Contact Information

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Create a MobileIron Device Compliance Policy ................................................ 26
Prerequisites ........................................................................................................ 26
Create a Device Compliance Policy ................................................................. 26
Which Endpoints Are Inspected - Policy Scope .............................................. 29
How Devices Are Detected and Handled ........................................................ 29
Add Applications to the Unauthorized Application List .................................. 31
Configure Virtual Firewall Actions ................................................................ 33

Mobile Device Enrollment ............................................................................... 35

Display Asset Inventory Data ........................................................................... 37

Manage Offsite Devices .................................................................................... 38

Create Custom MobileIron Policies .............................................................. 39
Detect MobileIron Devices - Policy Properties .............................................. 39
MobileIron ........................................................................................................ 40
MobileIron Apps .............................................................................................. 40
MobileIron Details .......................................................................................... 40
MobileIron Label Membership ..................................................................... 41
MobileIron Policies ........................................................................................ 41
Asset Classification ........................................................................................ 41
Control MobileIron Devices - Policy Actions .................................................. 41
MobileIron Apply to Label .............................................................................. 42
MobileIron Force Device Check-In ................................................................. 42
MobileIron Remove From Label .................................................................. 42
MobileIron Wipe ............................................................................................. 43

Additional Forescout Documentation ............................................................. 43
Documentation Downloads .......................................................................... 44
Documentation Portal ..................................................................................... 44
Forescout Help Tools ....................................................................................... 45
About MobileIron Integration

The Forescout platform integrates with MobileIron® to help IT administrators streamline the process to provision, manage, and secure today’s expanding suite of smartphones and tablets, all from a single portal. The integration of the Forescout platform with MobileIron 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 an on-premises system and as 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.

The Forescout platform’s 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**, with support for 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**, with 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**, with auto-quarantine for Exchange, and alerts IT personnel to approve all new devices. Additionally this integration supports easy user self-enrollment via web, email, or SMS.

About Certification Compliance Mode

Forescout eyeExtend for MobileIron supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*.

Additional MobileIron Documentation

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

About this Module

Integration with the Forescout platform lets you deliver a comprehensive solution that provides powerful monitoring and enforcement capabilities not available when working solely with the MobileIron solution. Use Forescout eyeExtend for MobileIron to complete the cycle of security by leveraging valuable capabilities:

- Automated real-time, continuous detection and compliance of mobile devices from 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, in order to:
  - 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.
- Device tagging at the MobileIron console, based on detections by the Forescout platform.
- Enhancement of the Asset Inventory by populating it with MobileIron Core information.

How it Works

Forescout eyeExtend for MobileIron 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 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 to the Enterprise Manager.
Continuous Query Refresh

MobileIron query mechanisms recheck endpoint attributes at a static frequency—approximately once a day. However, after module installation, querying of endpoint properties is based on the Forescout platform's 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 of the Forescout platform policies.

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 module must learn endpoint MAC addresses in order to initiate the query process.

Offsite Device Management

The module leverages integration with MobileIron to manage devices even when they are not in the corporate network. The module 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 [Manage Offsite Devices](#).

Supported Devices

The following devices are supported by Forescout eyeExtend for MobileIron:

- iOS
- Android
For operating system version support information, refer to the following MobileIron documentation:

- [https://community.mobileiron.com/welcome](https://community.mobileiron.com/welcome) (credentials required)

## Supported Network Infrastructures

MobileIron supports the following:

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

## About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, *IPv6 addresses are not yet supported by this module.* The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this module.

## What to Do

Perform the following steps to set up the MobileIron integration:

1. Verify that you have met system requirements. See Requirements.
2. Verify the MDM Web Service Setup.
4. Install the Module.
5. Configure the Module.

## Requirements

This section describes system requirements and recommendations.

- Forescout Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements
- MobileIron Requirements
- Networking Requirements
- Endpoint Requirements
• Additional Deployment Recommendations

**Forescout Requirements**

The following Forescout releases can work with this module.

- Forescout version 8.1 or 8.2.
- A module license for Forescout eyeExtend for MobileIron. See Forescout eyeExtend (Extended Module) Licensing Requirements.

**Forescout eyeExtend (Extended Module) Licensing Requirements**

This Forescout eyeExtend product requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

**To identify your licensing mode:**

- From the Console, select Help > About Forescout.

