FORESCOUT

Forescout

eyeExtend for IBM MaaS360

Configuration Guide

Version 1.9

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

2020-02-26 11:13

Table of Contents

About MaaS360 Integration 5
About Certification Compliance Mode 5

Additional Forescout MDM Documentation 5

About this Module 6
How it Works 6
Continuous Query Refresh 7
Offsite Device Management 7
Supported Devices 7
Supported Network Infrastructure 8
What to Do 8

Requirements 8
Forescout Requirements 9
Forescout eyeExtend (Extended Module) Licensing Requirements 9
Per-Appliance Licensing Mode 9
Flexx Licensing Mode 10
More License Information 10
Registration and Activation Requirements 11
Networking Requirements 11
Endpoint Requirements 11
Additional Deployment Recommendations 11
About Support for Dual Stack Environments 12

Verify the MDM Web Service Setup 12

Install the Module 13

Configure the Module 13

Test Module Communication with the Service 16

Create MaaS360 Policies Using Templates 17
Create a MaaS360 Enrollment Policy 18
Prerequisites 18
Multiple MDM Service Enrollment 18
Create an Enrollment Policy 19
Which Endpoints Are Inspected – Policy Scope 21
How Devices Are Detected and Handled 21
Create an MDM Classification Policy 23
Prerequisites 23
How Devices Are Detected and Handled 23
Create a MaaS360 Device Compliance Policy 26
Prerequisites 26
Create a Device Compliance Policy 26

Which Endpoints Are Inspected – Policy Scope 28
How Devices Are Detected and Handled 28
Add Applications to the Unauthorized Application List 31
Configure Virtual Firewall Actions 33

Display Asset Inventory Data 34

Manage Offsite Devices 35

Work with the Forescout Platform's Policies 36
Detect MaaS360 Devices – Policy Properties 36
Primary Classification 37
Core Attributes 37
Security and Compliance 38
Hardware Inventory 39
Network Information 39
Additional Information 39
Tag MaaS360 Devices – Policy Actions 39
Custom Attribute Value Action 39
Refresh Device Information Action 40

Additional Forescout Documentation 40
Documentation Downloads 41
Documentation Portal 41
Forescout Help Tools 42

About MaaS360 Integration

The Forescout platform integration with MaaS360® helps 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 MaaS360 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.

MaaS360 is available as an *on-premises* system and as a *cloud service*. 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.

Integration of the Forescout platform 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 all major smartphone and tablet platforms including iOS and Android, 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 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 IBM MaaS360 supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide.*

Additional Forescout MDM Documentation

Refer to the documents linked from the following file for more technical information about the Forescout MDM solution.
http://updates.forescout.com/online/help/mdm/ForeScout_MDM_doc.pdf

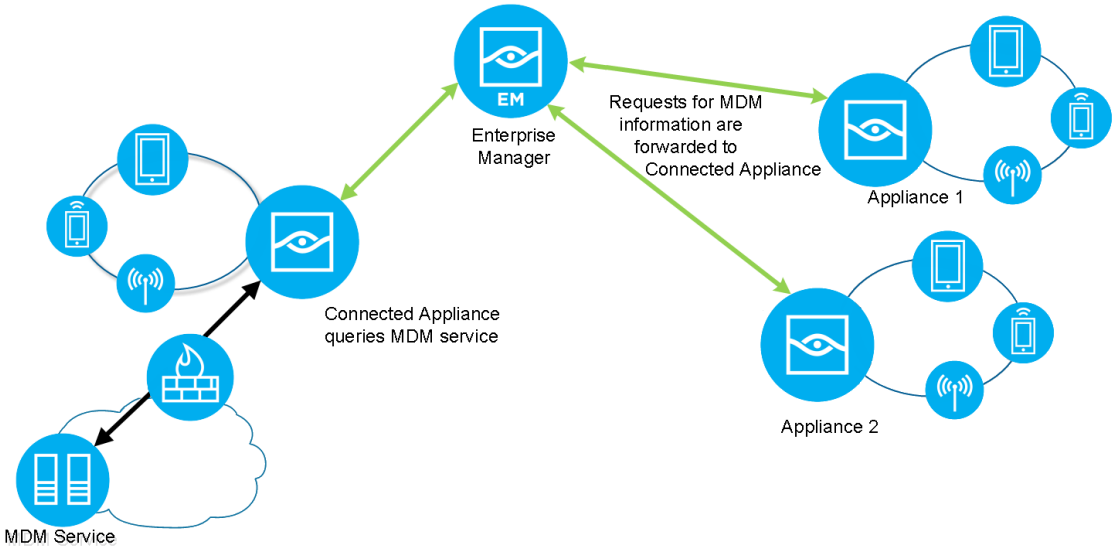
About this Module

Integration with the Forescout platform lets you deliver a comprehensive MDM solution that provides powerful monitoring and enforcement capabilities not available when working solely with the MaaS360 solution. Use Forescout eyeExtend for IBM MaaS360 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.
- Unified network access control policy enforcement options:
  - Allow compliant and managed devices on the network.
  - Limit network access based on device type, device ownership, time of day, and device compliance. The limited access network can allow 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 completely.
- Device tagging at the MaaS360 console, based on the Forescout platform's detections.
- Enhancement of the Forescout platform inventory by populating it with MaaS360 information.

How it Works

Forescout eyeExtend for IBM MaaS360 queries the MaaS360 Cloud Service for device attributes, for example, core attributes, security and compliance information, hardware inventory, and network information. All MaaS360 queries are performed by a single CounterACT® Appliance that is designated for this purpose. This designated CounterACT Appliance, the *MaaS360 Connected Appliance*, retrieves information from other CounterACT Appliances and the Enterprise Manager and forwards the information to the MaaS360 Cloud Service. Similarly, the MaaS360 Connected Appliance retrieves information from the MaaaS360 service and forwards it to other CounterACT Appliances and to the Enterprise Manager.



Continuous Query Refresh

MaaS360 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 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 Forescout platform 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 module must learn endpoint MAC addresses in order to initiate the query process.

Offsite Device Management

The module leverages integration with MaaS360 to manage devices even when they are not in the corporate network. The module retrieves updated host information for offsite devices through the MaaS360 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 MaaS360:

- iOS
- Android

- BlackBerry
- Windows Mobile
- Windows Phone
- Symbian

The following devices are supported by Forescout eyeExtend for IBM MaaS360:

- iOS
- Android

For exact operating system version support, refer to the MaaS360 documentation: http://updates.forescout.com/online/help/mdm/ForeScout_MDM_doc.pdf

Supported Network Infrastructure

MaaS360 supports devices connected to a network via a WiFi connection.

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See Requirements.
2. Verify the MDM Web Service Setup.
3. Install the Module.
4. Configure the Module.
5. Test Module Communication with the Service.
6. Create Forescout platform policies that detect, manage and remediate devices. See Create MaaS360 Policies Using Templates and Work with the Forescout Platform's Policies.
7. Connect to the Forescout MaaS360 Console to configure device policies: http://mdm.forescout.com/login

Refer to the following documents for technical information about the Forescout MDM solution. http://updates.forescout.com/online/help/mdm/ForeScout_MDM_doc.pdf

Requirements

This section describes system requirements and recommendations.

- Forescout Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements
- Registration and Activation Requirements
- Networking Requirements
- Endpoint Requirements

- Additional Deployment Recommendations

Forescout Requirements

This module requires the following Forescout release:

- Forescout version 8.1 or 8.2.
- A module license for Forescout eyeExtend for IBM MaaS360. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- 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.

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.

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. 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*.
- **Flexx Licensing**. Refer to the *Flexx Licensing How-to Guide*.

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

Registration and Activation Requirements

Register for access to the MaaS360 Cloud Service at: http://mdm.forescout.com

The MaaS360 Cloud Service is available as a 30-day free trial. After registering, you are sent a confirmation email; ***keep this email for future reference*** as it provides information required for configuring the MaaS360 Module.

Networking Requirements

The following ports must be open on enterprise firewalls to support communication between the Forescout platform and the MaaS360 service:

- 443/TCP.
- The port used to communicate with a proxy server (if one is used). Specify this port when you configure the module. See Configure the Module and Test Module Communication with the Service.

