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

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

Legal Notice
© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Table of Contents

About the AirWatch MDM Integration ........................................................... 5
  About Certification Compliance Mode ......................................................... 5

Additional AirWatch Documentation ............................................................... 5

About this Module ........................................................................................ 6
  How It Works ............................................................................................... 6
    Continuous Query Refresh ......................................................................... 7
    Offsite Device Management ...................................................................... 7
  Supported Devices ....................................................................................... 7
  Supported Vendor Information ...................................................................... 8
  Supported Network Infrastructures .............................................................. 8
  About Support for Dual Stack Environments ................................................. 8
  What to Do .................................................................................................. 8

Requirements ............................................................................................... 8
  Forescout Requirements ................................................................................ 9
  Forescout eyeExtend (Extended Module) Licensing Requirements ...................... 9
    Per-Appliance Licensing Mode .................................................................. 9
    Flexx Licensing Mode ............................................................................. 10
    More License Information ........................................................................ 10
  Networking Requirements .......................................................................... 11
  Endpoint Requirements ............................................................................... 11

Define a Forescout User on the AirWatch Service ....................................... 11

Install the Module ...................................................................................... 12

Configure the Module ................................................................................. 13

Test Module Communication with the AirWatch Service ............................. 16

MDM Web Service Verification ..................................................................... 16

Create AirWatch Policies Using Templates .................................................. 17
  AirWatch Enrollment Policy Template ......................................................... 18
    Prerequisites ........................................................................................... 18
    Multiple MDM Service Enrollment ........................................................... 19
  Create an AirWatch Device Enrollment Policy ............................................. 19
    Which Endpoints Are Inspected – Policy Scope ......................................... 21
    How Devices Are Detected and Handled .................................................... 21
  MDM Classification Policy Template ........................................................... 24
    Prerequisites ........................................................................................... 24
    Which Endpoints Are Inspected – Policy Scope ......................................... 24
    How Devices are Detected and Handled .................................................... 24
  AirWatch Device Compliance Policy Template ........................................... 27
Prerequisites ........................................................................................................... 27
Create an AirWatch Device Compliance Policy ................................................... 28
Which Endpoints Are Inspected – Policy Scope ..................................................... 29
How Devices Are Detected and Handled ............................................................... 29
Add Applications to the AirWatch Unauthorized Mobile Applications List .......... 32
Configure Virtual Firewall Actions ......................................................................... 34

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

Display Inventory Data ............................................................................................ 39

Manage Offsite Devices ........................................................................................... 39

Create Custom AirWatch Policies ........................................................................... 40
Detect AirWatch Devices – Policy Properties ......................................................... 40
AirWatch Applications Installed .............................................................................. 42
AirWatch Security Attributes .................................................................................... 42
AirWatch Certificates Installed ................................................................................. 42
AirWatch General Attributes ..................................................................................... 42
AirWatch User Attributes ......................................................................................... 43
AirWatch Profile Attributes ....................................................................................... 43
AirWatch Network Attributes ..................................................................................... 43
Additional Attributes ............................................................................................... 43

Manage AirWatch Devices – Policy Actions ............................................................. 44
AirWatch Lock Device Action ................................................................................... 44
AirWatch Push Notification Action .......................................................................... 45
AirWatch Request Device Check-In Action .............................................................. 45
AirWatch Send Email Action ..................................................................................... 45
AirWatch Send SMS Action ..................................................................................... 46
AirWatch Wipe Device Action .................................................................................. 46

Additional Forescout Documentation ..................................................................... 47
Documentation Downloads ...................................................................................... 47
Documentation Portal ............................................................................................... 48
Forescout Help Tools ................................................................................................. 48
About the AirWatch MDM Integration

Forescout 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. Forescout/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 personally owned devices.

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

Forescout integration with MDM services provides a whole new level of centralized visibility and control for actionable insights into your entire computing landscape. It lets you:

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

About Certification Compliance Mode

Forescout eyeExtend for VMware AirWatch supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide. See Additional Forescout Documentation for information on how to access this guide.

