# Table of Contents

About the AirWatch MDM Integration ........................................................... 4  
Additional AirWatch Documentation ............................................................. 4  
About this Module ........................................................................................ 4  
  - How it Works ............................................................................................... 5  
    - Continuous Query Refresh ..................................................................... 5  
    - Offsite Device Management .................................................................. 6  
  - Supported Devices ....................................................................................... 7  
  - Supported Vendor Information ................................................................... 6  
  - Supported Network Infrastructures ................................................................. 6  
  - About Support for Dual Stack Environments ............................................. 6  
  - What to Do .................................................................................................. 7  
Requirements ............................................................................................... 7  
  - CounterACT Software Requirements .......................................................... 7  
  - ForeScout Extended Module License Requirements ....................................... 7  
    - Per-Appliance Licensing Mode ................................................................. 8  
    - Centralized Licensing Mode .................................................................... 9  
    - More License Information ....................................................................... 9  
  - Networking Requirements ............................................................................. 10  
  - Endpoint Requirements ............................................................................... 10  
MDM Web Service Verification ........................................................................ 10  
Define a CounterACT User at the AirWatch Service ..................................... 11  
Install the Module .......................................................................................... 12  
Configure and Test the Module ...................................................................... 14  
  - Configure the Module .................................................................................. 14  
  - Test Module Communication with the AirWatch Service ................................ 15  
Run AirWatch Policy Templates ..................................................................... 16  
  - AirWatch Enrollment Policy Template .......................................................... 17  
    - Prerequisites .............................................................................................. 17  
  - Multiple MDM Service Enrollment ............................................................... 17  
    - Running the Template ............................................................................... 18  
    - Which Endpoints are Inspected - Policy Scope ......................................... 20  
    - How Devices are Detected and Handled .................................................. 20  
  - MDM Classification Policy Template ............................................................ 22  
    - Prerequisites .............................................................................................. 22  
    - Which Endpoints are Inspected - Policy Scope ......................................... 23  
    - How Devices are Detected and Handled .................................................. 23
AirWatch Device Compliance Policy Template .......................................................... 24
Prerequisites ........................................................................................................... 25
Running the Template .......................................................................................... 25
Which Endpoints are Inspected - Policy Scope .................................................... 27
How Devices are Detected and Handled .............................................................. 27
Adding Applications to the AirWatch Unauthorized Mobile Applications List ....... 29
Configuring Virtual Firewall Actions ................................................................... 30

Mobile Device Enrollment ................................................................................... 31

Display Inventory Data ........................................................................................ 34

Managing Offsite Devices ................................................................................... 35

Create Custom AirWatch Policies ....................................................................... 35
  Detecting AirWatch Devices – Policy Properties ............................................... 35
  AirWatch Applications Installed ................................................................. 36
  AirWatch Security Attributes ....................................................................... 37
  AirWatch Certificates Installed .................................................................... 37
  AirWatch General Attributes ...................................................................... 37
  AirWatch User Attributes ........................................................................... 37
  AirWatch Profile Attributes ....................................................................... 38
  AirWatch Network Attributes .................................................................... 38
Managing AirWatch Devices – Policy Actions .................................................. 38
  AirWatch Lock Device Action ..................................................................... 39
  AirWatch Push Notification Action ............................................................. 39
  AirWatch Request Device Check-In Action .................................................... 39
  AirWatch Send Email Action ..................................................................... 40
  AirWatch Send SMS Action ...................................................................... 40
  AirWatch Wipe Device Action ................................................................... 40

Additional CounterACT Documentation ......................................................... 41
  Documentation Downloads ......................................................................... 41
  Documentation Portal .................................................................................. 42
  CounterACT Help Tools .............................................................................. 42
About the AirWatch MDM Integration

ForeScout CounterACT® integrates with VMware AirWatch® MDM to help IT administrators streamline the process to provision, manage and secure today’s expanding suite of smartphones and tablets, all from a single portal. CounterACT/AirWatch 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.

AirWatch 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 AirWatch Documentation

Refer to AirWatch online documentation for more information about the AirWatch MDM solution: [http://www.air-watch.com/resources/brochures](http://www.air-watch.com/resources/brochures)

About this Module

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

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

**How it Works**

The AirWatch MDM Module queries the AirWatch Service for mobile device attributes, for example core attributes, security and compliance information, hardware inventory and network information. All AirWatch queries are performed by a single CounterACT Appliance that is designated for this purpose. This designated CounterACT Appliance, the *CounterACT Connected Device*, retrieves information from other CounterACT Appliances and the CounterACT Enterprise Manager and forwards the information to the AirWatch Service. Similarly, the CounterACT Connected Device retrieves information from the AirWatch service and forwards it to other CounterACT Appliances and the CounterACT Enterprise Manager.

