CounterACT™ MaaS360 Plugin
Configuration Guide

Version 1.7.0 and Above
# Table of Contents

- **About MaaS360 Integration** 4
- **Additional Documentation** 4
- **About this Plugin** 4
  - How it Works 5
  - Continuous Query Refresh 5
  - Offsite Device Management 6
  - Supported Devices 6
  - Supported Network Infrastructure 6
  - What to Do 7
- **Requirements** 7
  - CounterACT Software Requirements 7
  - ForeScout Module License Requirements 7
    - Requesting a License 8
    - More License Information 8
  - Registration and Activation Requirements 8
  - Networking Requirements 9
  - Endpoint Requirements 9
  - Additional Deployment Recommendations 10
- **MDM Web Service Verification** 10
- **Install the Plugin** 11
- **Configure and Test the Plugin** 12
  - Configure the Plugin 12
  - Test Plugin Communication with the Service 14
- **Run MaaS360 Policy Templates** 15
  - MaaS360 Enrollment Policy Template 15
    - Prerequisites 16
    - Multiple MDM Service Enrollment 16
    - Running the Template 16
    - Which Endpoints are Inspected - Policy Scope 19
    - How Devices are Detected and Handled 19
  - MDM Classification Policy Template 21
    - Prerequisites 21
    - Which Endpoints are Inspected - Policy Scope 21
    - How Devices are Detected and Handled 21
  - MaaS360 Device Compliance Policy Template 23
    - Prerequisites 23
    - Running the Template 24
Which Endpoints are Inspected - Policy Scope ........................................... 26
How Devices are Detected and Handled...................................................... 27
Adding Applications to the Unauthorized Application List ................................. 28
Configuring Virtual Firewall Actions .............................................................. 30

Displaying Inventory Data........................................................................ 31
Managing Offsite Devices ....................................................................... 32

Working with CounterACT Policies .............................................................. 33
Detecting MaaS360 Devices - Policy Properties ............................................. 33
Asset Classification ................................................................................ 34
Core Attributes ..................................................................................... 34
Security and Compliance ........................................................................ 35
Hardware Inventory ............................................................................... 36
Network Information .............................................................................. 36
Additional Information ........................................................................... 36
Tag MaaS360 Devices - Policy Actions ......................................................... 37
Custom Attribute Value Action ................................................................ 37
Refresh Device Information Action ............................................................ 37

Additional CounterACT Documentation ...................................................... 37
Documentation Portal ................................................................................ 38
Customer Support Portal ............................................................................ 38
CounterACT Console Online Help Tools ..................................................... 38
About MaaS360 Integration

CounterACT/ MaaS360 integration helps IT administrators streamline the process to provision, manage and secure today’s expanding suite of smartphones and tablets, all from a single portal. CounterACT/MaaS360 integration yields an easy to use platform that includes all of the essential functionality for end-to-end management of mobile devices. You can secure and manage apps, docs, and devices for global organizations, and support both corporate and individual owned devices.

MaaS360 is available as both an on premise system and a cloud service. This means with a single unified security management and reporting system, you can ensure that your network is secured, regardless of the type of device a user may be carrying. Instead of implementing new security silos that are limited to mobile devices, you can extend your PC and network security systems to encompass mobile devices.

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

- **Secure all Mobile Devices**: supports 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**: provides workflows to discover, enroll, manage and report on personally owned devices as part of your mobile device operations.
- **Experience simple device enrollment and approval**: provides auto-quarantine for Exchange, and alerts IT personnel to approve all new devices. Additionally it provides for easy user self-enrollment via web, email or SMS.

Additional ForeScout MDM Documentation

Refer to the documents linked from the following file for more technical information about the ForeScout MDM solution.


About this Plugin

Integration with CounterACT lets you deliver a comprehensive MDM solution that provides powerful monitoring and enforcement capabilities not available when working solely with the MaaS360 solution. Use the MaaS360 MDM Plugin to complete the cycle of security by obtaining valuable capabilities:

- Automated real-time, continuous detection and compliance of mobile devices the moment they try to connect to your network, including unmanaged and unknown devices.
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.
- Tag devices at the MaaS360 console, based on CounterACT detections.
- Enhance CounterACT inventory by populating it with MaaS360 information.

