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

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

**Concepts and Components** .............................................................................. 6
  Concepts ............................................................................................................ 7
  Components ..................................................................................................... 8
  Considerations ................................................................................................... 9
  What to Do .......................................................................................................... 9

**Requirements** .................................................................................................. 9
  Forescout Requirements ................................................................................... 9
  Forescout eyeExtend (Extended Module) Licensing Requirements ..................... 10
    Per-Appliance Licensing Mode .................................................................... 10
    Flexx Licensing Mode ............................................................................... 11
    More License Information ........................................................................... 12
  Third-Party Requirements ............................................................................. 12

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

**Configure the Module** ...................................................................................... 13
  Configure the Forescout ePO Extension .......................................................... 14
  Configure Primary ePO Database .................................................................... 17
  Assign CounterACT Devices .......................................................................... 19
  Configure Secondary ePO Database .............................................................. 20
  DB Search Criteria ........................................................................................... 22

**Test the Module** .............................................................................................. 23

**Install and Configure the Forescout ePO Extension** ......................................... 25
  Install the Forescout ePO Extension ............................................................... 25
  Configure the ePO Detected System ............................................................... 28
    Configure a User .......................................................................................... 28
    Define and Assign Permission Sets ............................................................... 30
  Automatic Responses Configurations ............................................................... 35
    Define an ePO Registered Server ................................................................ 36
    Configure the ePO Automatic Response Credentials ................................... 38
    Configure Automatic Responses .................................................................. 39

**Work with McAfee ePO Policy Templates** .................................................... 41
  ePO Agent Communications Audit Policy Template ............................................ 41
  ePO Client Audit Policy Template ................................................................... 46
ePO Endpoint Test Policy Template ................................................................. 50
ePO Event Received Policy Template ............................................................. 54

Create Custom ePO Policies ........................................................................ 58
Detect Endpoints with ePO Attributes – Policy Properties ......................... 62
ePO Agent Last Communication .................................................................. 62
ePO Agent Managed State ......................................................................... 63
ePO DB is UP .......................................................................................... 64
ePO Tags .............................................................................................. 64
ePO Events ........................................................................................... 64
ePO Point Product Properties .................................................................... 65
ePO Point Product Setting Boolean ............................................................ 66
ePO Point Product Setting Date .................................................................. 67
ePO Point Product Setting Integer .............................................................. 67
ePO Point Product Setting String ................................................................. 68
ePO RSD Detected System Linked Table Boolean ....................................... 68
ePO RSD Detected System Linked Table Date ............................................. 69
ePO RSD Detected System Linked Table Integer ......................................... 69
ePO RSD Detected System Linked Table String .......................................... 70
ePO RSD Detected System Table Boolean .................................................. 70
ePO RSD Detected System Table Date ....................................................... 71
ePO RSD Detected System Table Integer ................................................... 71
ePO RSD Detected System Table String .................................................... 72

Manage ePO Endpoints – Policy Actions ....................................................... 72
Report Detected Hosts to the ePO Detected System .................................. 72

Display McAfee ePO Detections .................................................................. 73

Endpoint Module Information ....................................................................... 75

Additional Forescout Documentation .......................................................... 75
Documentation Downloads ......................................................................... 75
Documentation Portal .................................................................................. 76
Forescout Help Tools .................................................................................. 76
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 can query 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.

Run NAC Actions on Suspicious Endpoints

If ePO detects that an endpoint on the network has become non-compliant, ePO can send the Forescout platform the non-compliant IP address and an event label. The Forescout platform resolves the event as a property on the endpoint and can take automated actions until the endpoint is remediated and becomes compliant. The different actions are based on corporate policy and can include:

- Assigning the endpoint to a VLAN
- Isolating the endpoint by turning off its switch port and preventing it from communicating with the network
- Launching a third-party vulnerability scan through a vulnerability management integration made possible by the orchestration capabilities of the Forescout platform

See ePO Event Received Policy Template for details.
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. See Additional Forescout Documentation for information on how to access this guide.

