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

Legal Notice

© 2019 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 McAfee ePolicy Orchestrator (ePO) Integration** .................................. 5
- Use Cases ........................................................................................................ 5
- About Certification Compliance Mode .......................................................... 5
- Additional McAfee ePO Documentation ......................................................... 6

**About This Module** .................................................................................. 6

**Concepts and Components** .................................................................. 6
- Concepts ........................................................................................................ 6
- Components .................................................................................................. 7
- What to Do ..................................................................................................... 8

**Requirements** ........................................................................................ 8
- Forescout Requirements .............................................................................. 8
- About Support for Dual Stack Environments ............................................ 9
- Forescout eyeExtend (Extended Module) Licensing Requirements ........ 9
  - Per-Appliance Licensing Mode ................................................................. 9
  - Flexx Licensing Mode .............................................................................. 11
  - More License Information ...................................................................... 11
- Third-Party Requirements .......................................................................... 11

**Install the Module** .................................................................................. 11

**Configure the Module** .......................................................................... 12
- Configure the Forescout ePO Extension .................................................... 13
- Configure ePO Database Credentials ........................................................ 16
- Assign CounterACT Devices ....................................................................... 18

**Test the Module** .................................................................................... 20

**Install and Configure the Forescout ePO Extension (Optional)** .......... 22
- Install the Forescout ePO Extension .......................................................... 22
- Configure the ePO Detected System .......................................................... 23
  - Define Permission Sets .......................................................................... 23
  - Configure a User ...................................................................................... 26

**Work with McAfee ePO Policy Templates** ........................................... 27
- ePO Agent Communications Audit Policy Template .................................. 27
  - How Endpoints are Detected and Handled .............................................. 30
- ePO Client Audit Policy Template ............................................................. 32
  - How Endpoints are Detected and Handled .............................................. 34
- ePO Endpoint Test Policy Template .......................................................... 36
  - How Endpoints are Detected and Handled .............................................. 38

**Create Custom ePO Policies** ................................................................. 40
Detect Endpoints with ePO Attributes – Policy Properties .................................................. 44
  ePO Agent Last Communication .......................................................... 44
  ePO Agent Managed State ............................................................... 45
  ePO DB is UP .............................................................................. 46
  ePO Tags ................................................................................. 46
  ePO Point Product Properties ............................................................... 46
  ePO Point Product Setting Boolean .................................................. 48
  ePO Point Product Setting Date ....................................................... 48
  ePO Point Product Setting Integer ................................................... 49
  ePO Point Product Setting String ....................................................... 50
  ePO RSD Detected System Linked Table Boolean .................................. 50
  ePO RSD Detected System Linked Table Date .................................... 51
  ePO RSD Detected System Linked Table Integer .................................. 51
  ePO RSD Detected System Linked Table String .................................... 52
  ePO RSD Detected System Table Boolean ........................................... 53
  ePO RSD Detected System Table Date .............................................. 53
  ePO RSD Detected System Table Integer ........................................... 54
  ePO RSD Detected System Table String .............................................. 54
Manage ePO Endpoints – Policy Actions ..................................................... 55
Report Detected Hosts to the ePO Detected System ....................................... 55

Display McAfee ePO Detections ........................................................................ 56

Endpoint Module Information ........................................................................ 57

Additional Forescout Documentation ............................................................. 58
  Documentation Downloads ..................................................................... 58
  Documentation Portal .......................................................................... 59
  Forescout Help Tools .......................................................................... 59
About McAfee ePolicy Orchestrator (ePO) Integration

Forescout is recognized as a leading network access control solution with continuous, agentless discovery of endpoint devices whether they are managed, unmanaged, or otherwise unknown. McAfee® ePolicy Orchestrator® (ePO) delivers security management technology for network endpoints by providing real-time information and application integration for network, desktop, and server security.

This integration combines the benefits of the McAfee ePO and Forescout platforms to offer greater coverage and control to more devices on the network.

Use Cases

This section describes important use cases supported by Forescout eyeExtend for McAfee ePolicy Orchestrator. To understand how this module helps you achieve these goals, see About This Module.

Report New Endpoints to ePO

The Forescout platform offers real-time visibility and control over 100% of the devices on your network. When the Forescout platform detects an endpoint not managed by McAfee ePO, it can provide ePO with the IP address for installation of the ePO Agent. For more information, see ePO Client Audit Policy Template.