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.

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.

Verify the MDM Web Service Setup

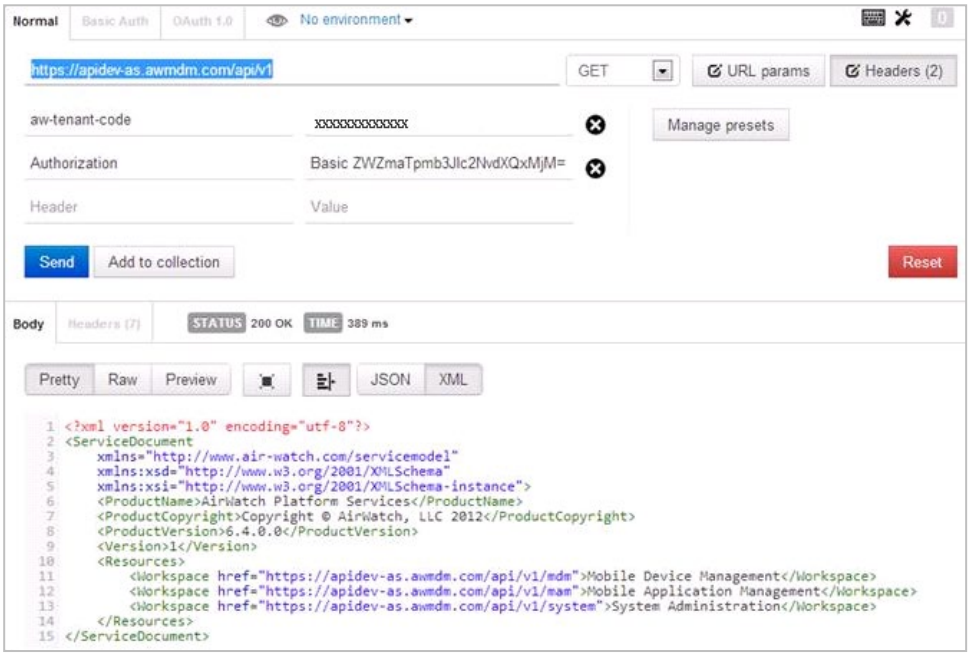
This section describes how to verify that the Web service is properly set up and that the MaaS360 console supports Web services.

To verify the setup:

1. Install the Firefox *RESTClient* plugin from the following URL: http://addons.mozilla.org/en-US/firefox/addon/restclient/
2. Launch the *RESTClient* plugin by selecting **Tools -> RESTClient.**
3. In the REST client user interface, enter the URL of the REST API on the MaaS360 server.

   The provided URL must be the same as the **MaaS360 Web Service URL Name** that is defined. See Configure the Module.
4. Verify that you have defined user authentication using MaaS360 credentials.
5. Select **Send**.

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



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.

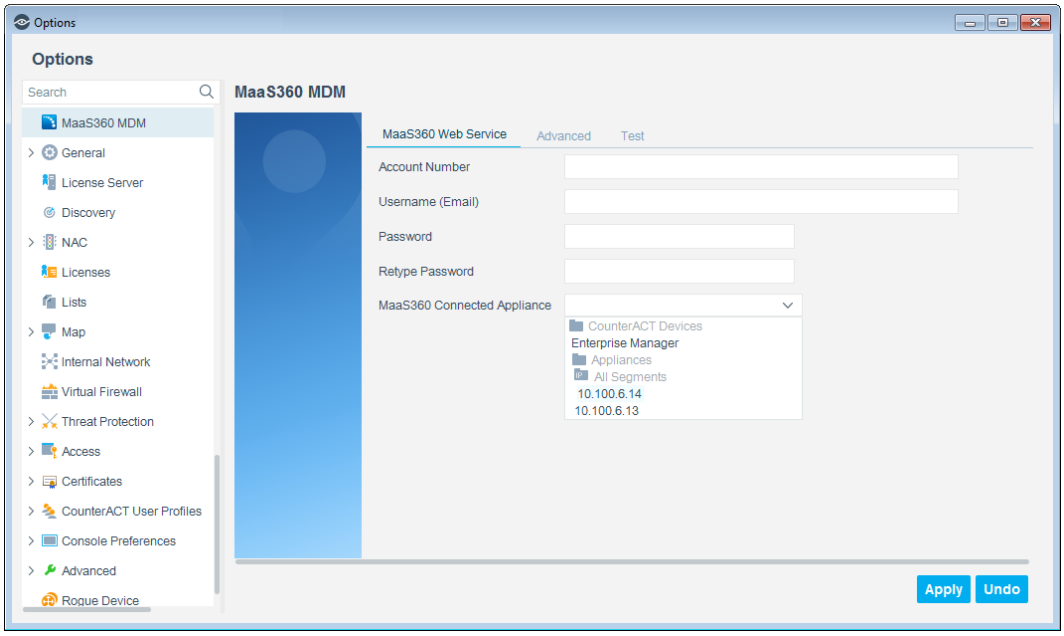
Once installed, the module automatically adds an HTTP Redirect exception to the CounterACT NAC Redirect Exception list. CounterACT NAC HTTP redirect exceptions are designed to ensure users can access business essential Internet sites or important files on the Internet while allowing required HTTP blocking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

Configure the Module

After Forescout eyeExtend for MaaS360 is installed, configure the module to communicate with the MaaS360 Cloud Service.

To configure the module:

1. In the Console, select **Options** from the **Tools** menu.
2. Select **Modules**.
3. Select **MaaS360 MDM** from the Options pane and then select **Configure**.

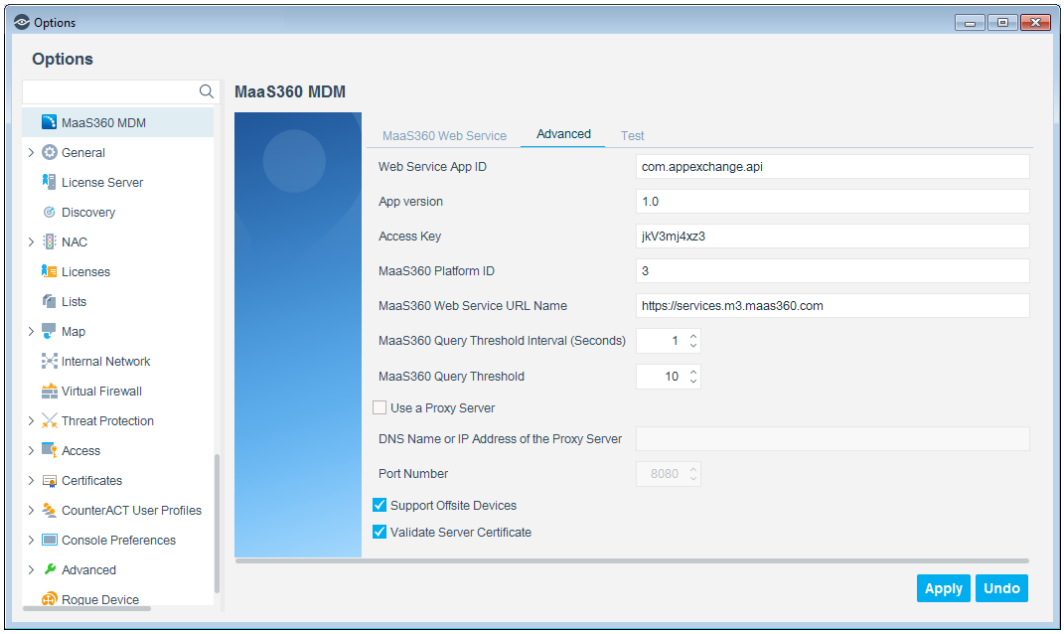


For the required information, refer to the confirmation email you received after registering at http://mdm.forescout.com for access to the MaaS360 Cloud Service.