How it Works
The MaaS360 Plugin 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 CounterACT Enterprise Manager and forwards the information to the MaaS360 Cloud Service. Similarly, the MaaS360 Connected Appliance retrieves information from the MaaS360 service and forwards it to other CounterACT Appliances and the CounterACT Enterprise Manager.

Continuous Query Refresh
MaaS360 query mechanisms recheck endpoint attributes at a static frequency—approximately once a day. However, after plugin installation, querying of endpoint properties is based on CounterACT policy recheck definitions that define the conditions under which to recheck hosts that match a policy. Specifically, you can specify:
- How often hosts are rechecked once they match a policy
- Under what conditions to carry out the recheck

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

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

**Offsite Device Management**

The plugin leverages integration with MaaS360 to manage devices even when they are not in the corporate network. The plugin 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 [Managing 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 the MaaS360 MDM Plugin:

- iOS
- Android


**Supported Network Infrastructure**

Devices connected to a network via a WiFi connection.
What to Do

To use the MaaS360 MDM Plugin, perform the following tasks:

1. Verify that you have met software and networking requirements. See Requirements.
2. Install, configure and test the plugin. See Install the Plugin and Configure and Test the Plugin.
3. Create CounterACT policies that detect, manage and remediate devices. See Run MaaS360 Policy Templates and Working with CounterACT Policies.
4. Connect to the ForeScout MaaS360 Console to configure device policies: http://mdm.forescout.com/login

Refer to the documents at the following location for more 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.

- CounterACT Software Requirements
- ForeScout Module License Requirements
- Registration and Activation Requirements
- Networking Requirements
- Endpoint Requirements
- Additional Deployment Recommendations

CounterACT Software Requirements

The following CounterACT releases can work with this plugin.

- CounterACT version 7.0.0 with Hotfix 1.3 and above.

ForeScout Module License Requirements

This plugin is packaged as a ForeScout Module, and requires a module license. When installing the plugin you are provided with a 90-day demo module license.

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

When the demo period expires, you will be required to purchase a permanent module license. In order to continue working with the plugin, you must purchase the license.
Demo license extension requests and permanent license requests are made from the CounterACT Console.

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

**Requesting a License**

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

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.

**More License Information**

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

**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 Plugin.
Networking Requirements

The following ports must be open on enterprise firewalls to support communication between CounterACT 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 plugin. See Configure and Test the Plugin.

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

Endpoint Requirements

Queries to MDM services are based on endpoint MAC addresses. As such, CounterACT must learn endpoint MAC addresses in order to initiate the query process. MAC addresses can be learned from the following sources:

- Wireless plugin (Client table)
- Packet-Engine (ARP and DHCP traffic)
- L3 switches (ARP table)
Additional Deployment Recommendations

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

MDM Web Service Verification

This section describes how to verify that the Web service is properly set up. To verify setup, test REST API calls on the MaasS360 Server by verifying that the MaasS360 console supports Web services.

1. Install the Firefox RESTClient plugin from the following URL:
2. Launch the RESTClient plugin by selecting Tools -> RESTClient.
3. In the REST client user interface, enter the URL of the REST API on the MaasS360 server, as follows: https://services.fiberlink.com (default). The provided URL must be the same as the MaaS360 Web Service URL Name that will be defined in Configure the Plugin.
4. Verify that you have defined user authentication using MaasS360 credentials.
5. Select Send.

The REST client user interface displays the returned Response body; this information is provided in XML format.
Install the Plugin

This section describes how to install the MaaS360 Plugin.

**To install the plugin:**

1. Acquire a copy of the plugin in either one of the following ways:
   a. If you are installing a Beta release of this plugin, acquire the plugin .fpi file from your ForeScout representative or contact beta@forescout.com.
   b. Otherwise, navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.

2. Save the file to the machine where the CounterACT Console is installed.

3. Log in to the CounterACT Console and select Options from the Tools menu.


5. Select Install. The Open dialog box opens.

6. Browse to and select the saved plugin .fpi file.

7. Select Install.

8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.

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

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

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

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

Once installed, the plugin automatically adds 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 and Test the Plugin

This section describes how to configure and test the MaaS360 Plugin.