Query ePO Database for Host Property Values

The Forescout platform offers querying the ePO database for host property values. These values identify and address corporate devices that have missing, disabled, or broken agents. Based on your device posture and configured security policies, the query either allows, denies, or limits network access. Before allowing network access, the Forescout platform verifies that the ePO Agent is installed and operational on devices. For more information, see Work with McAfee ePO Policy Templates and Create Custom ePO Policies.

About Certification Compliance Mode

Forescout eyeExtend for McAfee ePolicy Orchestrator supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.
Additional McAfee ePO Documentation

Refer to online documentation for more information about the McAfee ePolicy Orchestrator solution:

https://support.mcafee.com/ppdокументation

About This Module

This integration lets you:

- Use the Forescout platform to report newly discovered hosts to the *ePO Detected System*. See [Report Detected Hosts to the ePO Detected System](#) for details.
- Instruct the Forescout platform to discover endpoints with an extensive range of ePO attributes, such as:
  - *ePO Agent Managed State*
  - *ePO Agent Last Communication*
  - *ePO Tags*
  - *ePO Point Product Properties*
See [Detect Endpoints with ePO Attributes – Policy Properties](#) for details.

Concepts and Components

This section provides a basic overview of the architecture of the McAfee ePO and Forescout platforms:

- **Concepts** – basic integration concepts.
- **Components** – devices in your network that participate in the integration.

Concepts

The Forescout platform integrates with McAfee ePO in the following ways:

- Use the Forescout ePO Extension when integrating through the Rogue System Detection Module.
- Directly query the ePO database to resolve ePO host properties.

Integration lets you map one or more CounterACT® Appliances or Enterprise Managers to a unique ePO server. When multiple CounterACT devices are mapped to a single ePO server, one of the CounterACT devices functions as the proxy, called the *connecting CounterACT device*. This device handles communication between the ePO server and all CounterACT devices mapped to that server. Using a proxy enables the module to control the query rate from the Forescout platform to the ePO server, thus ensuring more efficient traffic control.
One ePO server is designated as the default server to handle CounterACT devices not mapped to a specific ePO server. This may happen, for example, when new Appliances are registered with an Enterprise Manager, but are not yet assigned to an ePO server.

**Deployment Options**

There are two topologies that can be used to set up multiple CounterACT devices and multiple ePO servers.

- The actual deployments can be designed to combine both topologies to meet particular network requirements.

**Peer-to-Peer:** Each CounterACT device communicates directly with an ePO server. This is a one-to-one relationship, where each CounterACT Appliance or Enterprise Manager prompts its connected server to initiate queries whenever required. This is often the typical topology for remote sites.

**Appliance Proxy:** One connecting CounterACT device serves as a channel (proxy) to an ePO server. The connecting device queues queries from the CounterACT Appliances assigned to it, and controls the number of requests to ensure more efficient traffic control and to avoid overloading the ePO server.

A single CounterACT device can be assigned to only one ePO server.

**Components**

**Connecting CounterACT Device:** In an environment where more than one CounterACT device is assigned to a single ePO server, the connecting device functions as a proxy between the ePO server and the CounterACT devices assigned to that server. The connecting device communicates directly with the ePO server, forwarding all queries and requests from it and the other CounterACT devices to the ePO server.
**Assigned CounterACT Device:** This CounterACT device is assigned to an ePO server, but it does not communicate with the server directly. All communication between the ePO server and its assigned CounterACT devices is handled by the connecting CounterACT device defined for the ePO server. All IP addresses handled by an assigned device must also be handled by the ePO server to which the devices are assigned.

**Default ePO Server:** This is the server to which CounterACT devices are assigned by default if they are not explicitly assigned to another ePO server.

**What to Do**

This section lists the steps to integrate your system with McAfee ePO.

1. Verify that you have met module requirements. See **Requirements**.
2. **Install the Module**.
3. **Configure the Module** to define target ePO Extension and ePO Database settings.
4. If needed, **Install and Configure the Forescout ePO Extension**.
5. **Create Custom ePO Policies** to create a policy that detects endpoint admissions and ePO attributes on network endpoints.