4. Configure the following settings:

Account Number	Enter the account number. This information is used in the Manageability template, HTTP notification actions when redirecting endpoint Web sessions to the MDM enrollment site. See Create a MaaS360 Enrollment Policy for details.
Username (Email)	Enter the username.
Password	Enter the password.
Retype Password	Re-enter the password to verify it.
MaaS360 Connected Appliance	Select the name of the Appliance to serve as a proxy between the MaaS service and the Enterprise Manager and enterprise Appliances. The CounterACT device listed here is the only device that communicates directly with the MaaS360 Cloud Service. An Enterprise Manager may not be selected here.

5. Select the Advanced tab.



If you are upgrading from a previous version of the module, the default values displayed reflect your existing service settings. Use the existing values.

6. Configure the following settings:

Web Service App ID	Enter the Web service application ID or edit the default. The default is web.services.forescout.
App version	Enter the application version or edit the default. The default value is 1.0.
Access Key	Enter the access key or edit the default. The default is 3CMjCM4nsg.
MaaS360 Platform ID	Enter the MaaS360 platform ID or edit the default. The default value is 3.
MaaS360 Web Service URL Name	Enter the MaaS360 Web service URL name or edit the default.
MaaS360 Query Threshold Interval (Seconds)	Specify how frequently the module queries the MaaS360 Cloud Service.
MaaS360 Query Threshold	Define the maximum number of query requests to the MaaS360 Cloud Service per threshold interval (defined in the previous field).
Use a Proxy Server	Select this option if there is a proxy between the MaaS360 Connected Appliance and the MaaS360 Cloud Service.
DNS Name or IP Address of the Proxy Server	Enter the DNS name or the IPv4 address of the proxy server.
Port Number	Enter the required proxy server port.

Support Offsite Devices	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.
Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*.

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

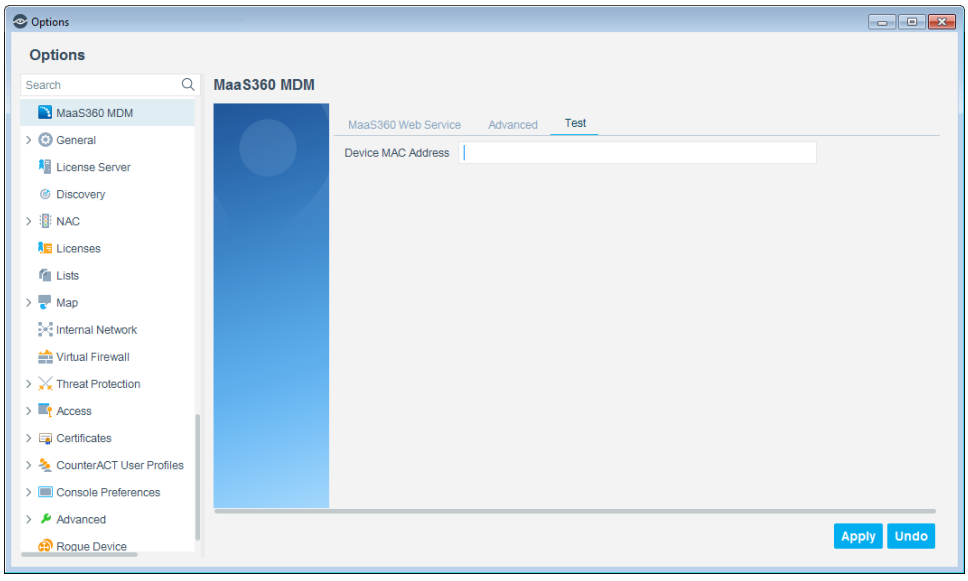
The best practice is to perform a **Test** after setting up a connection. See Test Module Communication with the Service.

Test Module Communication with the Service

Test the module communication with the MaaS service.

To test communication:

1. In the MaaS360 MDM pane, select the Test tab.



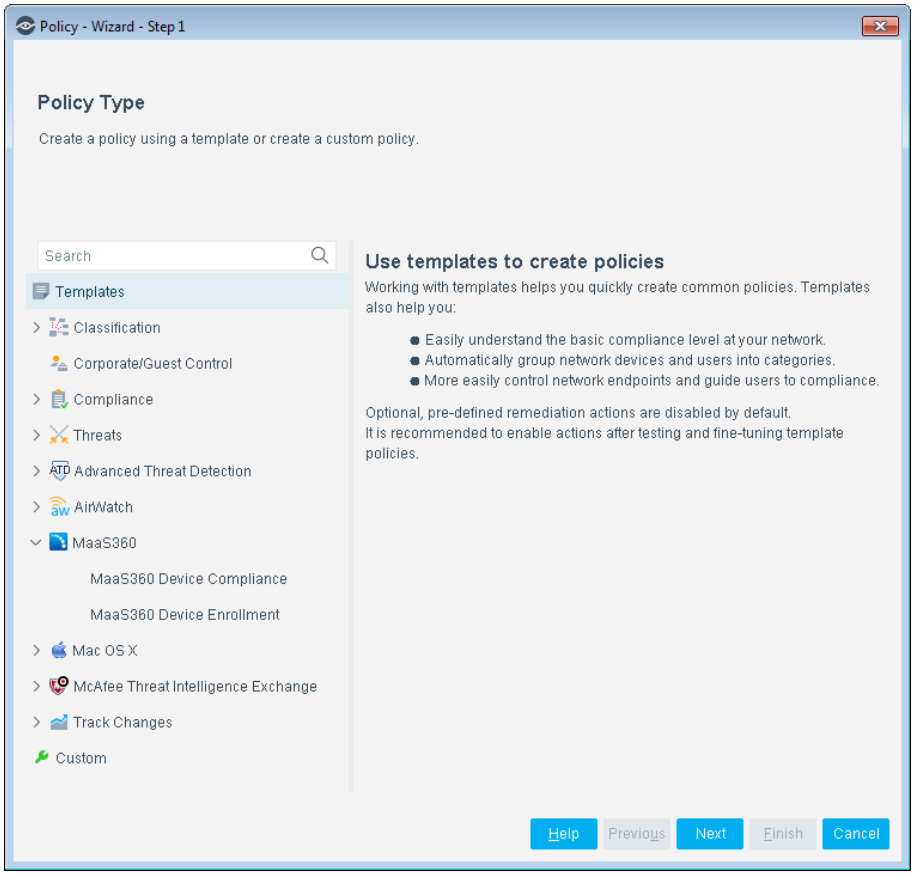
2. In the **Device MAC Address** field, enter the MAC address of the device to test module communication with the MaaS service. Do not enter colons. Use lower case characters.
3. Select **Apply**.

Create MaaS360 Policies Using Templates

This section describes how to use FireEye HX templates to create policies to detect and manage endpoints. Refer to the following sections:

- Create a MaaS360 Enrollment Policy to detect corporate hosts not enrolled with the MaaS360 service, and prompt 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 may have already been created, and the existing version of the policy will be retained.
- Create a MaaS360 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. See the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.



Create a MaaS360 Enrollment Policy

Use the MaaS360 Enrollment Policy Template policy to create a policy that detects corporate devices that have not enrolled with the MaaS360 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

Prior to running 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 MaaS360 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 MaaS360 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.

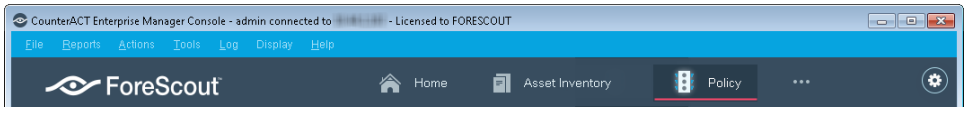
- If MDM services are deployed by geographical region or network segment, see Which Endpoints Are Inspected – Policy Scope.
- To add a general rule that checks for previously enrolled endpoints, see Detecting and Handling Devices Not Qualified for Enrollment.