**Continuous Query Refresh**

AirWatch query mechanisms recheck endpoint attributes at a static frequency—approximately once a day. However, after module 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.

**Offsite Device Management**

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

- iOS®
- Android®

For OS version support of the AirWatch service, refer to AirWatch documentation: http://www.air-watch.com/resources/brochures

**Supported Vendor Information**

The AirWatch MDM Plugin supports AirWatch versions up to 9.1.x.

To take advantage of the fixes in this plugin version and subsequent plugin releases, you must upgrade to AirWatch 9.1.x.

**Supported Network Infrastructures**

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

**About Support for Dual Stack Environments**

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component.** 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 component.
What to Do

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

1. Verify that you have met system requirements. See Requirements.
2. Define a CounterACT User at the AirWatch Service.
3. Install the Module.
4. Configure and Test the Module.
5. Run AirWatch Policy Templates.

Requirements

This section describes:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- Networking Requirements
- Endpoint Requirements

CounterACT Software Requirements

The following CounterACT releases can work with this module.

- CounterACT version 8.0.
- A module license for the VMWare AirWatch Module

ForeScout Extended Module License Requirements

This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a ForeScout CounterACT See license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select Options > Licenses to see whether you have a ForeScout CounterACT See license listed in the table.
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

**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 representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

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

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

허용되는 장치의 수는 CounterACT via MDM 서비스를 통해 관리되는 모바일 장치 수에 기반합니다. 이 수는 CounterACT의 Module License Request wizard의 Devices pane에서 입력되어야 합니다.

### 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 CounterACT via the MDM service.

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

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the See license.

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

More License Information

Refer to the CounterACT Administration Guide for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

Networking Requirements

The following ports must be open on enterprise firewalls to support communication between CounterACT and the AirWatch service.
- 443/TCP (default) or the port used to communicate with the AirWatch service. Specify this port when you configure the module.
- 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 for instructions on configuring these port values.

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)

## 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 AirWatch Server by verifying that the AirWatch console supports Web services.


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

3. In the REST client user interface, do the following:
   a. Enter the URL of the REST API on the AirWatch server, as follows: https://<AirWatch server name>/api/system/info. Provide the same AirWatch server name that will be defined in Configure the Module.
   b. Define the HTTP header Authorization (basic). Provide the same username and password that will be defined in Configure the Module.
   c. Define the HTTP header Aw-Tenant-Code: Provide the same API key that will be defined in Configure the Module.

4. Select Send.

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

CounterACT logs in to the AirWatch server as a user defined at the AirWatch Service Portal. The CounterACT user information is required during the module configuration.

To define a CounterACT user in the AirWatch service portal

1. Define a CounterACT user account on the AirWatch service portal. This account must be an administrator (Add > Admin). Edit this user and assign them the Console Administrator role (formerly called API Admin).

   - Record the login information and Location Group for this user. You will enter this information in CounterACT module configuration screens.
2. In the AirWatch service management platform, select Groups & Settings > All Settings to acquire an API key. Under the System options tree, select Advanced > API > REST API. Copy the value of the API Key field. You will enter this value in CounterACT module configuration screens.

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:
To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.

2. Download the module .fpi file.

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

4. Log into the CounterACT 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 will not proceed if you do not agree to the license agreement.

The installation will begin 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.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a ForeScout CounterACT See license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select Options > Licenses to see whether you have a ForeScout CounterACT See license listed in the table.
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

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 AirWatch Service and still receive required HTTP notifications.

Configure and Test the Module

This section describes how to configure and test the module.

Configure the Module

The module configuration is used to ensure that the module can communicate with the AirWatch service.

To configure the module:

1. In the CounterACT console, select Options from the Tools menu.
2. Select Modules.
3. Select AirWatch MDM from the Options pane, and then select Configure.

Enter the following information. Use the user account and API Key values you recorded in the AirWatch service portal.