**Requirements**

This section describes the following system requirements:

- **Forescout Requirements**
- **Forescout eyeExtend (Extended Module) Licensing Requirements**
- **Third-Party Requirements**

**Forescout Requirements**

The module requires the following Forescout releases and other components:

- Forescout version 8.1.
- A module license for Forescout eyeExtend for McAfee ePolicy Orchestrator. See **Forescout eyeExtend (Extended Module) Licensing Requirements**.
- Endpoint Module version 1.1, with the HPS Inspection Engine component running. See **Endpoint Module Information**.
- When working with the Forescout ePO Extension:
  - Forescout ePO Extension, version 1.3.0
About Support for Dual Stack Environments

Forescout version 8.1 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.

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 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.

*To continue working with the module after the demo period expires, you must purchase a permanent module 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. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

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

To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.
**Flexx Licensing Mode**

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature 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.

**Third-Party Requirements**

- McAfee ePolicy Orchestrator (ePO) server version 5.3 or 5.9
- When working directly with the ePO database:
  - A Microsoft SQL Server user that belongs to the ePO database with read permissions to conduct a *select* query
- A solid understanding of McAfee ePO functionality

**Install the Module**

This section describes how to install the module.

The Forescout HPS Inspection Engine Plugin must already be installed or this module installation will fail.
To install the module:

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

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

2. Download the module .fpi file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select Options from the Tools menu.
5. Select Modules. The Modules pane opens.
6. Select Install. The Open dialog box opens.
7. Browse to and select the saved module .fpi file.
8. Select Install. The Installation screen opens.
9. Select I agree to the License Agreement to confirm that you have read and agree to the terms of the License Agreement, and select Install. The installation 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.

Configure the Module

Configure the module to ensure that the Forescout platform can communicate with McAfee ePO.

To configure the module:

1. In the Console, select Options from the Tools menu. The Options pane opens.
2. Select McAfee ePO.
3. Select **Device** and then select **Add**. The Add ePO Server wizard opens.

4. Configure the module and optional ePO Extension. For details, see [Configure the Forescout ePO Extension](#), [Configure ePO Database Credentials](#), and [Assign CounterACT Devices](#).

**Configure the Forescout ePO Extension**

-In addition to configuring the module, you can also install the optional Forescout ePO Extension on the ePO server. This allows the usage of RSD Detection System properties. See [Install and Configure the Forescout ePO Extension](#) for details.
To configure the Forescout ePO Extension:

1. In the ePO Extension Configuration pane of the Add ePO Server wizard, configure the connection as follows:

<table>
<thead>
<tr>
<th><strong>Enable ePO Extension Configuration</strong></th>
<th>Select this option and use the URL format shown to locate the extension file.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name</strong></td>
<td>Enter the ePO server name, a Fully Qualified Domain Name (FQDN) or the IPv4 address of the server.</td>
</tr>
<tr>
<td><strong>Server Port Number</strong></td>
<td>Enter the ePO server port.</td>
</tr>
</tbody>
</table>
**Validate ePO 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.

**ePO Detected System Credentials:**
Enter the credentials of the user defined in the ePO Server with Rogue System Detection (RSD) permissions. Configure the options in **ePO Detected System Credentials** if you are using the Forescout platform to report rogue hosts to the ePO Detected System.

**CounterACT User Name**
Enter the user name defined in the ePO server.

**CounterACT User Password**
Enter the password assigned to the user.

**Verify Password**
Re-enter the password to verify it.

**Detected System Threshold**
Define the maximum number of hosts that can be reported to the ePO server within the defined **Detected System Threshold Interval**. Define the maximum number of messages, such as reports of hosts for the ePO RSD table that the connecting CounterACT device can send to the ePO server during a given interval. For example, send messages for no more than 40 hosts every three seconds.

**Detected System Threshold Interval (Seconds)**
Specify how frequently (in seconds) the module sends reports to the ePO server.

**ePO Extension Version**
Select the Forescout ePO Extension version that is installed on the ePO server. By default, Version 1.3.x is selected. It is recommended that you install the latest version of the Forescout ePO Extension.
Create unique NetBIOS Hostname when required

By default, this option is selected. If it is selected and the Forescout platform cannot resolve the NetBIOS hostname of the detected endpoint, the module creates a unique NetBIOS hostname for the endpoint, based on the MAC address of the endpoint. The format of the created NetBIOS hostname is MAC-<endpoint MAC address>. This option must be selected when using the ePO Add to Detected System action.