Create an Enrollment Policy

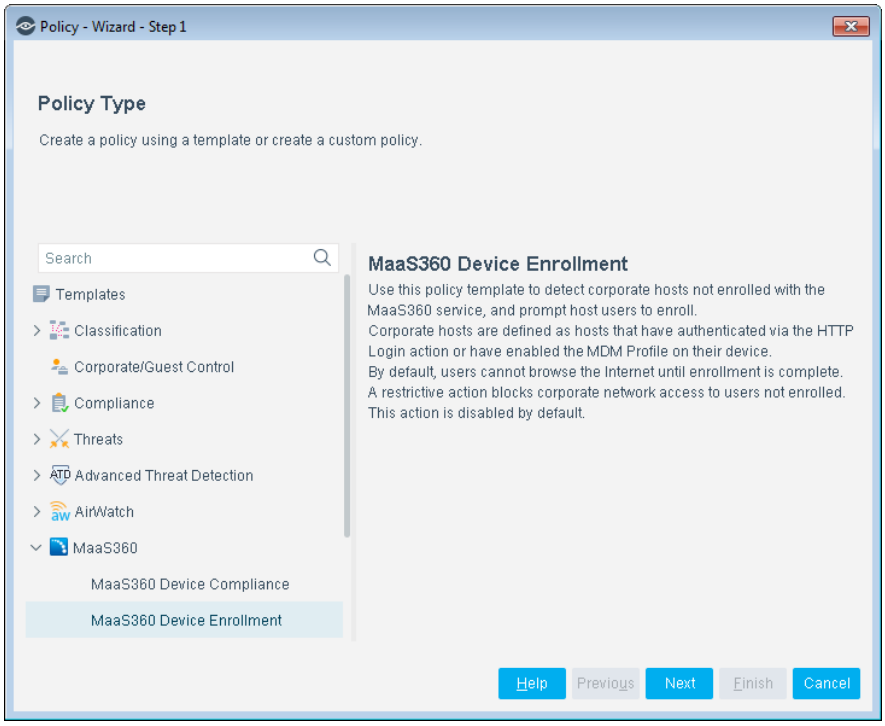
This section describes how to use this template to create a MaaS360 Device Enrollment policy.

To create a policy:

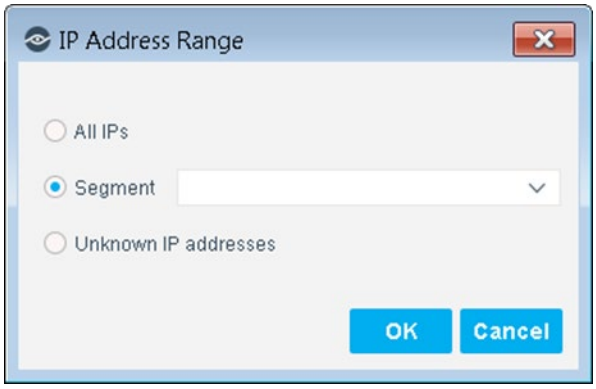
1. In the Console, select **Policy**.



2. Select **Add**. The Policy Wizard opens.
3. Select **MaaS360** and then select **MaaS360 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.



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** in the IP Address Range dialog box.
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.

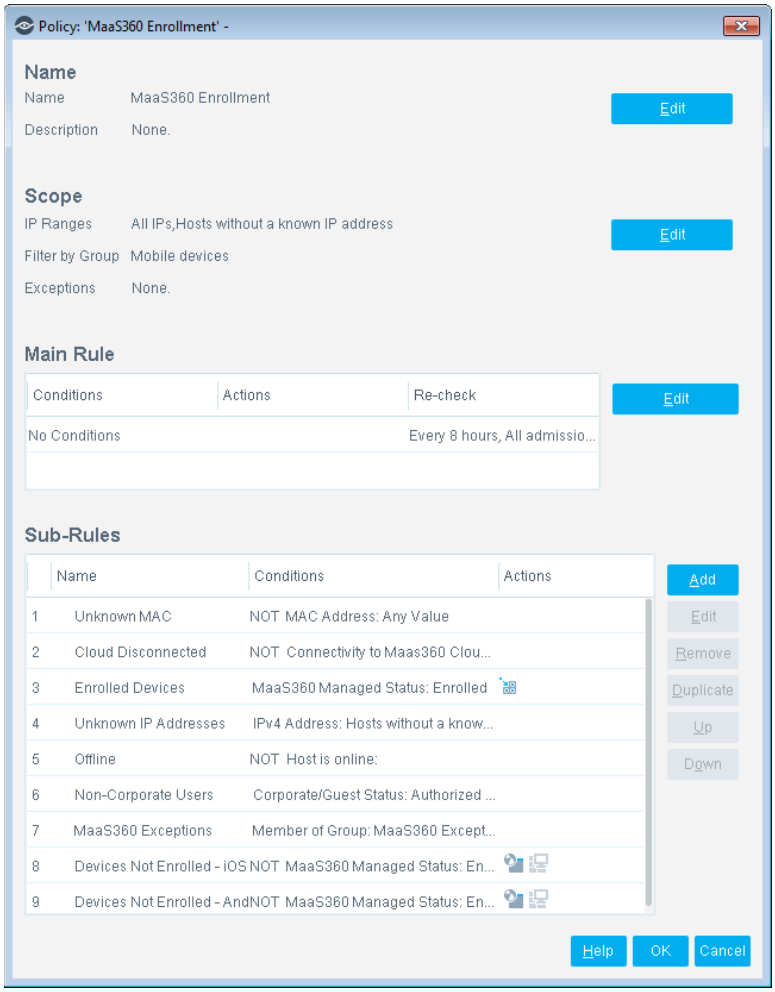
10. Select **Finish**. The policy is created.

Which Endpoints Are Inspected – Policy Scope

By default, MaaS360 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 MaaS360 Device 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.

The policy sub-rules filter situations and endpoints for which MaaS360 enrollment is not applicable. The final sub-rules enroll qualified mobile devices in the MaaS360 service.

Detecting and Handling Devices Not Qualified for Enrollment

The initial sub-rules of the policy detect and bypass devices that are not candidates for enrollment, for example, devices not part of the corporate domain, or devices listed in the MaaS360 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 *MaaS360 Enrolled Devices* group.

1. **Unknown MAC** – The Forescout platform queries MaaS360 for host information based on the MAC Address of the device. If no MAC Address is known for an endpoint, the MaaS360 service cannot be used to manage the device.
2. **MaaS360 Server Disconnected** – This rule tests for the Forescout platform's connectivity with the MaaS360 web service, which is necessary for enrollment. This rule suspends evaluation of the policy if there is no connectivity with the MaaS360 service platform.
3. **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.
4. **Enrolled Device** – This rule detects devices already enrolled in the MaaS360 service.

    The Add to Group action adds devices that match this rule to the *MaaS360 Enrolled Devices* group.

   No further enrollment action is necessary for these endpoints, and their evaluation ends at this rule.
5. **MaaS360 Exceptions** – Devices listed in the *MaaS360 Exceptions* group are excluded from enrollment.
6. **Offline** – Enrollment cannot be implemented if the device has gone offline.
7. **Non-Corporate Users** – By default, only corporate user devices are enrolled in the MaaS360 service.

Detecting and Handling Devices Qualified for Enrollment

The following sub-rules detect devices that are qualified for enrollment in the MaaS360 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 *MaaS360 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 *MaaS360 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.

 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 MaaS360 Enrolled Devices group. If the enrollment interaction completes successfully, rule 4 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 may have already been created, and the existing version of the policy will be retained.

If this policy does not already exist, the MaaS360 Device Enrollment Policy template creates this policy in addition to the MaaS360 Enrollment policy.