**Per-Appliance Licensing Mode**

When installing the module 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 sales 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 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 Forescout Administration Guide 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 that you want this license to handle. Licenses for this module are based on the number of mobile devices managed by Forescout via the MDM service.
Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.

![Example Module License Request - Step 3 of 4](image)

### Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each product you want to work with in your deployment, including eyeExtend products. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend products. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

- **No demo license is automatically installed during system installation.**

License entitlements are managed in the [ForeScout Customer Portal](https://www.forescout.com). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module, but does not exceed the capacity of the Forescout eyeSight license.

- **Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging individual licensed modules are supported. The Open Integration Module is an eyeExtend product even though it packages more than one module.**

### More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the [Forescout Administration Guide](https://www.forescout.com).
- **Flexx Licensing.** Refer to the [Flexx Licensing How-to Guide](https://www.forescout.com).

You can also contact your Forescout sales representative for more information.
MobileIron Requirements

- MobileIron Core version 9.0, 9.1, 9.3, and 9.5 (on-premises or Connected Cloud).
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Networking Requirements

The following ports must be open on enterprise firewalls to support communication between the Forescout platform 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 module. See Configure the Module.

- 443/TCP

In addition, define exceptions to the Virtual Firewall action for these ports. See Configure Virtual Firewall Actions.

Endpoint Requirements

Queries to MDM services are based on endpoint MAC addresses. As such, the Forescout platform 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)

Additional Deployment Recommendations

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

Verify the MDM Web Service Setup

This section describes how to verify that the Web Service is properly set up and that the MobileIron console supports Web services.
To verify the setup:

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 Module.
   - Define the HTTP header Authorization (basic). Provide the same
     username and password that will be defined in Configure the Module.
   - Define the HTTP header Accept, as follows: application/xml.

4. Select Send.

The returned Response body is displayed in the REST client user interface.
This information is provided in XML format.

Define a Forescout User at the MobileIron Admin Portal

The Forescout platform logs in to the MobileIron Core Service as this user. The
Forescout user information is required during the module configuration.

To define a Forescout user in the MobileIron Admin portal:

1. Define a user account for the Forescout platform in the MobileIron Admin
   administration portal.

2. Select Admin.
3. Select the Forescout 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 the user account settings. This information is required to configure the module.*

### Install the Module

This section describes how to install the module.

**To install the module:**

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - **Product Updates Portal** - *Per-Appliance Licensing Mode*
   - **Customer Portal, Downloads Page** - *Flexx Licensing Mode*

   To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file.

3. Save the file to the machine where the Console is installed.

4. Log into the Console and select **Options** from the **Tools** menu.

5. Select **Modules**. The Modules pane opens.

6. Select **Install**. The Open dialog box opens.

7. Browse to and select the saved module `.fpi` file.

8. Select **Install**. The Installation screen opens.

9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

*The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

*In modules that contain more than one component, the installation proceeds automatically one component at a time.*
10. When the installation completes, select Close to close the window. The installed module is displayed in the Modules pane.

- Some components are not automatically started following installation.

- Once installed, the module 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 the Module**

After Forescout eyeExtend for MobileIron is installed, configure the module to communicate with the MobileIron Web Service.

**To configure the module:**

1. In the Console, select **Options** from the **Tools** menu.
2. Select **Modules**.
3. Select **MobileIron MDM** from the Options pane, and then select **Configure**.

![Configure the Module](image)

4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username, which is the user account defined on the MobileIron Administration Portal.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password.</td>
</tr>
<tr>
<td><strong>Retype Password</strong></td>
<td>Re-enter the password to verify it.</td>
</tr>
</tbody>
</table>
5. Select the Advanced tab.

6. Configure the following settings:
<table>
<thead>
<tr>
<th><strong>MDM Query Threshold Interval (Seconds)</strong></th>
<th>Specify how frequently the module queries the MobileIron Core Service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MDM Query Threshold</strong></td>
<td>Define the maximum number of query requests to the MobileIron Core Service per threshold interval (defined in the previous field).</td>
</tr>
<tr>
<td><strong>Use a Proxy Server</strong></td>
<td>Select this option if there is a proxy between the Connecting CounterACT Device and the MobileIron Core Service.</td>
</tr>
<tr>
<td><strong>DNS Name or IP Address of the Proxy Server</strong></td>
<td>Enter the DNS name or the IPv4 address of the proxy server.</td>
</tr>
<tr>
<td><strong>Port Number</strong></td>
<td>Enter the required proxy server port.</td>
</tr>
<tr>
<td><strong>Support Offsite Devices</strong></td>
<td>Select this option to manage mobile devices not in the Internal Network Range of the network. The module retrieves updated host information for off-site devices through the service platform.</td>
</tr>
</tbody>
</table>

7. Select **Apply** to save the configuration changes.

The best practice is to perform a test after setting up a connection. See **Test Module Communication with the MobileIron Service**.