Additional McAfee ePO Documentation

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

https://support.mcafee.com/ppdocumentation

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.
- Deliver ePO Event information to the Forescout platform and carry out Network Access Control (NAC) actions based on events. See ePO Events 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 Events
  - 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.
- Considerations - setup details and common network structure issues to keep in mind when you implement this module.
Concepts

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

- Use the Forescout ePO Extension when integrating through the following modules:
  - Automatic Responses Module
  - Rogue System Detection Module
- Directly query the ePO database to resolve ePO host properties, with the exception of the ePO Events property.

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.

**Server Type:** Allows the CounterACT device to connect to multiple ePO databases for resolving DB-based host properties queries:

- **Primary:** The standard CounterACT device is the Primary server.
- **Secondary:** Secondary database-only servers can be added that are used for database searches if the database search from the primary server fails.

If the database is configured in the Primary and there are one or more Secondary database servers, a database query first be made to the Primary database and then to each Secondary database until a match is made.
Considerations

**RSD Events:** The ePO Add to Detected System action adds the selected endpoint to the list of Detected Systems on the ePO server. When an endpoint is added to the list, the ePO server can return an ePO event to the Forescout platform. The ePO event uses the label defined in the ePO Automatic Responses module.

**Threat Events:** If an ePO Client is installed on the endpoint, RSD events and also threat events can be sent to the 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 for details.
- Endpoint Module version 1.1 with the HPS Inspection Engine component running. See Endpoint Module Information.
- When working with the Forescout ePO Extension:
  - ePO Extension, version 1.4.0 is required for the full functionality of this release
  - ePO Extension, version 1.3.0 is supported for upgrade
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 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 5.9.1 or 5.10
- 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 the module installation fails.

To install the module:
1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - Per-Appliance Licensing Mode
   - Customer Portal, Downloads Page - Flexx Licensing Mode
   To identify your licensing mode, select Help > About ForeScout from the Console.
2. Download the module .fpi file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

- The installation begins immediately after selecting Install and cannot be interrupted or canceled.
- In modules that contain more than one component, the installation proceeds automatically one component at a time.

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

- Some components are not automatically started following installation.

**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 the **Modules** folder.
3. In the **Modules** pane, select **McAfee ePO**. The McAfee ePO pane opens to the Device tab.
4. Select **Add**. The Add ePO Server wizard opens to the ePO Extension Configuration pane.

5. To configure the module and optional ePO Extension, see [Configure the Forescout ePO Extension](#), [Configure Primary ePO Database](#), 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>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ePO Extension Configuration</td>
<td>Select this option and use the URL format shown to locate the extension file.</td>
</tr>
<tr>
<td>ePO Server</td>
<td>Enter the ePO server as a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the server. If the ePO server is an IPv6 address or a hostname that returns an IPv6 address, the ePO Add to Detected System action adds the IPv6 address. If there is no IPv6 address known to the Forescout platform, the action adds the IPv4 address.</td>
</tr>
<tr>
<td>Server Port Number</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 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 1.4.x is selected. (Version 1.3.x does not support the full functionality of this release, such as ePO events or IPv6.) 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 if you are using the Forescout platform to retrieve ePO Events. (The extension configuration lets you integrate with the Automatic Responses Module that delivers events information.) Use the ePO Events property in a Forescout platform policy to retrieve the information. See ePO Events for details. |
| **Authentication Key** | Enter the local server authentication key. The value must match the authentication key that was entered in Menu > Registered Servers > Details when the ePO server was added. |
| **Verify Authentication Key** | Re-enter the authentication key to verify it. |

2. Select **Next**. The ePO Database Configuration pane opens. See [Configure Primary ePO Database](#).
Configure Primary ePO Database

Configure basic parameters and login credentials for the primary ePO database if you are resolving Forescout ePO properties, including the Events property. 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. See DB Search Criteria.

To configure the primary ePO database:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ePO database access</td>
<td>By default, this option is selected.</td>
</tr>
<tr>
<td>Database Server Name</td>
<td>Enter the database server as a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the database server. If the database server is an IPv6 address, connections to the ePO database are made using the IPv6 address.</td>
</tr>
<tr>
<td>Server Instance</td>
<td>Enter the name of the database.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the port configured on the server to access the ePO database.</td>
</tr>
</tbody>
</table>
### Use encrypted connection

By default, this option is selected. This option indicates the SQL connection to the ePO database must be encrypted.