Prerequisites

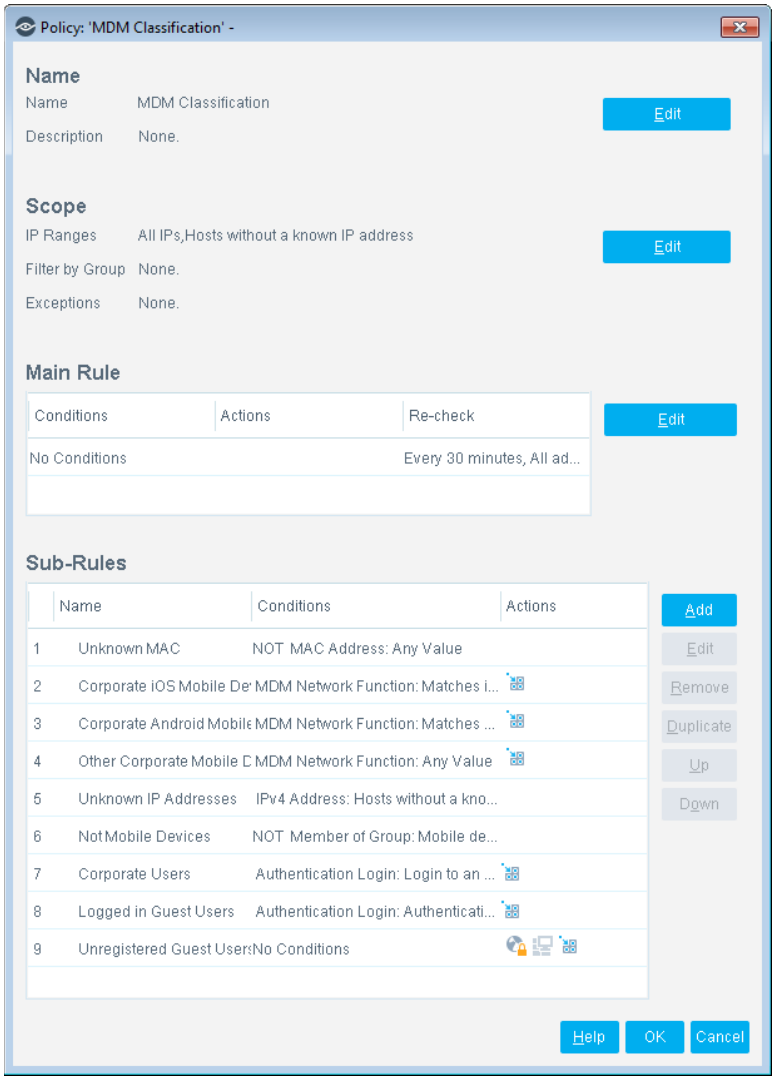
This policy sorts endpoints based on previous classification by the Primary Classification and Mobile Classification policies, and corporate/guest status as determined by Corporate/Guest Control policies. Run these policies before you run this policy.

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 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 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.

The policy sub-rules perform the following evaluations:

- 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 condition.

- **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.

1. **Corporate iOS Mobile Devices**
2. **Corporate Android Mobile Devices**
3. **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 and 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.

1. **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 are detected by the previous rules, even if they are currently outside the corporate network.)
2. **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.

1. **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.
2. **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.

3. **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 information about enabling this action.

Create a MaaS360 Device Compliance Policy

Use the MaaS360 Device Compliance policy template to create a policy that verifies device compliance with the Forescout platform network requirements and MaaS360 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.

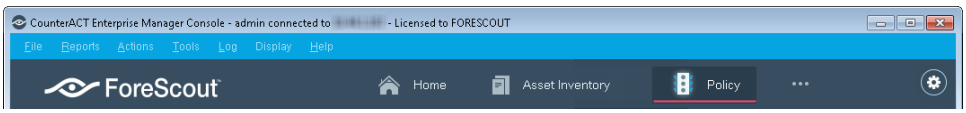
You must create and run a policy based on the MaaS360 Device Enrollment template ***before*** you use this template to create policies. This template uses groups and other information created by the MaaS360 Device Enrollment policy.

Create a Device Compliance Policy

This section describes how to use the template to create a MassS360 device compliance policy.

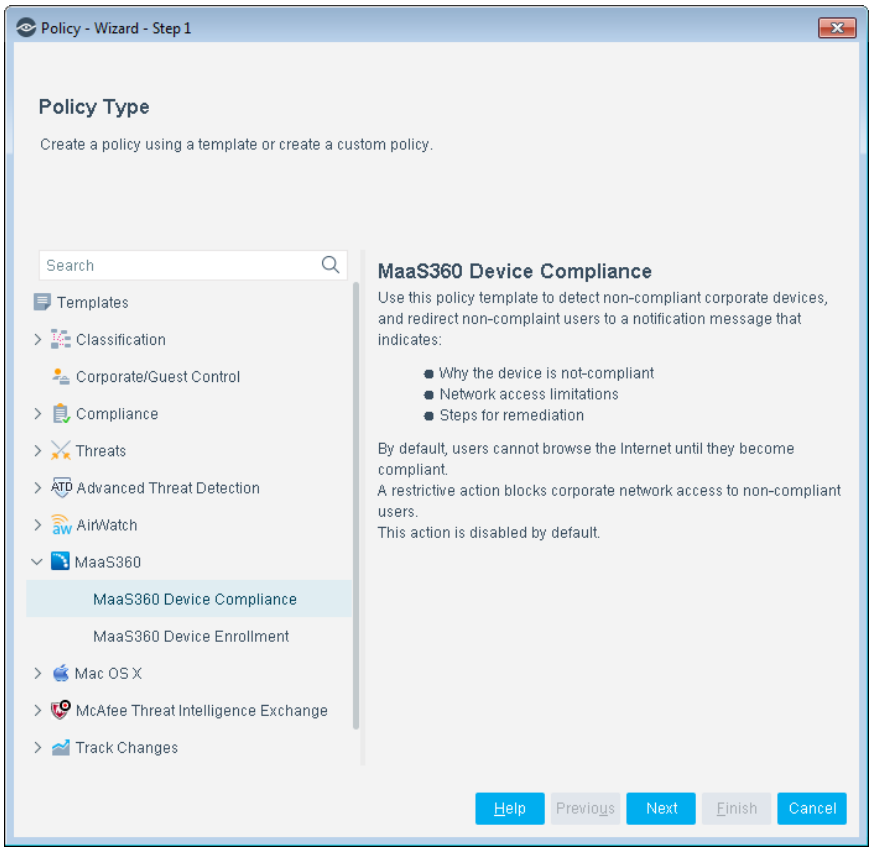
To create a policy:

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

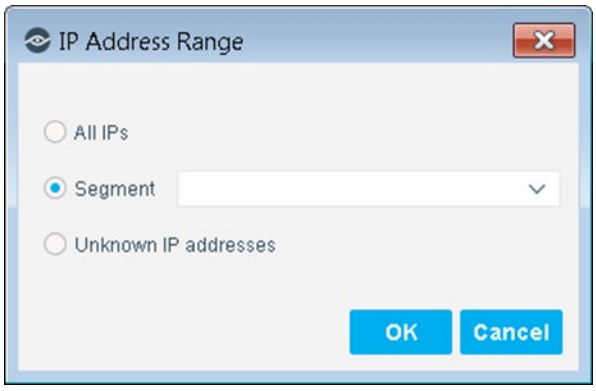


2. Select **Add**. The Policy Wizard opens.

3. Select **MaaS360** and then select **MaaS360 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. 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 policy scope. This is equivalent to selecting the **Unknown IP addresses** in the IP Address Range dialog box.
8. Select **Next**. The Sub-Rules pane opens.
9. Select **Finish**. The policy is created.

