  - **Notify**: Send Email

Note that no Restriction or HTTP redirection actions can be applied to offsite devices.

Create Custom MobileIron Policies

You may choose to create custom policies to deal with issues not covered in the MobileIron policy templates. Custom policy tools provide you with an extensive range of options for detecting and handling endpoints.

This section describes the policy properties and actions available when the MobileIron plugin is installed.
Detecting MobileIron Devices - Policy Properties

CounterACT policy conditions and properties let you detect mobile devices based on information from the MobileIron service.

In the conditions screen, expand the MobileIron folder in the Properties tree to use MobileIron properties in a policy condition. An extensive range of properties can be detected. The categories include:

- **MobileIron**
- **MobileIron Apps**
- **MobileIron Details**
- **MobileIron Label Membership**
- **MobileIron Policies**
- **Asset Classification**

---

### MobileIron

<table>
<thead>
<tr>
<th>MobileIron Connectivity to MobileIron Cloud</th>
<th>Indicates connectivity to the MobileIron Cloud.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron Device Last Update</td>
<td>Indicates the time that the device was last updated.</td>
</tr>
<tr>
<td>MobileIron Listed in Service</td>
<td>Indicates if the device is listed as being in service.</td>
</tr>
</tbody>
</table>

### MobileIron Apps

| MobileIron Apps | Indicates if specific software is installed on the MobileIron device. |
## MobileIron Details

<table>
<thead>
<tr>
<th>MobileIron Android Device Rooted</th>
<th>Indicates if an enrolled Android device is rooted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron Compliance State</td>
<td>Indicates the compliance state of MobileIron.</td>
</tr>
<tr>
<td>MobileIron Country Code</td>
<td>Indicates the country code for the device.</td>
</tr>
<tr>
<td>MobileIron Current MCC (iOS)</td>
<td>Indicates the local service operator when the device was roaming.</td>
</tr>
<tr>
<td>MobileIron Device ID</td>
<td>Indicates the device unique identifier.</td>
</tr>
<tr>
<td>MobileIron JailBroken iOS Device</td>
<td>Indicates if the MobileIron iOS device is jailbroken.</td>
</tr>
<tr>
<td>MobileIron E/C</td>
<td>Indicates that the device was registered as owned by the user (TRUE) or by the company (FALSE).</td>
</tr>
<tr>
<td>MobileIron Email</td>
<td>Indicates the user's Email address as entered during registration.</td>
</tr>
<tr>
<td>MobileIron Last Check-In</td>
<td>Indicates the date and time when the device was last connected to the MobileIron Core.</td>
</tr>
<tr>
<td>MobileIron Locale</td>
<td>Indicates the device language during device registration (autogenerated).</td>
</tr>
<tr>
<td>MobileIron Manufacturer</td>
<td>Indicates the device manufacturer as automatically reported by the device during registration.</td>
</tr>
<tr>
<td>MobileIron MDM Managed</td>
<td>Indicates whether or not the MDM was enabled.</td>
</tr>
<tr>
<td>MobileIron Model</td>
<td>Indicates the model for the device as reported by the device during registration.</td>
</tr>
<tr>
<td>MobileIron Name</td>
<td>Indicates the user’s name that is displayed on the MobileIron Core.</td>
</tr>
<tr>
<td>MobileIron Number</td>
<td>Indicates the phone number as entered by the user or administrator during registration.</td>
</tr>
<tr>
<td>MobileIron Operator</td>
<td>Indicates the local service operator when the device was roaming.</td>
</tr>
<tr>
<td>MobileIron Out Of Compliance Reasons</td>
<td>Indicates that MobileIron is out of compliance reasons.</td>
</tr>
<tr>
<td>MobileIron Platform</td>
<td>Indicates the device platform as entered during registration.</td>
</tr>
<tr>
<td>MobileIron User ID</td>
<td>Indicates the user identifier for the device.</td>
</tr>
</tbody>
</table>

## MobileIron Label Membership

<table>
<thead>
<tr>
<th>MobileIron Label Membership</th>
<th>Indicates if specific software is installed on the MobileIron device.</th>
</tr>
</thead>
</table>
MobileIron Policies

| MobileIron Policies | Indicates all policies that are associated to the device. |

Asset Classification

| MDM Network Function | Indicates the mobile operating system of an MDM managed endpoint. This property is common to all plugins of the MDM Integration Module, and appears in the Asset Classification folder of the Properties tree. |

Controlling MobileIron Devices - Policy Actions

CounterACT policy actions let you apply MobileIron service actions to mobile devices based on CounterACT policy detections.

In the Actions screen, expand the MobileIron folder in the Actions tree to use MobileIron actions in a policy. You can apply the following actions to mobile devices that are detected by a CounterACT policy.

- MobileIron Apply to Label
- MobileIron Force Device Check-In
- MobileIron Remove From Label
- MobileIron Wipe

MobileIron Apply to Label

This action applies a label to a device.
MobileIron Force Device Check-In
This action wakes up a device, forcing it to connect to the MobileIron Core.

MobileIron Remove From Label
This action removes a label from a device.

MobileIron Wipe
This action removes all data and custom settings, restoring the factory defaults. Once wiped, the device status changes to Wiped.
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

*Console User Manual*
Select **CounterACT Help** from the **Help** menu.

*Plugin Help Files*

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Plugins**.
2. Select the plugin and then select **Help**.

*Documentation Portal*
Select **Documentation Portal** from the **Help** menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. (“ForeScout”). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-10-05 11:16