### Validate ePO DB 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the ePO database name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password assigned to the user.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the password to verify it.</td>
</tr>
<tr>
<td>Request Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>Request Threshold Interval (Seconds)</td>
<td>Specify how often the module queries the database. It is recommended that you use the default setting (1 second).</td>
</tr>
</tbody>
</table>

2. Select **Next**. The CounterACT Devices pane opens. See Assign CounterACT Devices.
Assign CounterACT Devices

Select 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.

4. Select **Apply**.

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

You can also configure a secondary ePO database. See Configure Secondary ePO Database.

## Configure Secondary ePO Database

You can configure multiple secondary database-only servers for resolving DB-based host properties. If there are one or more secondary database servers, a database query is made to the primary database and then to each secondary database until a match is made.

**To configure a secondary database:**

1. After configuring the primary server, in the McAfee ePO pane, select the primary server.

2. Select **Add DB**. The secondary server you are about to configure is associated with the primary server you selected.
3. Configure parameters and credentials as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server Name</td>
<td>Enter the database server as a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the database server. If the database server is an IPv6 address, connections to the ePO database are made using the IPv6 address.</td>
</tr>
<tr>
<td>Server Instance</td>
<td>Enter the name of the database.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the port configured on the server to access the ePO database.</td>
</tr>
<tr>
<td>Use encrypted connection</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 DB 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.

The secondary ePO database has the same Request Threshold and Request Threshold Interval settings as the primary. See Configure Primary ePO Database.

4. Select OK.

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

**DB Search Criteria**

The configuration of the primary and secondary databases lets you access the ePO MSSQL database, which is required for retrieving properties.

Forescout eyeExtend for McAfee ePolicy Orchestrator searches the MSSQL database to retrieve endpoint properties, such as, when there is a policy that checks if an endpoint is managed.

By default, MSSQL database searches check the following criteria, in the following order:

- FQDN
- NBT host (the name of the Windows-only field containing the NetBIOS name)
- MAC address

The order is from more unique criteria to less unique criteria. The DB search is successful with the first criteria matched.
The default DB search criteria can be changed. Use the fstool command to change the config.db_search_criteria.value property on the focal Appliance.

To change the default DB search criteria, set the config.db_search_criteria.value property. The valid values are: fqdn, nbhost, and mac. For example:

```
# fstool epo set_property config.db_search_criteria.value mac
```

In this example, only the MAC address is matched. This maintains the DB search criteria used in prior releases of Forescout eyeExtend for McAfee ePO.

You can also use the fstool command to change the default order of the DB search criteria.

---

**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.
- Secondary databases are also verified.

**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 Address** field, enter the FQDN or the IPv4 or IPv6 address of the host to be tested.

- **Add this Host to the ePO Detected System** adds the host to the RSD table on the ePO server.

- **Display ePO Agent Managed State** 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

This section describes how to install the optional 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.
- Receive ePO Events to be used as a property in Forescout platform policies. The extension lets you integrate with the Automatic Responses 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. Verify that you have added the McAfee ePO Extension to Options > Access > Web. Refer to the Define Web Access section in the Forescout Administration Guide for details. See Additional Forescout Documentation for information on how to access this guide.
2. Download the Forescout ePO Extension file from the CounterACT Appliance location, in the format http://<appliance-ip>/epo/extension.jsp.

3. Save the downloaded file.

4. Log on to the ePO Enterprise server as an administrator.

5. In the McAfee ePO Console, select **Extensions** from the Software list.
6. If there is already a ForeScout CounterACT extension installed, select it and check its version. If the version is not 1.4.0, select **Remove**.

7. Select **Install Extension**.

8. Go to the location where you saved the Forescout ePO Extension file and select **OK** to install the file. The **ForeScout CounterACT** extension, version 1.4.0, is displayed in the Extensions pane.
Configure the ePO Detected System

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

- Configure a User
- Define and Assign Permission Sets

Configure a User

The credentials defined in the ePO user account should be used when configuring the Forescout ePO Database Configuration parameters. See [Configure Primary ePO Database](#).