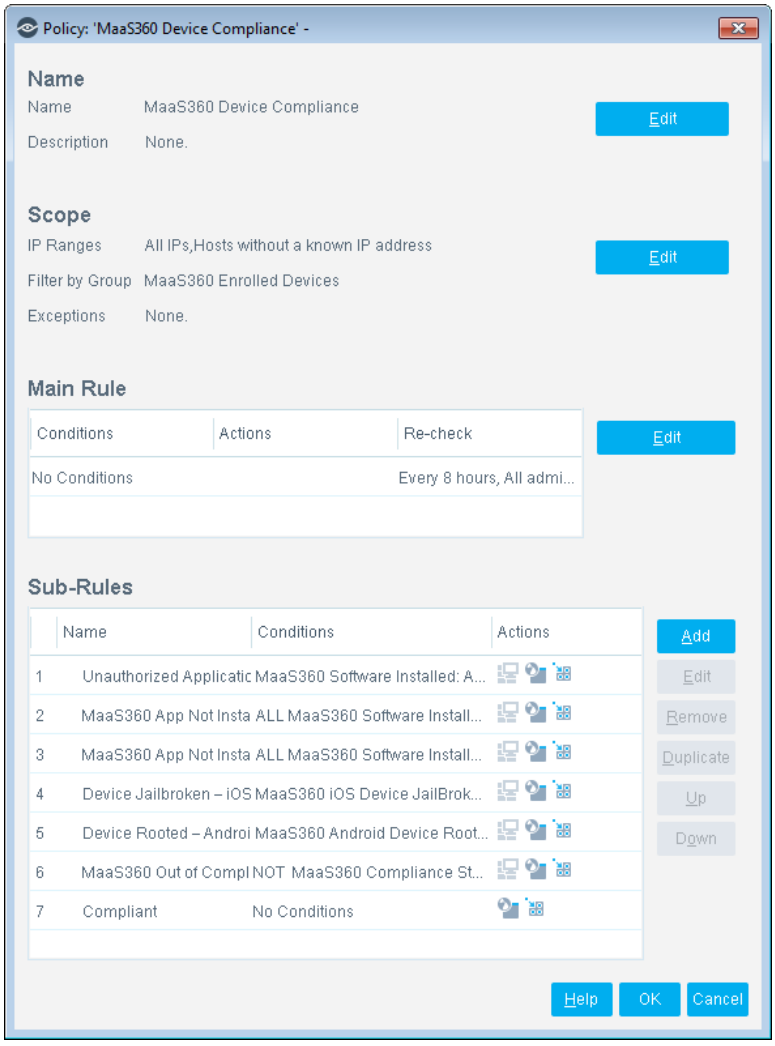
Which Endpoints Are Inspected – Policy Scope

Policies based on this template inspect only devices previously enrolled in the MaaS360 service. The *MaaS360 Enrolled Devices* group is used to filter the scope of this policy.

Because notification and enrollment use HTTP redirection actions, do not select 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.

The policy sub-rules 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 **MaaS360 Software Inventory** host property against the MaaS360 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 *MaaS360 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 MaaS360 Service App

The following rules examine applications listed in the **MaaS360 Software Inventory** host property to identify previously enrolled devices that do not have the MaaS360 service enrollment package installed.

2. **MaaS360 App Not Installed – iOS**
3. **MaaS360 App Not Installed – Android**

When a device matches one of these rules:

An HTTP Notification action redirects users to a service enrollment interaction.

The Add to Group action assigns the device to the *MaaS360 App Not Installed – iOS* or the *MaaS360 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 **MaaS360 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 *MaaS360 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 MaaS360 Service Compliance

5. **MaaS360 Out of Compliance** – This rule tests the **MaaS360 Compliance Status** host property to detect devices that do not meet compliance criteria of the MaaS360 service. When a device matches one of these rules:

   An HTTP Notification action informs the user that the device does not meet MaaS360 service compliance criteria, and its access to the corporate network is restricted.

   The Add to Group action assigned the device to the *MaaS360 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 details.

6. **MaaS360 Compliant** – Endpoints that did not match previous rules are considered to be compliant. When a device matches one of these rules:

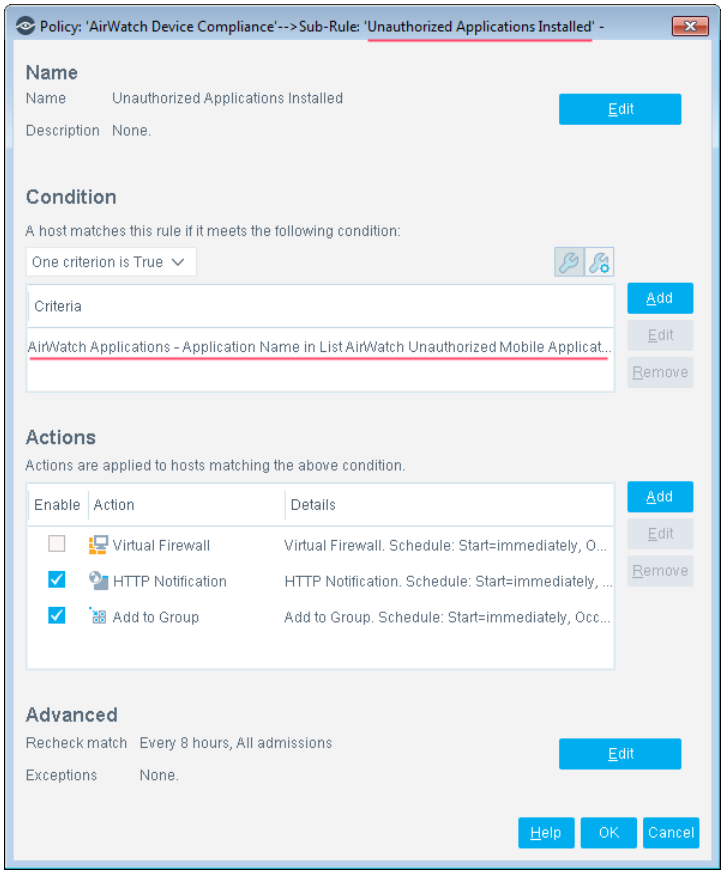
   An HTTP Notification action informs the user that the device is compliant, and prompts the user to continue browsing in the corporate network.

   The Add to Group action assigns the device to the *MaaS360 Compliant Devices* group.

Add Applications to the Unauthorized Application List

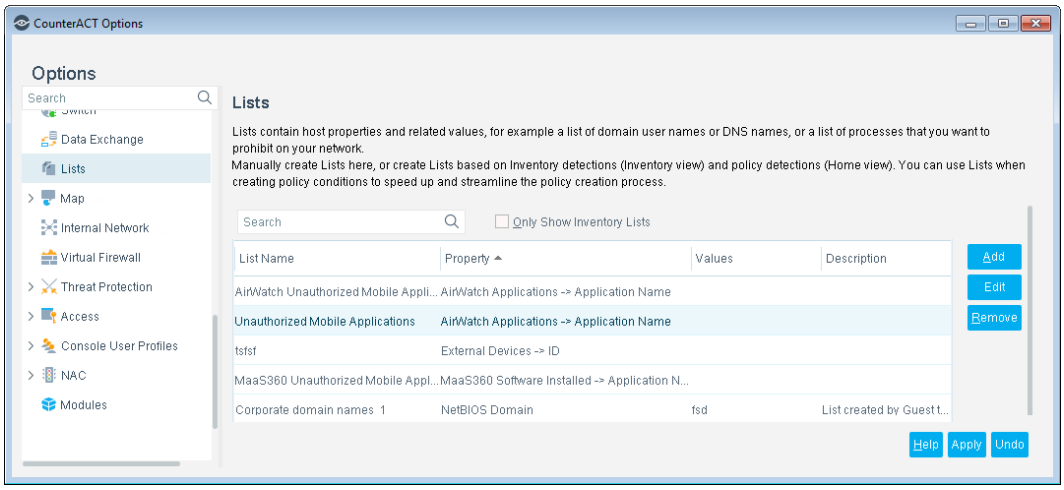
In order to work with the MaaS360 Compliance Policy template, you must compile a list of applications that you want to prohibit on your network.

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.

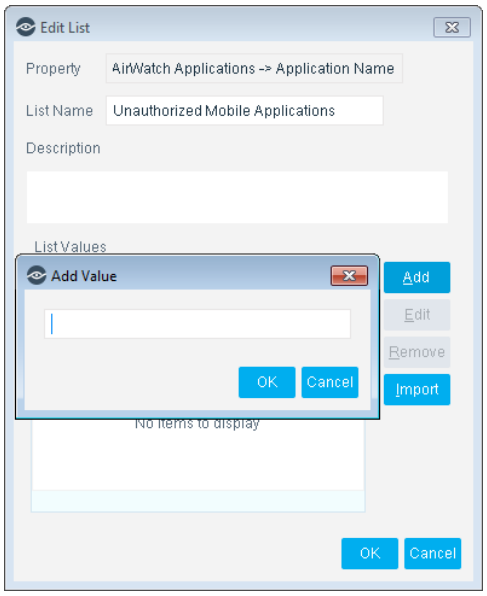


To prohibit an application:

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



2. Select the **Unauthorized Mobile Application** entry for MaaS360.
3. Select **Edit**. The Edit List dialog box opens.
4. Select **Add**.