- Username (Email)
- Password
- AirWatch Server Name. Verify that the MDM server is accessible to the CounterACT Appliance. To specify a port for communication with the server, use the format: 
  <server_name>:<port>
  For example:
  apidev-as.awmdm.com:8843
- API Key
- In the CounterACT Connected Device drop-down list, select the name of the device that will serve as a proxy between the AirWatch service and the CounterACT Enterprise Manager and Appliances. The CounterACT device listed here is the only device that will communicate directly with the AirWatch Service. An Enterprise Manager may not be selected here.
4. Select the Advanced tab.
   - In the **MDM Query Threshold Interval (Seconds)** field, specify the frequency that the module should query the AirWatch service.
   - In the **MDM Query Threshold** field, define the maximum number of query requests to the AirWatch service per threshold interval (defined in the preceding field).
   - Select **Use a Proxy Server** if there is a proxy between the CounterACT Connected Device and the AirWatch 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.
   - In the **AirWatch Enrollment Group ID** field, enter the Location Group that AirWatch assigned to the CounterACT user.

5. Select **Apply** to save configuration changes.

**Test Module Communication with the AirWatch Service**

Test the module communication with the AirWatch 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 module communication with the AirWatch service. Do not enter colons. Use lower case alphanumeric characters. Select Apply.

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

Run AirWatch Policy Templates

This module provides the following policy templates to detect, manage and remediate mobile devices in an AirWatch environment:

- **AirWatch Enrollment Policy Template** – generates a CounterACT policy that detects corporate hosts not enrolled with the AirWatch service and prompts host users to enroll.

- **MDM Classification Policy Template** – generates a CounterACT policy that classifies all mobile devices into groups. All plugins in the MDM Integration Module use this policy. If another plugin is already installed, this policy was probably already created, and the existing version of the policy is retained.

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

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

Use this policy to detect corporate devices that have not enrolled with the AirWatch 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, first 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 AirWatch 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 AirWatch 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.

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

3. Select **AirWatch** and then select **AirWatch 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. See the *CounterACT Administration Guide* for more information about defining the scope of a policy.

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. Select **Next**. The Offsite Hosts page opens. If you selected the **Support offsite devices** option when you configured the module, 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, AirWatch 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 AirWatch 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 AirWatch enrollment is not applicable. The final sub-rules enroll qualified mobile devices in the AirWatch 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 *AirWatch 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 *AirWatch Enrolled Devices* group.

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

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

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

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

5. **AirWatch Exceptions** – devices listed in the *AirWatch 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 AirWatch service.

**Detecting and Handling Devices Qualified for Enrollment**

The following two sub-rules detect devices that are qualified for enrollment in the AirWatch 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 *AirWatch 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 *AirWatch Enrolled Devices* group, it is a candidate for enrollment.

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

- An *HTTP Notification* action redirects users to an enrollment interaction. See [Mobile Device Enrollment](#) for typical enrollment interaction.

- An optional *Virtual Firewall* action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See [Configuring Virtual Firewall Actions](#) for information about enabling this action.
Newly enrolled endpoints are not immediately added to the AirWatch 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 AirWatch Enrollment Policy template creates this policy in addition to the AirWatch 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 module 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.

**AirWatch Device Compliance Policy Template**

Use this template to create a policy that verifies device compliance with CounterACT network requirements and AirWatch 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 mobile applications you must add them to the AirWatch Unauthorized Mobile Application list. An empty list is automatically created when the module is installed. See Adding Applications to the AirWatch Unauthorized Mobile Applications List.

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

AirWatch Device Compliance

Use this policy template to detect non-compliant corporate devices, and redirect non-compliant users to a notification message that indicates:

- Why the device is non-compliant
- Network access limitations
- Steps for remediation

By default, users cannot browse the Internet until they become compliant. A restrictive action that blocks corporate network access to non-compliant users is available. This action is disabled by default.
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. See the *CounterACT Administration Guide* for more information about defining the scope of a policy.

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

6. Select **Next**. The Offsite Hosts page opens. If you selected the **Support offsite devices** option when you configured the module, 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 AirWatch service. The *AirWatch 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 module 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 AirWatch Software Inventory host property against the AirWatch Unauthorized Mobile Applications list. See Adding Applications to the AirWatch Unauthorized Mobile Applications 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 AirWatch 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 AirWatch Service App**

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

1. **AirWatch App Not Installed – iOS**
2. **AirWatch App Not Installed – Android**

When a device matches one of these rules:

- An **HTTP Notification** action redirects users to a service enrollment interaction. See Mobile Device Enrollment for typical enrollment interaction.
- The **Add to Group** action assigns the device to the AirWatch App Not Installed – iOS or the AirWatch 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 AirWatch 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 AirWatch 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 AirWatch Service Compliance

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

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

Adding Applications to the AirWatch Unauthorized Mobile Applications List

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

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

To add an application to the list:

1. Select **Options** from the **Tools** menu and then select **Lists**.
2. Select the **AirWatch Unauthorized Mobile Applications** list for AirWatch.