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

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

How It Works

Forescout eyeExtend for VMware AirWatch 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 CounterACT Appliance, the CounterACT Connected Device, retrieves information from other CounterACT Appliances and the 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 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 the Forescout platform policy *recheck* definitions that set the conditions for rechecking hosts that match a policy. Specifically, you can specify:

- How often hosts are rechecked once they match a policy
- Under what conditions to carry out the recheck

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

**Offsite Device Management**

This module leverages integration with AirWatch to manage devices even when they are not in the corporate network. Forescout eyeExtend for VMware AirWatch 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 [Manage Offsite Devices](#).

**Supported Devices**

The following devices are supported by this module:

- iOS®
- Android®

For OS version support of the AirWatch service, refer to AirWatch documentation: [http://www.air-watch.com/resources/brochures](http://www.air-watch.com/resources/brochures)
Supported Vendor Information

- To take advantage of the fixes in this version and subsequent releases, you must upgrade to AirWatch 9.1.x.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Supported Network Infrastructures

The following network infrastructures are supported by this module:

- 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

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

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See Requirements.
2. Define a Forescout User on the AirWatch Service.
3. Install the Module.
4. Configure the Module.
5. Test Module Communication with the AirWatch Service.

Requirements

Verify that the following requirements are met:

- Forescout Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements
- Networking Requirements
- Endpoint Requirements
Forescout Requirements
The module requires the following Forescout releases and components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for VMware AirWatch. See Forescout eyeExtend (Extended Module) Licensing Requirements.

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

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

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

Per-Appliance Licensing Mode
When installing the module you are provided with a 90-day demo module license. If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout sales representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

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

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

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

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

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

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

No demo license is automatically installed during system installation.

License entitlements are managed in the ForeScout Customer Portal. After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

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

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

- Per-Appliance Licensing. Refer to the Forescout Administration Guide.
- Flexx Licensing. Refer to the Flexx Licensing How-to Guide.

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

The following ports must be open on enterprise firewalls to support communication between the Forescout platform 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 Configure Virtual Firewall Actions.

Endpoint Requirements

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

- Wireless Plugin (Client table)
- Packet-Engine (ARP and DHCP traffic)
- L3 switches (ARP table)

Define a Forescout User on the AirWatch Service

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

To define a Forescout user:

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

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

---

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

2. Download the module .fpi file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select Options from the Tools menu.
5. Select Modules. The Modules pane opens.
6. Select Install. The Open dialog box opens.
7. Browse to and select the saved module .fpi file.
8. Select Install. The Installation screen opens.
9. Select I agree to the License Agreement to confirm that you have read and agree to the terms of the License Agreement and select Install. The installation cannot proceed unless you agree to the license agreement.

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

In modules that contain more than one component, the installation proceeds automatically one component at a time.

10. When the installation completes, select Close to close the window. The installed module is displayed in the Modules pane.

Some components are not automatically started following installation.

Once installed, the module automatically adds an HTTP Redirect exception to the CounterACT NAC Redirect Exception list. CounterACT NAC HTTP redirect exceptions 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 the Module**

After Forescout eyeExtend for VMware AirWatch is installed, configure the module to ensure that the Forescout platform can communicate with the AirWatch service.

To configure the module:

1. In the Console, select Options from the Tools menu.
2. Select Modules.
3. Select AirWatch MDM from the Options pane, and then select Configure.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username of the user account you created in the AirWatch service portal.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password.</td>
</tr>
<tr>
<td><strong>Retype Password</strong></td>
<td>Re-enter the password to verify it.</td>
</tr>
<tr>
<td><strong>AirWatch Server Name</strong></td>
<td>Enter the AirWatch server name, a Fully Qualified Domain Name (FQDN) or the IPv4 address. Verify that the MDM server is accessible to the CounterACT Appliance.</td>
</tr>
<tr>
<td><strong>API Key</strong></td>
<td>Enter the API Key you recorded in the AirWatch service portal.</td>
</tr>
<tr>
<td><strong>Retype API Key</strong></td>
<td>Re-enter the API Key to verify it.</td>
</tr>
</tbody>
</table>
| **Validate Server Certificate** | Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:  
  - Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance  
  - Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance  

Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the Forescout Administration Guide.

| **CounterACT Connected Device** | Select the device that will serve as a proxy between the AirWatch service and the Enterprise Manager and CounterACT Appliances. The selected CounterACT device will be the only device that communicates directly with the AirWatch Service. An Enterprise Manager may not be selected here. |
5. Select the Advanced tab.

6. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM Query Threshold Interval (Seconds)</td>
<td>Specify how often (in seconds) the module should query the AirWatch service.</td>
</tr>
<tr>
<td>MDM Query Threshold</td>
<td>Define the maximum number of query requests to the AirWatch service per MDM Query Threshold Interval.</td>
</tr>
<tr>
<td>Use a Proxy Server</td>
<td>Select this option if there is a proxy between the CounterACT Connected Device and the AirWatch service.</td>
</tr>
<tr>
<td>DNS Name or IP Address of the Proxy Server</td>
<td>Enter the DNS name or the IPv4 address of the proxy server.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Enter the required proxy server port.</td>
</tr>
<tr>
<td>AirWatch Enrollment Group ID</td>
<td>Enter the Location Group that AirWatch assigned to the Forescout user.</td>
</tr>
<tr>
<td>Support Offsite Devices</td>
<td>Select this option to support offsite devices.</td>
</tr>
</tbody>
</table>

7. Select Apply to save configuration changes.

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

The best practice is to test the module communication with the AirWatch service after setting up the connection.

To test communication:

1. In the AirWatch MDM pane, 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.

3. Select **Apply**.

4. In the Options pane, select **Modules**. Then select **AirWatch MDM** and select **Test**.

Using configured settings, the Forescout platform attempts to connect with the AirWatch service and to retrieve endpoint property values for the specified device.

5. Select **Close**.

MDM Web Service Verification

To verify that the Web service is properly set up, the test REST API calls on the AirWatch Server to verify that the AirWatch console supports Web services.

To verify the Web service setup:


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. This AirWatch server name must be the same as defined when you configure the module.

b. Define the HTTP header **Authorization** (basic). The username and password must be the same as defined when you configure the module.

c. Define the HTTP header **Aw-Tenant-Code**. The API key must be the same as defined when you configure the module.

4. Select **Send**.

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

---

**Create AirWatch Policies Using Templates**

This section describes how to use AirWatch policy templates to detect, manage, and remediate mobile devices. Refer to the following sections:

- **AirWatch Enrollment Policy Template** – generates a Forescout platform policy that detects corporate hosts not enrolled with the AirWatch service and prompts host users to enroll.
• **MDM Classification Policy Template** – generates a Forescout platform policy that classifies all mobile devices into groups. All MDM Integration modules 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 Forescout platform policy that detects and remediates non-compliant devices.

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

---

**AirWatch Enrollment Policy Template**

Use an AirWatch Enrollment 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 *Primary 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 MDM Integration modules 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 MDM Integration modules are installed, edit this and other enrollment policies to omit endpoints that are already enrolled in another active MDM service.

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

**Create an AirWatch Device Enrollment Policy**

This section describes how to use the AirWatch Device Enrollment template to create a policy.

**To create a policy:**

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

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

3. Expand the **AirWatch** folder and select **AirWatch Device Enrollment**.
4. Select **Next**. The Name pane opens.

5. Define a unique name for the policy you are creating based on this template.

6. Select **Next**. The Scope pane opens.

Refer to the *Forescout 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.

7. Select **Next**.
8. 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 policy scope. This is equivalent to selecting the **Unknown IP addresses** option in the Scope pane.

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

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

**Which Endpoints Are Inspected – Policy Scope**

By default, 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.
Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

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

**Sub-Rules**

The sub-rules 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 placed in the AirWatch Enrolled Devices group.

1. **Unknown MAC** – The Forescout platform 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. **Cloud Disconnected** – This rule tests for the Forescout platform's 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. **Enrolled Devices** – 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.

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

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

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

7. **AirWatch Exceptions** – Devices listed in the AirWatch Exceptions group are excluded from enrollment.

Detecting and Handling Devices Qualified for Enrollment

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

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

9. **Devices Not Enrolled – Android** – If a device has been classified into the Android group but is not a member of the 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 details.