Configure the Plugin

Configure the plugin to communicate with the MaaS360 Cloud Service.

To configure the plugin:

1. In the CounterACT console, select Options from the Tools menu.
2. Select Plugins.
3. Select MaaS360 MDM from the Options pane and then select Configure.
4. Enter the following information about the MaaS360 Cloud Service:

   - Account Number (This information is used in the Manageability template, HTTP notification actions when directing endpoint Web sessions to the MDM enrollment site. See the MaaS360 Enrollment Policy for details.)
   - Username (Email)
   - Password
   - In the MaaS360 Connected Appliance drop-down list, select the name of an Appliance that will service as a proxy between the MaaS service and the Enterprise Manager and enterprise Appliances. The CounterACT device listed here is the only device that will communicate directly with the MaaS360 Cloud Service. An Enterprise Manager may not be selected here.

   For the information to enter, refer to the confirmation email you received after registering at http://mdm.forescout.com for access to the MaaS360 Cloud Service.
5. Select the Advanced tab. The following fields display default values:
   - **Web Service App ID**  
     Default: web.services.forescout
   - **App version**  
     Default: 1.0
   - **Access Key**  
     Default: 3CMjCM4ns
g   - **MaaS360 Platform ID**  
     Default: 3
   - **MaaS360 Web Service URL Name**  
     Default: https://services.fiberlink.com

   Edit the values as necessary.

   ⚠️ If you are upgrading from a previous version of the plugin, the default values displayed reflect your existing service settings. Use the existing values.
   - In the **MaaS360 Query Threshold Interval (Seconds)** field, specify the frequency that the plugin should query the MaaS360 Cloud Service.
   - In the **MaaS360 Query Threshold** field, define the maximum number of query requests to the MaaS360 Cloud Service per threshold interval (defined in the preceding field).
   - Select **Use a Proxy Server** if there is a proxy between the MaaS360 Connected Appliance and the MaaS360 Cloud Service.
   - Enter the IP address of the proxy server in the **DNS Name or IP Address of the Proxy Server** field.
   - Enter the required proxy server port in the **Port Number** field.
   - To manage mobile devices not in the Internal Network Range of the network, select the **Support Offsite Devices** option. The plugin retrieves updated host information for off-site devices through the service platform.
6. Select **Apply** to save configuration changes.

**Test Plugin Communication with the Service**

Test the plugin communication with the MaaS service.

**To test communication:**

1. Select the Test tab.

2. In the **Device MAC Address** field, type the MAC address of the device to test plugin communication with the MaaS service. Do not enter colons. Use lower case.
Run MaaS360 Policy Templates

This plugin provides the following policy templates to detect, manage and remediate mobile devices in a MaaS360 environment.

- The **MaaS360 Device Enrollment** policy template generates the following CounterACT policies:
  - **MaaS360 Enrollment Policy** - this policy detects corporate hosts not enrolled with the MaaS360 service, and prompts host users to enroll.
  - **MDM Classification Policy** – this policy classifies all mobile devices into groups. All plugins in the MDM Integration Module use this policy. If another plugin of this module is already installed, this policy was probably already created, and the existing version of the policy is retained.

- The **MaaS360 Device Compliance Policy Template** generates a policy that detects and remediates non-compliant devices.

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

### MaaS360 Enrollment Policy Template

Use this policy to detect 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

Before you run a policy based on this template, run policies based on the Asset Classification, Mobile Classification, iOS Classification and Android Classification templates. Policies based on these templates create groups and classify devices into 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 plugins of the MDM module 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 plugins of the MDM module are installed, edit this and other enrollment policies to omit endpoints that are already enrolled in another active MDM service.

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

Running the Template

This section describes how to run the template.

To run the template:

1. Select the Policy tab from the Console.


3. Select MaaS360 and then select MaaS360 Device Enrollment.
4. Select Next. The Name page opens. Define a unique name for the policy you are creating based on this template.

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

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

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

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

7. Select **Next**. The Summary page opens and lists the policies generated by the template.
   - If the **MDM Classification** policy did not already exist, it is also created.