## Test Module Communication with the MobileIron Service

Test the module 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, enter the MAC address of a mobile device that is registered with the MobileIron service. Do not enter colons. Use lowercase, alphanumeric characters only.

3. Select **Apply**.

4. In the Options pane, select **Modules**. Select **MobileIron MDM** and select **Test**. Using configured settings, the Forescout platform attempts to connect with the MobileIron service and to retrieve endpoint property values for the specified device.

**Create MobileIron Policies Using Templates**

This section describes how to use MobileIron templates to create Forescout platform policies to detect, manage, and remediate mobile devices in a MobileIron environment. Refer to the following sections:

- [Create a MobileIron Enrollment Policy](#) to detect corporate hosts not enrolled with the MobileIron service and prompts host users to enroll.

- [Create an MDM Classification Policy](#) to classify all mobile devices into groups. All MDM Integration modules use this policy. If another 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.

- [Create a MobileIron Device Compliance Policy](#) to detect and remediate non-compliant devices.

> *It is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.*
Create a MobileIron Enrollment Policy

Use the MobileIron Enrollment Policy template 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 Primary Classification, Mobile Classification, iOS Classification and Android Classification templates. Policies based on these templates create groups and classify devices into groups. The MobileIron Enrollment Policy uses these groups to filter and select devices.

Multiple MDM Service Enrollment

When additional MDM services are active in the network environment, other MDM Integration modules 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 MDM Integration modules 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.

Create an Enrollment Policy

This section describes how to use this template to create a MobileIron Device Enrollment policy.

To create a policy:

1. In the Console, select Policy.


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

5. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

6. Use the IP Address Range dialog box to define which endpoints are inspected.

   ![IP Address Range dialog box](image)

   The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

7. Select **OK**. The added range is displayed in the Scope pane.

   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.

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

10. 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 select 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.
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 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** – The Forescout platform 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 the Forescout platform’s 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 Configure 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.

Create an MDM Classification Policy

Use the MDM Classification Policy 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 MDM Integration modules use this policy. If another 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 Primary 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, select the Unknown IP Address option when you define the range for policies based on this template. This option is selected 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 Integration module templates.
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 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, the Forescout platform 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 Forescout platform 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 sort corporate/guest users. These policy rules 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 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 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 *Configure Virtual Firewall Actions* for details.

## Create a MobileIron Device Compliance Policy

Use the MobileIron Device Compliance template to create a policy that verifies device compliance with the Forescout platform 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 non-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 module is installed. See *Add 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.

## Create a Device Compliance Policy

This section describes how to use the template to create a MobileIron device compliance policy.

**To create a policy:**

1. In the Console, select **Policy**.

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

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

5. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

6. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

7. Select **OK**. The added range is displayed in the Scope pane.

   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.

8. If you selected **Support off-site devices** when you configured the module, select the **Include offsite hosts** in the Offsite Hosts pane to add Endpoints without a known IP address to the scope of the policy. This is equivalent to selecting the **Unknown IP addresses** option in the Scope pane of the wizard.

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

11. 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 Integration module templates.
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 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 Add 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 Configure 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 Configure 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 [Configure 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 [Configure 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.

**Add 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 module 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.

3. Select **Edit**. The Edit List dialog box opens.

4. Select **Add**.
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 in the Edit List dialog box.

8. Select OK. The unauthorized applications that you added are displayed in the Values column.

**Configure 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 and then select **Edit**.

3. Configure the Blocking Exceptions as follows:
   - Allow traffic from the host
– Select **All IPs**
– Select **Single** and specify the port used to communicate with the MDM service.

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 module. See Networking Requirements.

**Mobile Device Enrollment**

The MobileIron Enrollment policy template creates the policies used to guide corporate users through enrollment. These policies detect corporate devices that have not enrolled and prompt those users to complete the enrollment process. See Create a MobileIron Enrollment Policy for details.

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 described below reflects iOS enrollment. Interaction may vary slightly on devices running Android mobile operating systems.