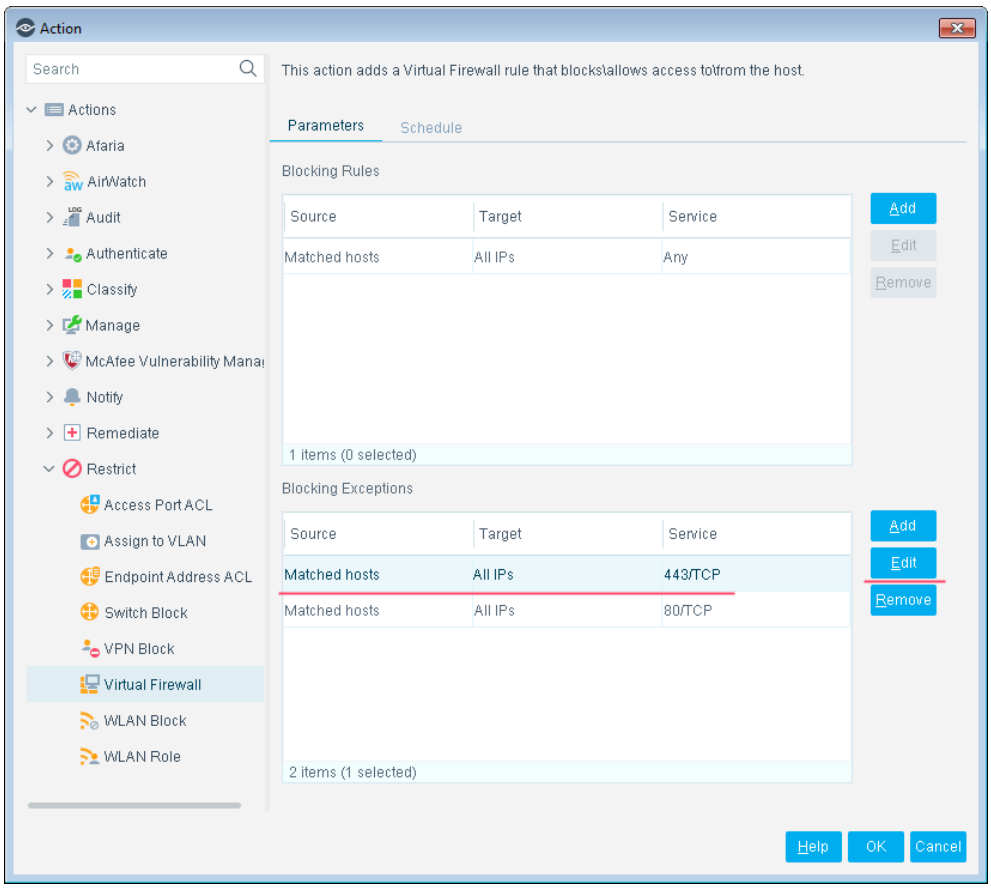
5. Enter the name of an application that you want to prohibit and then select **OK**.
6. Repeat steps 4 and 5 for other prohibited applications.
7. (Optional) Enter a description of the list in the **Description** field.
8. Select **OK**. The unauthorized applications are added in the Values column in the Lists pane.

Configure Virtual Firewall Actions

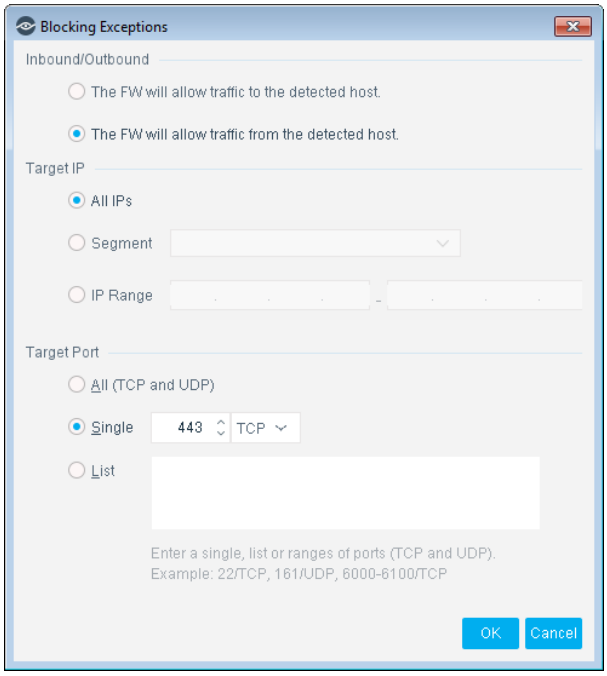
Policy templates include optional Virtual Firewall actions that block user access to the corporate network. These actions are disabled by default in policy templates. If you enable the Virtual Firewall action, edit action settings to permit MDM service communication with the device.

To configure virtual firewall actions:

1. Open a policy rule, then 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 ports required by the module. See Networking Requirements.

Display Asset Inventory Data

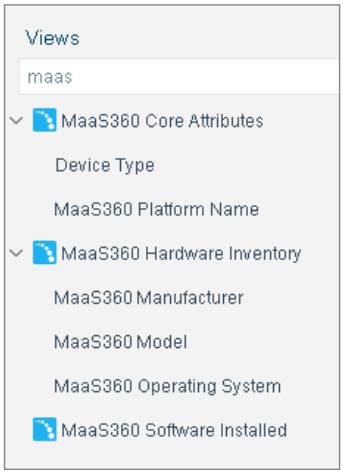
Use the Asset Inventory to view a real-time display of MaaS360 device network activity at multiple levels, for example, software installed, core attributes, or hardware information.

The Asset Inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific
- View MaaS360 devices that have been detected with specific attributes
- Easily track MaaS360 device activity
- Incorporate inventory detections into policies

To access the Asset Inventory:

1. In the Console, select **Asset Inventory**.
2. In the Views pane, go to the MaaS360 entries.



The following information is available:

- MaaS360 Core Attributes: Device Type, MaaS360 Platform Name
- MaaS360 Hardware Inventory: Manufacturer, Model, Operating System.
- MaaS360 Software Installed

Refer to *Working on the Console > 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, the module uses the MaaS360 service platform to retrieve updated host information and implement the Forescout platform policy actions.

To configure support for the 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 MaaS360 templates. See Create MaaS360 Policies Using Templates.

Consider the following when you create 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 MaaS360-specific actions provided by this module are supported on offsite devices. See Tag MaaS360 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.

Work with the Forescout Platform's Policies

This section describes how to use the Forescout platform's policies to detect and control MaaS360 devices. Create or edit a policy and use policy conditions to detect these devices with specific properties.

To create a policy:

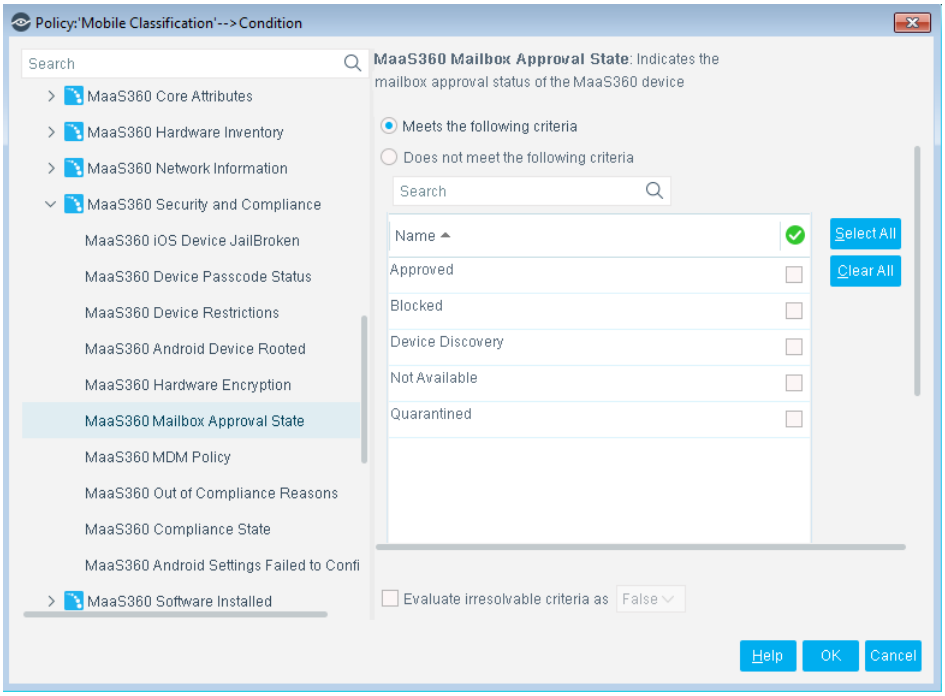
1. Log in to the Console and select **Policy**.
2. Create or edit a policy.