8. Select **Finish**. The policy is created.
Which Endpoints are Inspected - Policy Scope

By default, 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 include the Unknown IP Address option when you define the range for policies based on this template, because policy rules filter out these endpoints even if they are included in the scope.

How Devices are Detected and Handled

This section describes the rules and sub-rules of the policy created by the MaaS360 Enrollment Policy template.

Main Rule

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

Sub-Rules

Sub-rules of the policy filter situations and endpoints for which 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

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 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 place in the Maas360 Enrolled Devices group.
1. **Unknown MAC** – CounterACT 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 CounterACT 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 two sub-rules detect devices that are qualified for enrollment in the MaaS360 service, and prompt device users to enroll in the service.

1. **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.

2. **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 [Configuring 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 completed successfully, rule 4 assigns them to the group the next time this policy runs. 
MDM Classification Policy Template

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

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

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

Prerequisites

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

Which Endpoints are Inspected - Policy Scope

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

How Devices are Detected and Handled

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

Main Rule

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

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

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

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 CounterACT management components installed are assumed to be corporate user devices.

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

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

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

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 were 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 that were not classified into the **Mobile Devices** group are excluded from further evaluation.
Corporate/Guest User Evaluation for Mobile Devices

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

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 Configuring Virtual Firewall Actions for information about enabling this action.

MaaS360 Device Compliance Policy Template

Use this template to create a policy that verifies device compliance with CounterACT 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 not-compliant
- Network access limitations
- Steps for remediation

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

Prerequisites

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

You must create and run a policy based on the 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.
Running the Template
This section describes how to run the template.

To run the template:

1. Select the Policy tab from the Console.

3. Select MaaS360 and then select MaaS360 Device Compliance.

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

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

In the Filter by Group area, the scope of the policy is limited to members of the *MaaS360 Enrolled Devices group*. You must run the MaaS360 Enrollment template to create and populate this group.

6. The Offsite Hosts page opens. If you selected the **Support off-site devices** option when you configured the plugin, select the **Include offsite hosts** option. Endpoints without a known IP address are added to the scope of the policy. This is equivalent to selecting the **Unknown IP addresses** option in the Scope page of the wizard.
7. Select **Next**. The Sub-Rules page lists the rules of the policy.

8. 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 include the *Unknown IP Address* option when you define the range for policies based on this template.
How Devices are Detected and Handled

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

Main Rule

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

Sub-Rules

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

Detect Endpoints with Unauthorized Applications

The following rule detects and remediates devices with unauthorized applications:

1. Unauthorized Application Installed – this rule checks the applications listed in the MaaS360 Software Inventory host property against the MaaS360 Unauthorized Mobile Applications list. See Adding Applications to the Unauthorized Application List for information about creating this list.

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

- An HTTP Notification action informs the user that an unauthorized application is installed on the device.
- The Add to Group action assigned the device to the 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 Configuring 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.

1. MaaS360 App Not Installed – iOS
2. 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 Configuring Virtual Firewall Actions for information about enabling this action.

Detect Jailbroken or Rooted Endpoints

1. 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 Configuring Virtual Firewall Actions for information about enabling this action.

Detect Devices Out of MaaS360 Service Compliance

1. 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 Configuring Virtual Firewall Actions for information about enabling this action.

2. 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.

Adding 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.
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 MaaS360.

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

4. Select **Add**. The Add Value dialog box opens.
5. Enter the name of an application that you want to prohibit and then select OK.
6. Repeat steps 4 and 5 for other prohibited applications.
7. (Optional) Type a description of the list in the Description field of the Edit List dialog box.
8. Select OK. The unauthorized applications that you added appear in the Values column.

Configuring Virtual Firewall Actions

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

To configure virtual firewall actions:

1. Open a rule of the policy. Select the Virtual Firewall action, and select Edit. The Virtual Firewall action dialog box opens.
2. In the Blocking Exceptions table of the Parameters tab, select the exception that uses port 443/TCP. Select **Edit**:

3. In the Blocking Exceptions dialog, make the following selections:
   - Allow traffic from the host
   - All IPs
   - Select the port used to communicate with the MDM service.