1. When the Forescout platform detects new mobile endpoints on the network, it redirects users to the login page. Log in to the network as a corporate user. Other users can register as guests to enter the corporate network.

![Login Page](image)

2. The Forescout platform authenticates corporate users and prompts them to download the MobileIron App.
3. Users select **Download MobileIron App**.

4. The MobileIron Mobile@Work Client download page opens in a new window. Users download and install the application. *The redirection window contains information needed for enrollment. Users should not close this window.*

5. When profile installation is complete, users must return to the redirection page and select **Recheck my computer**.
6. The Forescout platform identifies the device as enrolled in MobileIron, and applies MobileIron-based compliance policies.

7. Enrolled users select **Continue** to access the corporate network.

### Display Asset Inventory Data

Use the Asset 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 Asset 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 asset inventory detections into policies

To access the Asset Inventory:

1. In the Console, select Asset Inventory.
2. In the Views pane, go 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 Forescout Administration Guide or the Console Online Help for information about how to work with the Asset Inventory.

Manage Offsite Devices

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

To configure support for management of offsite devices:

- Select the Support Offsite Devices option when you configure the module. See Configure the Module.

- Select the Include Offsite Hosts option when you create policies based on MobileIron templates. See Create MobileIron Policies Using Templates.

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

- The Forescout platform 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 module are supported on offsite devices. See Control MobileIron Devices - Policy Actions.
Not all general Forescout actions can be applied to offsite devices. The following actions can be applied to offsite devices:

- **Manage:** Add to Group / Classify / Delete Host
- **Notify:** Send Email

*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 Forescout eyeExtend for MobileIron is installed.

### Detect MobileIron Devices - Policy Properties

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

In the conditions dialog box, 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><strong>MobileIron Connectivit</strong>&lt;br&gt;to MobileIron Cloud</th>
<th>Indicates connectivity to the MobileIron Cloud.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MobileIron Device Last Update</strong></td>
<td>Indicates the time that the device was last updated.</td>
</tr>
<tr>
<td><strong>MobileIron Listed in Service</strong></td>
<td>Indicates if the device is listed as in service.</td>
</tr>
</tbody>
</table>

### MobileIron Apps

<table>
<thead>
<tr>
<th><strong>MobileIron Apps</strong></th>
<th>Indicates if specific software is installed on the MobileIron device.</th>
</tr>
</thead>
</table>

### MobileIron Details

<table>
<thead>
<tr>
<th><strong>MobileIron Android Device Rooted</strong></th>
<th>Indicates if an enrolled Android device is rooted.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MobileIron Compliance State</strong></td>
<td>Indicates the compliance state of MobileIron.</td>
</tr>
<tr>
<td><strong>MobileIron Country Code</strong></td>
<td>Indicates the country code for the device.</td>
</tr>
<tr>
<td><strong>MobileIron Current MCC (iOS)</strong></td>
<td>Indicates the local service operator when the device was roaming.</td>
</tr>
<tr>
<td><strong>MobileIron Device ID</strong></td>
<td>Indicates the device unique identifier.</td>
</tr>
<tr>
<td><strong>MobileIron iOS Device JailBroken</strong></td>
<td>Indicates if the MobileIron iOS device is jailbroken.</td>
</tr>
<tr>
<td><strong>MobileIron E/C</strong></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>------------------------</td>
<td>------------------------------------------------------------------</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 device model 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**

| MobileIron Label Membership | Indicates if specific software is installed on the MobileIron device. |

**MobileIron Policies**

| MobileIron Policies | Indicates all polices 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 MDM Integration modules, and is displayed in the Classification folder of the Properties tree. |

**Control MobileIron Devices - Policy Actions**

The Forescout platform policy actions let you apply MobileIron service actions to mobile devices based on policy detections.

In the Actions dialog box, 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 Forescout platform 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 Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools
Documentation Downloads

Documentation downloads can be accessed from the Forescout Technical Documentation Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – Product Updates Portal
- **Flexx Licensing Mode** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:
- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:
- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:
- Go to https://Forescout.force.com/support/ and select Downloads.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/
Forescout Help Tools
Access information directly from the Console.

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

Forescout Administration Guide
- Select Administration Guide from the Help menu.

Plugin Help Files
- After the plugin is installed, select Tools > Options > Modules, select the plugin and then select Help.

Documentation Portal
- Select Documentation Portal from the Help menu to access the Documentation Portal.