Create unique DNS Name when required

By default, this option is selected. If it is selected and the Forescout platform cannot resolve the DNS name of the detected endpoint, the module creates a unique DNS name for the endpoint, based on the IP address of the endpoint. The created DNS name replaces the dot (.) separators of the IP address with dash (-) separators. For example, the IP address 172.16.254.1 becomes the endpoint DNS name 172-16-254-1. This option must be selected when using the ePO Add to Detected System action.

ePO Automatic Response Credentials:
Enter the credentials for ePO automatic responses.

Authentication Key
Enter the authentication key.

Verify Authentication Key
Re-enter the authentication key to verify it.

2. Select Next. The ePO Database Configuration pane opens.

Configure ePO Database Credentials

Configure ePO database credentials if you are resolving Forescout ePO properties. See Detect Endpoints with ePO Attributes -- Policy Properties for details about these properties. This configuration lets you access the ePO MSSQL database, which is required for retrieving properties.
To configure ePO database credentials:

1. In the ePO Database Credentials pane of the Add ePO Server wizard, configure the credentials as follows:

<table>
<thead>
<tr>
<th><strong>Enable ePO database access</strong></th>
<th>By default, this option is selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Server Name</strong></td>
<td>Enter the Fully Qualified Domain Name (FQDN) or the IPv4 address of the McAfee ePO database server.</td>
</tr>
<tr>
<td><strong>Server Instance</strong></td>
<td>Enter the name of the database.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Select the port configured on the server to access the ePO database.</td>
</tr>
<tr>
<td><strong>Use encrypted connection</strong></td>
<td>By default, this option is selected. This option indicates the SQL connection to the ePO database must be encrypted.</td>
</tr>
</tbody>
</table>
Validate ePO Database Server Certificate

Select this option to validate the identity of the third-party server before establishing a connection, when the Plugin 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), as well as the server certificate, 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.

Name
Enter the ePO database name.

User Name
Enter a user name with select query permissions on the ePO database. To specify an existing Windows user account, include the domain name using the standard \Domain\username format.

Password
Enter the password assigned to the user.

Verify Password
Re-enter the password to verify it.

Request Threshold
Define the maximum number of query requests to the ePO database within the defined Request Threshold Interval. The default is 20.

Define the maximum number of query requests the connecting CounterACT device can send to the ePO database during a given time period. For example, the default values process up to 20 DB queries per second. A higher threshold can potentially overload the SQL server, while a lower threshold can cause the ePO module to get behind processing resolve requests.

Request Threshold Interval (Seconds)
Specify how often the module queries the database. It is recommended that you use the default setting (1 second).

2. Select Finish and then select Apply.

Assign CounterACT Devices

This section covers selecting a connecting CounterACT device when adding an ePO Server.
To configure CounterACT devices:

1. In the CounterACT Devices pane of the Add ePO Server wizard, select the Connecting CounterACT device to communicate with the ePO server. This device handles all communication with the target ePO server. It forwards requests submitted to it by the other CounterACT devices assigned to this server, and it returns the responses to the Forescout platform.

2. If other ePO servers have already been added, select one of the following options:
   - **Assign All Devices by Default**. Automatically assign all CounterACT devices, excluding devices explicitly assigned to another ePO server, to the ePO server defined in this configuration. If selected, this ePO server becomes the *default* server. Only one server can be the default server. If only one server is defined, it is the default server.
   - **Assign Specific Devices**. Assign other CounterACT devices to communicate with the ePO server through this connecting device. Each CounterACT device can be assigned to *only* one ePO server.
If no other ePO servers have been added to the module, all devices are assigned to this ePO server by default. In an environment with multiple ePO servers, consider the topology of your network when deciding which CounterACT devices to assign to each ePO server.

3. Select **Finish**. The new ePO server is displayed in the McAfee ePO pane.

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

### Test the Module

After Forescout eyeExtend for McAfee ePolicy Orchestrator has been configured, perform a test.

- If ePO extension configuration was enabled in the Add ePO Server wizard, the test verifies that the module is connected to the Forescout Extension and works properly.

- If ePO database access was enabled in the Add ePO Server wizard, the test verifies that:
  - The module can access the McAfee ePO MSSQL database.
  - Database query results on the tested host are correct.

**To test the connection:**

1. In the Console, select **Options** from the **Tools** menu. The Options pane opens.

2. Select the **Modules** folder.

3. In the **Modules** pane, select **McAfee ePO**. The McAfee ePO pane opens.

4. Select the **Test** tab.
5. In the **Host IP Address** field, enter the IP address of the host to be tested.

   - **Add this Host to the ePO Detected System** is selected by default. This adds the host to the RSD table on the ePO server.