3. Select **Edit**. The Edit List dialog box opens. Type a description of the list in the **Description** field of the Edit List dialog box.

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. Select **Ok**. The unauthorized mobile 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.

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

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

**Mobile Device Enrollment**

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

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

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

**To enroll:**

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

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

3. Users select **Download AirWatch App**. In a new window, the AirWatch MDM Agent download page opens.

4. Users download and install the application. After installation, users must run the application to complete enrollment. The ForeScout redirection window contains Server and Group ID information needed for enrollment. Users should not close this window.
5. When profile installation is complete, users must return to the ForeScout redirection page and select **Recheck my computer**.

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

Use the CounterACT Inventory to view a real-time display of AirWatch 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 AirWatch devices that have been detected with specific attributes
- Easily track AirWatch device activity
- Incorporate inventory detections into policies

To access the inventory:

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the AirWatch entries.

   The following information, based on AirWatch host properties, is available:
   - AirWatch Applications
   - AirWatch Certificates
   - AirWatch General Attributes
   - AirWatch Compromised Status
   - AirWatch Profiles
Managing Offsite Devices

When devices are not in the corporate network, the module uses the AirWatch 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 module. See Configure the Module.
- Select the Include Offsite Hosts option when you create policies based on AirWatch templates. See Run AirWatch 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 AirWatch-specific actions provided by this module are supported on offsite devices. See Managing AirWatch 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

\[\text{Note that no Restriction or HTTP redirection actions can be applied to offsite devices.}\]

Create Custom AirWatch Policies

You can create a custom policy to deal with issues not covered in the AirWatch policy templates. Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. This section describes the policy properties and actions available when the AirWatch module is installed.

Detecting AirWatch Devices – Policy Properties

CounterACT properties let you detect devices based on information from AirWatch. In the Conditions screen, expand the AirWatch folder in the Properties tree to use these properties in a policy condition.
An extensive range of properties can be detected; most of these properties are grouped into the following categories:

- **AirWatch Applications Installed**
- **AirWatch Security Attributes**
- **AirWatch Certificates Installed**
- **AirWatch General Attributes**
- **AirWatch User Attributes**
- **AirWatch Profile Attributes**
- **AirWatch Network Attributes**

These categories provide the following properties:

### AirWatch Applications Installed

The **AirWatch Applications** property provides information about the applications that are installed in an AirWatch managed endpoint. It contains the following criteria:

<table>
<thead>
<tr>
<th><strong>Application Name</strong></th>
<th>Name of the installed application, for example, AirWatch.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Status</strong></td>
<td>Status of the installed application, for example, Installed.</td>
</tr>
<tr>
<td><strong>Application Type</strong></td>
<td>Type of the installed application, for example, System.</td>
</tr>
<tr>
<td><strong>Application Version</strong></td>
<td>Version of the installed application, for example, 4.7.466.</td>
</tr>
<tr>
<td><strong>Application Size</strong></td>
<td>Size, in bytes, of the installed application, for example, 12247040.</td>
</tr>
</tbody>
</table>
## AirWatch Security Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Block level encryption</td>
<td>Indicates if block level encryption is enabled.</td>
</tr>
<tr>
<td>AirWatch Compromised status</td>
<td>Indicates if the device is compromised.</td>
</tr>
<tr>
<td>AirWatch Compromised status timestamp</td>
<td>Indicates the date/time of the Compromised status shown.</td>
</tr>
<tr>
<td>AirWatch Data Protection</td>
<td>Indicates if data protection is enabled.</td>
</tr>
<tr>
<td>AirWatch File level encryption</td>
<td>Indicates if file level encryption is enabled.</td>
</tr>
<tr>
<td>AirWatch Jailbroken(iOS)/rooted(Android)</td>
<td>Indicates if an enrolled iOS device is jailbroken or an Android device is rooted.</td>
</tr>
<tr>
<td>AirWatch Passcode compliance</td>
<td>Indicates if the passcode complies with AirWatch policy.</td>
</tr>
<tr>
<td>AirWatch Passcode present</td>
<td>Indicates if a passcode is enabled.</td>
</tr>
</tbody>
</table>