![Blocking Exceptions dialog](image)

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

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

### Displaying Inventory Data

Use the CounterACT 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 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 inventory:
1. Select the **Inventory** icon from the Console toolbar.
2. Navigate 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 at the Console > Working with Inventory Detections* in the *CounterACT Console User’s Manual* or the Console, Online Help for information about how to work with the CounterACT Inventory.

Managing Offsite Devices

When devices are not in the corporate network, the plugin uses the MaaS360 service platform to retrieve updated host information and implement CounterACT policy actions.

To configure support for management of offsite devices:

- Select the Support Offsite Devices option when you configure the plugin. See *Configure the Plugin*.
- Select the Include Offsite Hosts option when you create policies based on MaaS360 templates. See *Run MaaS360 Policy Templates*.

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

- CounterACT identifies offsite devices by their MAC address. To manage offsite devices, policies must include endpoints without a known IP address in their scope.
- All host properties can be evaluated for offsite devices.
All MaaS360-specific actions provided by this plugin are supported on offsite devices. See Tag MaaS360 Devices - Policy Actions.

Not all general CounterACT actions can be applied to offsite devices. The following CounterACT actions can be applied to offsite devices:
- Manage: Add to Group / Classify / Delete host
- Notify: Send email

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

Working with CounterACT Policies

This section describes how to use CounterACT 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 CounterACT Console.
2. Select the Policy tab from the Console toolbar.
3. Create or edit a policy.

Detecting MaaS360 Devices - Policy Properties

CounterACT policy conditions and properties let you instruct CounterACT 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:
- Asset Classification
- Core Attributes
- Security and Compliance
- Hardware Inventory
- Network Information
- Additional Information
Asset Classification

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

Core Attributes

| Device Type | Indicates the MaaS360 device ID. |
| 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

<table>
<thead>
<tr>
<th>MaaS360 Android Device Rooted</th>
<th>Indicates if an enrolled Android device is rooted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaaS360 Android Settings Failed to Configure</td>
<td>Indicates if certain settings were not configured on an Android host.</td>
</tr>
</tbody>
</table>
| 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 certain 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 |
Hardware Inventory

<table>
<thead>
<tr>
<th>MaaS360 Custom Attributes</th>
<th>Indicates devices that were detected with specific MaaS360 device attributes or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaaS360 Email Address</td>
<td>Indicates the Email Address of the MaaS360 device.</td>
</tr>
<tr>
<td>MaaS360 Manufacturer</td>
<td>Indicates the manufacturer of the MaaS360 device.</td>
</tr>
<tr>
<td>MaaS360 Model</td>
<td>MaaS360 Model</td>
</tr>
<tr>
<td>MaaS360 Operating System</td>
<td>Indicates the Operating System running on the MaaS360 device.</td>
</tr>
<tr>
<td>MaaS360 Ownership</td>
<td>Indicates the ownership of the MaaS360 device.</td>
</tr>
</tbody>
</table>

Network Information

<table>
<thead>
<tr>
<th>MaaS360 ICCID</th>
<th>Indicates an ICCID value detected on the MaaS360 device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaaS360 Phone Number</td>
<td>Indicates the phone number associated with the MaaS360 device.</td>
</tr>
</tbody>
</table>

Additional Information

<table>
<thead>
<tr>
<th>MaaS360 Software Installed</th>
<th>Indicates if specific software is installed on the MaaS360 device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity to MaaS360 Cloud</td>
<td>Indicates if CounterACT is connected to the MaaS360 cloud.</td>
</tr>
<tr>
<td>MaaS360 Listed in Service</td>
<td>Indicates if the device is listed in MaaS360 service.</td>
</tr>
</tbody>
</table>
Tag MaaS360 Devices - Policy Actions

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

- Custom Attribute Value Action
- Refresh Device Information Action

Custom Attribute Value Action

Detect devices using a CounterACT 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 CounterACT to detect devices that were resolved as guests and tag them as:

**Attribute Name:** East Coast Office

**Attribute Value:** Guest

Devices will appear 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 CounterACT Documentation

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

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

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

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

Customer Support Portal

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

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

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

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

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

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

*Documentation Portal*

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

Copyright © ForeScout Technologies, Inc. 2000-2016. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. (“ForeScout”). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

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

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

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

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

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

2016-03-24 12:32