   - **Display ePO Agent Managed State** is selected by default. This indicates whether the ePO Agent is managed or not.

6. Select **Display Point Product Properties for All Point Products** to collect additional information as needed for troubleshooting all attached McAfee point products.

7. Select **Display Point Product Setting for Specific Point Product** and enter the **Point Product Family Name**. Select this option to collect additional information as needed for troubleshooting specific McAfee point products.

8. Select **Display Detected System Table Properties** to enumerate the System Table Properties detected on the remote ePO server.

9. Select **Apply**.

10. Select the Device tab.

11. Select a Connecting CounterACT Device and then select **Test**.

   The test is performed, and the results are displayed in the Testing dialog box.

12. When testing is complete, select **Close**.
Install and Configure the Forescout ePO Extension (Optional)

This section describes how to install the Forescout ePO Extension. Use the extension when using the Forescout platform to report newly detected hosts to the ePO Detected System. The extension lets you integrate with the Detected Systems Module.

When working with the extension, you must configure the Forescout ePO Extension Configuration parameters. See Configure the Forescout ePO Extension.

Install the Forescout ePO Extension

This section describes how to install the Forescout ePO Extension.

To install the extension:

1. Download the Forescout ePO Extension file from the CounterACT Appliance location, in the format http://<appliance-ip>/epo/extension.jsp.
2. Save the downloaded file.
3. Log on to the ePO Enterprise server as an administrator.
4. In the McAfee ePO Console, select Extensions from the Software list.
5. Select Install Extension.
6. Go to the location where you saved the Forescout ePO Extension file and select OK to install the file. The ForeScout CounterACT extension is displayed in the Extensions pane.

Configure the ePO Detected System

This section describes the steps to configure permission sets and an ePO user account for the ePO Detected System.

- Define Permission Sets
- Configure a User

Define Permission Sets

This section describes how to define and run a new permission set that can be assigned to users.
Extension permission parameters are used when working with the ePO Add to Detected System action.

**To define a new permission set and add extension permissions:**

1. Log on to the ePO Enterprise server as an administrator.
2. In the ePO Console, select **Permission Sets** from the User Management list.

3. Select **New Permission Sets**.

4. Enter a name for the permission set in the **Name** field, and select one or more users other than the admin or system users.

   In the example, the permission set name is **Permissions_for_West_Coast**.

5. Select **Save**. The permission set is saved.
6. Select the new permission set, select ForeScout CounterACT, and then select Edit.

7. Select Run Permission and then select Save. The permissions are saved.
Configure a User

The credentials defined in the ePO user account should also be used when configuring the Forescout ePO Database Configuration parameters. See Configure ePO Database Credentials.

To configure a user:

1. Log on to the ePO server as an administrator.
2. In the McAfee ePO Console, select Users from the User Management list.
3. Create a user or select a user. Do not select the admin or system users.

4. Verify that the **Manually assigned permission sets** includes the correct permission set.

---

**Work with McAfee ePO Policy Templates**

This module provides the following policy templates used to detect, manage, and remediate endpoints.

- [ePO Agent Communications Audit Policy Template](#)
- [ePO Client Audit Policy Template](#)
- [ePO Endpoint Test Policy Template](#)

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

**ePO Agent Communications Audit Policy Template**

This template is used to create a policy that detects the last time the ePO Agent communicated with the ePO server.

Remediation actions can be used to:

- Notify the Forescout administrator that the ePO Agent has not reported recently.
- Send a Syslog message that the ePO Agent has not reported recently.
The policy organizes hosts into groups based on how long since the most recent communication.

**To create an ePO Agent Communications Audit policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the McAfee ePO folder and select **ePO Agent Communications Audit**.

4. Select **Next**.
Policy names are displayed in the Policy Manager, the Views pane, NAC Reports, and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criterion is to be met or not.
   - Avoid having another policy with a similar name.