## AirWatch Certificates Installed

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Certificates</td>
<td>Indicates the certificates associated with the device.</td>
</tr>
</tbody>
</table>

## AirWatch General Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Compliance status</td>
<td>Indicates the device compliance status.</td>
</tr>
<tr>
<td>AirWatch Compliance status timestamp</td>
<td>Indicates the date/time of the compliance status shown.</td>
</tr>
<tr>
<td>AirWatch Enrollment status</td>
<td>Indicates the device enrollment status.</td>
</tr>
<tr>
<td>AirWatch Enrollment status timestamp</td>
<td>Indicates the date/time stamp of the enrollment status shown.</td>
</tr>
<tr>
<td>AirWatch Last seen</td>
<td>Indicates the date/time stamp of the last time the AirWatch device was seen on the network.</td>
</tr>
<tr>
<td>AirWatch Model</td>
<td>Indicates the AirWatch device model.</td>
</tr>
<tr>
<td>AirWatch OS version</td>
<td>Indicates the AirWatch platform OS version</td>
</tr>
<tr>
<td>AirWatch Ownership</td>
<td>Indicates the AirWatch device ownership.</td>
</tr>
<tr>
<td>AirWatch Phone number</td>
<td>Indicates the device phone number.</td>
</tr>
<tr>
<td>AirWatch Platform</td>
<td>Indicates the AirWatch device platform.</td>
</tr>
<tr>
<td>AirWatch Serial Number</td>
<td>Indicates the device serial number.</td>
</tr>
<tr>
<td>AirWatch UDID</td>
<td>Indicates the device Unique Identifier.</td>
</tr>
<tr>
<td>AirWatch ID</td>
<td>Indicates the device alternate id.</td>
</tr>
</tbody>
</table>

## AirWatch User Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Contact Number</td>
<td>Indicates the contact number.</td>
</tr>
<tr>
<td>AirWatch Email</td>
<td>Indicates the user Email address entered during registration.</td>
</tr>
</tbody>
</table>
AirWatch Security type | Indicates the security type on the device.
---|---
AirWatch User | Indicates the currently-enrolled user of the device.

**AirWatch Profile Attributes**

<table>
<thead>
<tr>
<th>AirWatch Profiles</th>
<th>Indicates the AirWatch profiles installed on the device.</th>
</tr>
</thead>
</table>

**AirWatch Network Attributes**

<table>
<thead>
<tr>
<th>AirWatch IMEI</th>
<th>Indicates the IMEI number of the device.</th>
</tr>
</thead>
</table>

In addition to the above categorized properties, the following AirWatch properties are not listed under a sub-category:

<table>
<thead>
<tr>
<th>AirWatch Device Last Update</th>
<th>Indicates the last device update time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Listed in Service</td>
<td>Indicates if the device is listed in AirWatch Service</td>
</tr>
<tr>
<td>Connectivity to AirWatch Cloud</td>
<td>Indicates if the module is connected to the cloud.</td>
</tr>
<tr>
<td>MDM Network Function</td>
<td>Indicates the mobile operating system of an MDM managed endpoint. This property is common to all MDM Integration Module plugins and is found in the Asset Classification folder of the Properties tree.</td>
</tr>
</tbody>
</table>

**Managing AirWatch Devices – Policy Actions**

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

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

- AirWatch Lock Device Action
- AirWatch Push Notification Action
- AirWatch Request Device Check-In Action
- AirWatch Send Email Action
- AirWatch Send SMS Action
- AirWatch Wipe Device Action
AirWatch Lock Device Action
This action allows you to remotely lock a device.

AirWatch Push Notification Action
This action allows you to send a push notification to a device.

AirWatch Request Device Check-In Action
This action forces the device to connect to the AirWatch service.
AirWatch Send Email Action
This action allows you to send an email to a device.

AirWatch Send SMS Action
This action allows you to send an SMS to a device.

AirWatch Wipe Device Action
This action allows you to wipe a device of all content or of Enterprise content.
Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - Product Updates Portal
- **Centralized Licensing Mode** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

**To access the Product Updates Portal:**

2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:
2. Select Downloads or Documentation.

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

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

CounterACT 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.

CounterACT Administration Guide
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 Modules.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.

Identifying Your Licensing Mode in the Console
If your Enterprise Manager has a ForeScout CounterACT See license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select Options > Licenses to see whether you have a ForeScout CounterACT See license listed in the table.
Contact your ForeScout representative if you have any questions about identifying your licensing mode.
Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-15 17:34