- An optional Virtual Firewall action prevents users from accessing the corporate network until they are compliant. This action is disabled by default. See Configure Virtual Firewall Actions for details.
Newly enrolled endpoints are not immediately added to the AirWatch Enrolled Devices group. If the enrollment interaction completes successfully, rule 4 assigns them to the group the next time this policy runs.

MDM Classification Policy Template

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

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

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

Prerequisites

The MDM Classification policy sorts endpoints based on previous classification by the Primary Classification and Mobile Classification policies, and corporate/guest status as determined by Corporate/Guest Control policies. Run those 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 Integration module templates.
Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule 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 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, the Forescout platform cannot evaluate whether the device is managed by an MDM service. No actions are applied, and policy evaluation of the endpoint ends.

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

2. **Corporate iOS Mobile Devices**
3. **Corporate Android Mobile Devices**
4. **Other Corporate Mobile Devices**

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

- *Mobile Devices* group
- *Corporate Hosts* group – devices with any Forescout 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 sort corporate/guest users. The following rules exclude endpoints that cannot be classified as corporate/guest users. When an endpoint matches one of these rules, no actions are applied, and policy evaluation of the endpoint ends.

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

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

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

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

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

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

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

9. **Unregistered Guest Users** – If the user was not authenticated as a corporate host or signed-in guest, the following actions are applied:

   - The Add to Group action assigns the endpoint to the Guest Hosts group.
   - The HTTP Login action redirects the endpoint to an interaction for authentication.
   - An optional Virtual Firewall action prevents users from accessing the corporate network until they complete enrollment. See Configure Virtual Firewall Actions for details.

AirWatch Device Compliance Policy Template

Use this template to create a policy that verifies device compliance with Forescout 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(707,757),(878,788) 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 Add Applications to the AirWatch Unauthorized Mobile Applications List.

{eyeExtend for VMware AirWatch Configuration Guide}
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.

Create an AirWatch Device Compliance Policy

This section describes how to create to use the AirWatch Device Compliance template to create a policy.

To create a policy:

1. In the Console, select Policy.


3. Select AirWatch and then select AirWatch Device Compliance.

4. Select Next. The Name pane opens.
5. Define a unique name for the policy you are creating based on this template.

6. Select Next. The Scope pane opens. Use the IP Address Range dialog box to define which endpoints are inspected. Refer to the Forescout 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.

7. Select Next.

8. 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 policy scope. This is equivalent to selecting the Unknown IP addresses option in the Scope pane.

9. Select Next. The Summary pane lists the rules of the policy.

10. 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 Integration module templates.
Endpoints that match the Main Rule are included in the policy inspection. **Endpoints that do not match this rule are not inspected for this policy.** Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule 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 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 Add Applications to the AirWatch Unauthorized Mobile Applications List for details.

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 Configure Virtual Firewall Actions for details.

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.

2. AirWatch App Not Installed – iOS

3. 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 Configure Virtual Firewall Actions for information about enabling this action.

Detect Jailbroken or Rooted Endpoints

4. 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 Configure Virtual Firewall Actions for information about enabling this action.

Detect Devices Out of AirWatch Service Compliance

5. **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 Configure Virtual Firewall Actions for information about enabling this action.

6. **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.

Add 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.

4. Type a description of the list in the **Description** field.

5. Select **Add**.

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

7. Repeat steps 5 to 6 for other prohibited applications.

8. Select **OK**. The unauthorized mobile applications are listed in the Values column.
Configure Virtual Firewall Actions

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

**To configure virtual firewall actions:**

1. Open a policy rule, select the **Virtual Firewall** action, and select **Edit**.

2. In the **Blocking Exceptions** table on the Parameters tab, select the exception that uses port 443/TCP and select **Edit**.
3. In the Blocking Exceptions dialog box, configure the following settings:
   - Select **The FW will allow traffic from the detected host**
   - Select **All IPs**
   - Select **Single**, and specify the port used to communicate with the MDM service.

4. Select **OK** to save changes to the exception.

5. In the Action dialog box, select **OK** to finish editing the action.

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

**Mobile Device Enrollment**

The AirWatch Device Enrollment policy template creates policies that detect unenrolled corporate devices and guide corporate users through the enrollment process. See AirWatch Enrollment Policy Template for details.