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

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

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

8. Select **OK**. The added range is displayed in the Scope pane.
9. Select **Next**. The Main Rule pane opens. See **How Endpoints are Detected and Handled** for details of default policy logic.
10. Select **Next**. The Sub-Rules pane opens.
11. Review the sub-rule conditions and actions, and then select **Finish**.
12. In the Policy Manager, select **Apply** to save the policy. The Policy Manager refreshes with the ePO Agent Communications Audit rule and all the sub-rules.
13. Select **Start** to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

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 of this policy checks if this host is managed by the McAfee ePO server. The Condition Criteria section is populated by default.
Sub-Rules

The sub-rules of the ePO Agent Communications Audit policy detects when the ePO Agent last communicated with the ePO server.
The Sub Rules pane lists all the Sub-Rules associated with the ePO Agent Communications Audit policy.

- Refer to the Forescout Administration Guide to understand the symbols listed in the Actions column.

**ePO Client Audit Policy Template**

This template is used to create a policy that checks for both NAC and ePO-managed endpoints and categorizes the hosts accordingly.

- It is a known limitation that Forescout eyeExtend for McAfee ePolicy Orchestrator does not support dual-homed hosts.

Optional remediation actions can be set to:
- Notify the Forescout administrator about the Managed state of the endpoint.
- Send a Syslog message about the Managed state of the endpoint.

- For an endpoint to be considered NAC-managed, it must belong to the group Managed Windows Devices.

**To create an ePO Client Audit policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the McAfee ePO folder and select **ePO Client Audit**.
4. Select **Next**.

![Policy Wizard - Step 2 of 5]

- **Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.**

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as *My_Compliance_Policy*.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria is to be met or not.
   - Avoid having another policy with a similar name.

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

7. Use the IP Address Range dialog box to define which endpoints are inspected.
The following options are available:

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

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

9. Select **Next**. The Main Rule pane opens. See **How Endpoints are Detected and Handled** for details of default policy logic.

10. Select **Next**. The Sub-Rules pane opens.

11. Review the sub-rule conditions and actions, and then select **Finish**.

12. In the Policy Manager, select **Apply** to save the policy. The Policy Manager refreshes with the ePO Client Audit rule and all the sub-rules.

13. Select **Start** to execute the policy.

### How Endpoints are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

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 of this policy checks if the endpoint is a member of the group *Windows*. The Condition Criteria section is populated by default.
The sub-rules of the ePO Client Audit policy detects several types of managed states.

The Sub Rules pane lists all the Sub-Rules associated with the ePO Client Audit policy.
Refer to the Forescout Administration Guide to understand the symbols listed in the Actions column.

**ePO Endpoint Test Policy Template**

This template is used to create a policy that verifies at least one communication has been received from the ePO Agent within the given time period.

**To create an ePO Endpoint Test policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the McAfee ePO folder and select **ePO Endpoint Test**.
4. Select **Next**.
5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria is to be met or not.
   - Avoid having another policy with a similar name.

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

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

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

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

**9.** Select **Next**. The Main Rule pane opens. See [How Endpoints are Detected and Handled](#) for details of default policy logic.

**10.** Select **Next**. The Sub-Rules pane opens.

**11.** Review the sub-rule conditions and actions, and then select **Finish**.

**12.** In the Policy Manager, select **Apply** to save the policy. The Policy Manager refreshes with the ePO Endpoint Test rule and all the sub-rules.

**13.** Select **Start** to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

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 of this policy checks if the most recent communication with the ePO Agent is older than 8 hours. The Condition Criteria section is populated by default.
Main Rule

Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

- All criteria are True

Criteria

- ePO Agent Last Communication - Older than 6 hours

Actions

Actions are applied to hosts matching the above condition.

- Add to Group
- Send Email
- Send Message to Syslog
Sub-Rules

By default, there are no sub-rules in the ePO Endpoint Test policy; however, you can add your own.

The Sub Rules pane lists all the Sub-Rules associated with the ePO Endpoint Test policy.

Refer to the Forescout Administration Guide to understand the symbols listed in the Actions column.

Create Custom ePO Policies

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct the Forescout platform to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

This section describes how to create a policy that detects endpoints with ePO attributes. In addition, you can use other actions to handle hosts detected by your McAfee ePO policy.

Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain Operating System or having a certain application installed.
Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to an isolated VLAN or send the device user or IT team an email.

In addition to the properties and actions bundled in the Forescout platform and available for detecting and handling endpoints, you can work with McAfee ePO related properties and actions to create the custom policies. These items are available when you install the module.

For more information about working with policies, select Help from the Policy Wizard.