Detect MaaS360 Devices – Policy Properties

The Forescout platform policy conditions and properties let you instruct the Forescout platform which MaaS360 devices to detect.

In the conditions screen, expand the MaaS360 folder in the Properties tree to use MaaS360 properties in a policy condition. An extensive range of properties can be detected. The categories include:

- Primary Classification
- Core Attributes
- Security and Compliance
- Hardware Inventory
- Network Information
- Additional Information



Primary Classification

MDM Network Function	Indicates the mobile operating system of an MDM managed endpoint. This property is common to all MDM Integration modules, and are displayed in the Classification folder of the Properties tree.

Core Attributes

Device Type	
MaaS360 Device ID	Indicates the MaaS360 device ID.
MaaS360 Device Name	Indicates the MaaS360 device name.
MaaS360 Device Online	Indicates if the MaaS360 device is online.
MaaS360 Device Status	Indicates the active status of the MaaS360 device.
MaaS360 Last Reported	Indicates the date/time of the last reported event on a host.
MaaS360 Managed Status	Indicates the managed status of the MaaS360 device: ▪ Enrolled ▪ Not Active ▪ Not Enrolled ▪ Pending Control Removal ▪ User Removed Control
MaaS360 Platform Name	Indicates the platform on which the MaaS360 device is running.

	▪ Android ▪ iOS
MaaS360 User Name	Indicates the user name associated with the MaaS360 device.

Security and Compliance

MaaS360 Android Device Rooted	Indicates if an enrolled Android device is rooted.
MaaS360 Android Settings Failed to Configure	Indicates if specific settings are not configured on an Android host.
MaaS360 Compliance State	Indicates the MaaS360 compliance state of the host: ▪ Compliant ▪ Not Available ▪ Not Compliant
MaaS360 Device Passcode Status	Indicates the MaaS360 device passcode status: ▪ Compliant ▪ Not Available ▪ Not Compliant per Profiles ▪ Not Compliant ▪ Not Compliant per all Requirements ▪ Not Enabled ▪ Passcode Policy Configured ▪ Passcode Policy Not Configured ▪ Pending Compliance Confirmation
MaaS360 Device Restrictions	Indicates restrictions configured on the MaaS360 device: ▪ Allow Installing of Applications ▪ Allow Screen Capture ▪ Allow Use of Camera ▪ Allow Use of YouTube ▪ Allow Use of iTunes Music Store ▪ Allow Use of Safari
MaaS360 Hardware Encryption	Indicates if specific hardware encryption values were detected on the host.
MaaS360 MDM Policy	Indicates an MDM policy applied to the MaaS360 device.
MaaS360 Mailbox Approval State	Indicates the mailbox approval status of the MaaS360 device: ▪ Approved ▪ Blocked ▪ Device Discovery ▪ Not Available ▪ Quarantined

MaaS360 Out of Compliance Reasons	Indicates if specific out-of-compliance reasons were detected on the host.
MaaS360 iOS Device JailBroken	Indicates if the MaaS360 device is jailbroken.

Hardware Inventory

MaaS360 Custom Attributes	Indicates devices that were detected with specific MaaS360 device attributes or values.
MaaS360 Email Address	Indicates the Email Address of the MaaS360 device.
MaaS360 Manufacturer	Indicates the manufacturer of the MaaS360 device.
MaaS360 Model	MaaS360 Model
MaaS360 Operating System	Indicates the Operating System running on the MaaS360 device.
MaaS360 Ownership	Indicates the ownership of the MaaS360 device.

Network Information

MaaS360 ICCID	Indicates an ICCID value detected on the MaaS360 device.
MaaS360 Phone Number	Indicates the phone number associated with the MaaS360 device.

Additional Information

MaaS360 Software Installed	Indicates if specific software is installed on the MaaS360 device.
Connectivity to MaaS360 Cloud	Indicates if the Forescout platform is connected to the MaaS360 cloud.
MaaS360 Listed in Service	Indicates if the device is listed in the MaaS360 service.

Tag MaaS360 Devices – Policy Actions

This section describes Forescout actions you can use to tag MaaS360 devices.

- Custom Attribute Value Action
- Refresh Device Information Action

Custom Attribute Value Action

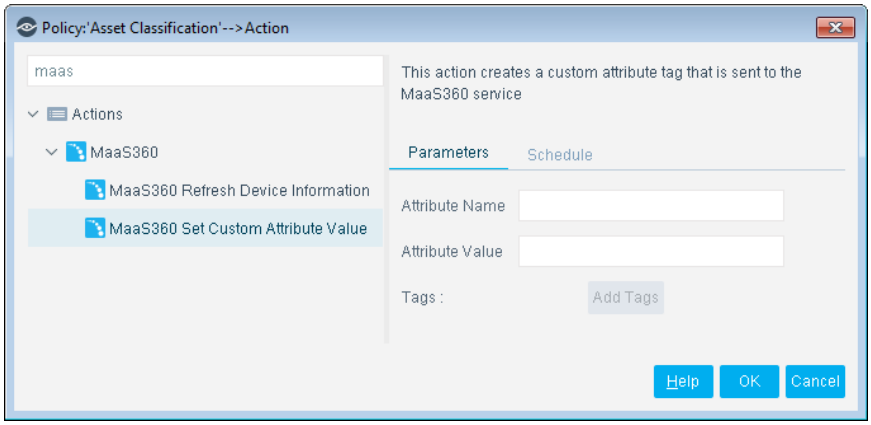
Detect devices using a Forescout platform policy and tag the devices with a user-defined *Attribute Name* and *Attribute Value*. This information is sent to the MaaS360

Cloud Service. For example, use the Forescout platform to detect devices that are resolved as guests and tag them as:

Attribute Name: East Coast Office

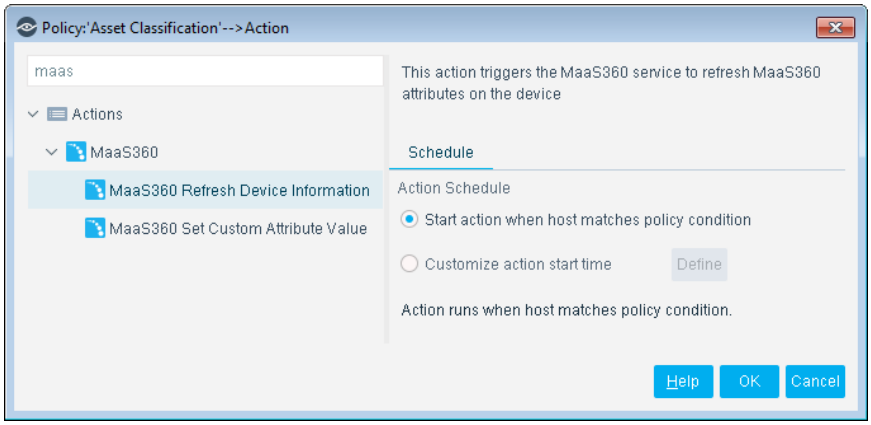
Attribute Value: Guest

Devices are displayed as *East Coast Office Guests* at the MaaS360 Console.



Refresh Device Information Action

The Refresh Device Information action triggers the MaaS360 Cloud Service to refresh MaaS360 attributes on the device.



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.