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.
The following workflow 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.

1. The Forescout platform 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. The Forescout platform 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. The Forescout platform 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 Asset 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. In the Console, select Asset Inventory.
2. In the Views pane, expand the AirWatch folder.

The following information is available:
- AirWatch Applications
- AirWatch Certificates
- AirWatch General Attributes
- AirWatch Compromised Status
- AirWatch Profiles

Refer to Working at the Console > Working with Inventory Detections in the Forescout Administration Guide or the Console Online Help for information about how to work with the Asset Inventory.

Manage Offsite Devices

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

To configure support for management of offsite devices:

- Select the Support Offsite Devices option when you configure the module. See Configure the Module.
- Select the Include Offsite Hosts option when you create policies based on AirWatch templates. See Create AirWatch Policies Using Templates.

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

- The Forescout platform identifies offsite devices by their MAC address. To manage offsite devices, policies must include endpoints without a known IP address in their scope.
• All host properties can be evaluated for offsite devices.
• All AirWatch-specific actions provided by this module are supported on offsite devices. See Manage AirWatch Devices – Policy Actions.
• Not all Forescout actions can be applied to offsite devices. The following actions can be applied to offsite devices:
  – Manage: Add to Group, Classify, Delete host
  – Notify: Send email

Neither Restriction nor 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 Forescout eyeExtend for VMware AirWatch is installed.

Detect AirWatch Devices – Policy Properties

Forescout properties let you detect devices based on information from AirWatch. In the Conditions dialog box, 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**
**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>Application Name</th>
<th>Name of the installed application, for example, <em>AirWatch</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Status</td>
<td>Status of the installed application, for example, <em>Installed</em>.</td>
</tr>
<tr>
<td>Application Type</td>
<td>Type of the installed application, for example, <em>System</em>.</td>
</tr>
<tr>
<td>Application Version</td>
<td>Version of the installed application, for example, <em>4.7.466</em>.</td>
</tr>
<tr>
<td>Application Size</td>
<td>Size, in bytes, of the installed application, for example, 12247040.</td>
</tr>
</tbody>
</table>

**AirWatch Security Attributes**

<table>
<thead>
<tr>
<th>AirWatch Block level encryption</th>
<th>Indicates if block level encryption is enabled.</th>
</tr>
</thead>
<tbody>
<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>AirWatch Certificates</th>
<th>Indicates the certificates associated with the device.</th>
</tr>
</thead>
</table>

**AirWatch General Attributes**

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

**AirWatch User Attributes**

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

**AirWatch Profile Attributes**

| **AirWatch Profiles** | Indicates the AirWatch profiles installed on the device.          |

**AirWatch Network Attributes**

| **AirWatch IMEI** | Indicates the IMEI number of the device.                          |

**Additional Attributes**

The following additional AirWatch properties are not listed under a sub-category:

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

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

In the Actions dialog box, 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 Forescout platform 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 lets you remotely lock a device.

![AirWatch Lock Device Action](image-url)
AirWatch Push Notification Action
This action lets you send a push notification to a device.

![AirWatch Push Notification Action](image)

AirWatch Request Device Check-In Action
This action forces the device to connect to the AirWatch service.

![AirWatch Request Device Check-In Action](image)

AirWatch Send Email Action
This action lets you send an email to a device.

![AirWatch Send Email Action](image)
**AirWatch Send SMS Action**

This action lets you send an SMS to a device.

**AirWatch Wipe Device Action**

This action lets you wipe a device of all content or of Enterprise content.
Additional Forescout Documentation

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

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

**Documentation Downloads**

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

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

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

**Forescout Technical Documentation Page**

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

To access the Technical Documentation Page:

- Go to [https://www.Forescout.com/company/technical-documentation/](https://www.Forescout.com/company/technical-documentation/)
Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Support Portal

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

To access documentation on the Customer Support Portal:

- Go to https://Forescout.force.com/support/ and select Downloads.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select Administration Guide from the Help menu.

Plugin Help Files

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

Documentation Portal

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