To create a custom policy:

1. Log in to the Console and select Policy.

   ![Policy Wizard](image)

2. In the Policy Manager, select Add. The Policy Wizard opens.
3. Select Custom.
4. Select Next.
5. Enter a policy name and select **Next**. The policy Scope pane opens.
6. Enter a policy scope and select **Next**. The Main Rule pane opens.
7. Create policy rules. You can incorporate ePO rules as main rules or sub-rules. Select Help for details about working with rules.

8. In either the Main Rule or Sub-Rules panes, select Add in the Condition section. The Properties list opens. Go to the McAfee ePO folder and expand it. The ePO properties are displayed. For a description of the properties, see Detect Endpoints with ePO Attributes – Policy Properties.

9. Select and configure the appropriate condition properties, and then select and configure the appropriate actions.

10. Select Finish to save the policy.
Detect Endpoints with ePO Attributes – Policy Properties

The following properties describe ePO attributes that can be discovered by working with McAfee ePO policies. These properties are available when you install Forescout eyeExtend for McAfee ePO.

To access McAfee ePO properties:
1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the McAfee ePO folder in the Properties tree. The following properties are available:
   - ePO Agent Last Communication
   - ePO Agent Managed State
   - ePO DB is UP
   - ePO Tags
   - ePO Point Product Properties
   - ePO Point Product Setting Boolean
   - ePO Point Product Setting Date
   - ePO Point Product Setting Integer
   - ePO Point Product Setting String
   - ePO RSD Detected System Linked Table Boolean
   - ePO RSD Detected System Linked Table Date
   - ePO RSD Detected System Linked Table Integer
   - ePO RSD Detected System Linked Table String
   - ePO RSD Detected System Table Boolean
   - ePO RSD Detected System Table Date
   - ePO RSD Detected System Table Integer
   - ePO RSD Detected System Table String

ePO Agent Last Communication

Use this property to detect hosts that last communicated with the ePO server (via the ePO agent) at a specific time or before a certain date. For example, detect hosts that last communicated with the ePO server more than a week ago or more than three hours ago.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure ePO Database Credentials for details.
ePO Agent Managed State

Use this property to detect endpoints that are either managed or not managed by the ePO server. To detect managed hosts, select *Meets the following criteria*. To detect unmanaged hosts, select *Does not meet the following criteria*.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

If the endpoint is not managed, you can [Report Detected Hosts to the ePO Detected System](#).
**ePO DB is UP**

Use this property to determine whether Forescout eyeExtend for McAfee ePolicy Orchestrator can access the ePO database.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

**ePO Tags**

Use this property to detect endpoints with specific ePO tags.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

**ePO Point Product Properties**

Use this property to detect endpoints based on the settings of their installed Point Product properties. For more information on Point Product properties and their settings, refer to your ePO administrator or to McAfee ePO documentation.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.
Database References

<table>
<thead>
<tr>
<th>ePO DB Column</th>
<th>Attribute</th>
<th>Type</th>
<th>ePO DB Table Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProductFamily</td>
<td>ProductFamily</td>
<td>String</td>
<td>ePOProductFamilies</td>
</tr>
<tr>
<td>FamilyDispName</td>
<td>FamilyDispName</td>
<td>String</td>
<td>ePOProductFamilies</td>
</tr>
<tr>
<td>ProductCode</td>
<td>ProductCode</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Engine Version</td>
<td>EngineVer</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Engine (x64) Version</td>
<td>EngineVer64</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Dat Version</td>
<td>DATVer</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Product Version</td>
<td>ProductVersion</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Dat Date</td>
<td>DATDate</td>
<td>Date</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Installed Path</td>
<td>InstalledPath</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Service Pack</td>
<td>Servicepack</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>Hotfix/Patch Version</td>
<td>Hotfix</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>License Status</td>
<td>LicenseStatus</td>
<td>String</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>ExpirationDate</td>
<td>ExpirationDate</td>
<td>Date</td>
<td>ePOProductProperties</td>
</tr>
<tr>
<td>LastInstalled</td>
<td>LastInstalled</td>
<td>Date</td>
<td>ePOProductProperties</td>
</tr>
</tbody>
</table>
ePO Point Product Setting Boolean

Use this property to detect endpoints based on the Boolean value of a specific Point Product setting. For more information on Point Product properties and their settings, refer to your ePO administrator or to McAfee ePO documentation.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure ePO Database Credentials for details.

---

ePO Point Product Setting Date

Use this property to detect endpoints with a specific Point Product setting based on a date. For more information on Point Product properties and their settings, refer to your ePO administrator or to McAfee ePO documentation.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure ePO Database Credentials for details.
ePO Point Product Setting Integer

Use this property to detect endpoints based on the integer value of a specific Point Product setting. For example, `CheckNetworkMessageInterval` for `VirusScan Enterprise`. For more information on Point Product properties and their settings, refer to your ePO administrator or to McAfee ePO documentation.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure ePO Database Credentials for details.
**ePO Point Product Setting String**

Use this property to detect endpoints based on the string value of a specific Point Product setting. For more information on Point Product properties and their settings, refer to your ePO administrator or to McAfee ePO documentation.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

**ePO RSD Detected System Linked Table Boolean**

Use this property to detect endpoints based on the Boolean value in a specific column in a table that is linked to the RSDDetectedSystemProperties Table. Enter the **Table Name, Column Name**, and **Host ID**.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.
ePO RSD Detected System Linked Table Date

Use this property to detect endpoints having a specific value in a specific column in a table that is linked to the RSDDetectedSystemProperties table, based on a specific date. Enter the **Table Name**, **Column Name**, **Host ID**, and the date information.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

---

ePO RSD Detected System Linked Table Integer

Use this property to detect endpoints based on the integer value in a specific column in a table that is linked to the RSDDetectedSystemProperties table. Enter the **Table Name**, **Column Name** (for example, HealthLevel in NaHostStatus), **Host ID**, and the integer value.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.
ePO RSD Detected System Linked Table String

Use this property to detect endpoints based on the string value in a specific column in a table that is linked to the RSDDetectedSystemProperties table. Enter the **Table Name**, **Column Name**, **Host ID**, and the string value.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in the Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.
**ePO RSD Detected System Table Boolean**

Use this property to display endpoints based on the Boolean value in a specific column in `RSDDetectedSystemProperties` Table. Enter the table **Column Name**.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

**ePO RSD Detected System Table Date**

Use this property to detect endpoints having a specific value in a specific column in `RSDDetectedSystemProperties` table, based on a date. Enter the table **Column Name** and the date information.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.
**ePO RSD Detected System Table Integer**

Use this property to detect endpoints based on the integer value in a specific column in `RSDDetectedSystemProperties` table. Enter the table **Column Name** and the integer value.

Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure ePO Database Credentials](#) for details.

**ePO RSD Detected System Table String**

Use this property to detect endpoints based on the string value in a specific column in `RSDDetectedSystemProperties` table. Enter the table **Column Name** and the string value.
Use of this property requires access to the ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure ePO Database Credentials for details.

Manage ePO Endpoints – Policy Actions

The Forescout platform’s actions provide a wide range of tools that assist you in handling ePO endpoints, including:

- Report Detected Hosts to the ePO Detected System

To access actions:

1. Go to the Actions tree from the Policy Actions dialog box.
2. Expand the appropriate folder in the Actions tree.

Report Detected Hosts to the ePO Detected System

Use the Audit > ePO Add to Detected System action in Forescout policies to report endpoints detected by the Forescout platform to the ePO Detected System.

This action is available when the McAfee ePO extension is installed.
Display McAfee ePO Detections

McAfee ePO detections are displayed in the Detections pane.
To ensure that you see these detections:

1. In the Console, right-click a column header in the Detections pane and select Add/Remove.

2. In the left pane, under Properties, expand McAfee ePO.

3. Select the required columns in the left pane and select Add. The columns are moved to the right.

4. Select OK.

Refer to the Forescout Console User Manual or the Console Online Help for more information about displaying and filtering detections in the Detections pane.

Endpoint Module Information

The Forescout® Endpoint Module provides connectivity, visibility, and control to network endpoints through the following Forescout components:

- HPS Agent Manager
- HPS Inspection Engine
- Hardware Inventory Plugin
- Linux Plugin
- Microsoft SMS/SCCM Plugin
- OS X Plugin
The Endpoint Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of the Forescout platform. Components listed above are installed and rolled back with the Endpoint Module.

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 Resources Page, or 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 Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:


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 Portal
The Downloads page on the Forescout Customer 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 Forescout Customer 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.

- **If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.**

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

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 Forescout Help from the Help menu.

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

**Online Documentation**
- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).