**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. Select **New User** to create a new user.

4. Enter a User name, enable the Logon status, and then select an Authentication type and enter the credentials for it.
5. Scroll down the New User page to enter optional information. You do not have to select anything in the **Manually assigned permission sets** field. However, if you have already defined a permission set (see Define and Assign Permission Sets for details), you can select it here. Select **Save**.

In the example, a new non-admin user, ca_user, is created.

**Define and Assign 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 or when creating Registered Servers or Automatic Responses while logged in with a non-admin ePO user.

**To define a new permission set and assign permissions:**

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

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. See [Configure a User](#) for details on configuring users.

   In the example, the permission set name is *Permissions for West Coast* and the non-admin user is *ca_user*.

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

7. Select **Run Permission** and then select **Save**.
8. To give the non-admin user create and edit permissions for Automatic Response, select the permission set, scroll to **Automatic Response**, and then select **Edit**. See **Configure Automatic Responses** for details.

9. Select the Create, edit, view, and cancel Responses; view Response results in the Server Task Log option and then select **Save**.
10. To give the non-admin user create and edit permissions for Registered servers, select the permission set, scroll to Registered servers, and then select Edit. See Define an ePO Registered Server for details.

11. Select the View, create, and edit registered servers option for CounterACT and then select Save.

12. To give the non-admin user create and edit permissions for Rogue System Detection, select the permission set, scroll to Rogue System Detection, and then select Edit.
13. Select the Create and edit Rogue System information; manage Rogue Sensors; Deploy Agents and Add to System Tree option and then select **Save**.

The assigned permission sets are displayed.

**Automatic Responses Configurations**

To use the Forescout platform to retrieve ePO Events and configure Automatic Responses parameters.

- Define an ePO Registered Server
- Configure Automatic Responses
You also need to configure the authentication key in the Forescout ePO Extension Configuration, ePO Automatic Response Credentials section. See Configure the Forescout ePO Extension.

Define an ePO Registered Server

Register access from the ePO server to the Forescout platform.

To define an ePO registered server:

1. Log on to the ePO server as an administrator.
2. In the McAfee ePO Console, select Registered Servers from the Configuration list.

4. In the Server type drop-down menu, select **CounterACT**. Enter a Name and enter Notes (optional).

5. Select **Next**.
6. In the **Server Name** field, enter the hostname or IP address of the connecting CounterACT device.

7. Enter and confirm an authentication key. This key must be copied to the Forescout ePO Extension Configuration, ePO Automatic Response Credentials section. See [Configure the Forescout ePO Extension](#).

8. Select **Test Connection** to test the connection.

9. Select **Save**. The registered server is saved.

Configure the ePO Automatic Response Credentials

Configure the options in the **ePO Automatic Response Credentials** section if you are using the Forescout platform to retrieve *EPO_Events*. (The extension configuration lets you integrate with the Automatic Responses Module that delivers Events information.)
In the **ePO Automatic Response Credentials** section, enter and verify the local server Authentication Key.

This value must match the authentication key that was entered in the **Registered Servers** screen when the ePO server was added.

Use the **ePO Events** property in a Forescout platform policy to retrieve the information. See [ePO Events](#) for details.

### Configure Automatic Responses

#### To define automatic responses:

1. Log on to the ePO server as an administrator.
2. In the McAfee ePO Console, select **Automatic Responses** from the Automation list.

3. Select **New Response**.
4. In the Response Builder wizard, define tabs 1-3 as required. Ensure that the Automatic Response **Status** is **Enabled**.

5. In the **4 Actions** tab, **What actions** drop-down menu, select **Forward Event to ForeScout CounterACT**.
6. In the **ePO Event Label** section, enter a name for the event that you want the Forescout platform policy to detect. This name is displayed in the ePO Events property when the event occurs. To view an example of how to instruct the Forescout platform to detect this event, select **See example**.

7. In the **Host IP Address** or **Host Name** section, select a variable for the events.

8. Select **Next** to review the values set for the Automatic Responses.

9. Select **Save**.

---

**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**
- **ePO Event Received Policy Template**

It is recommended that you have a basic understanding of Forescout policies before working with the templates. Refer to the Policy Management and Policy Templates chapters of the *Forescout Administration Guide*. See *Additional Forescout Documentation* for information on how to access this guide.

**ePO Agent Communications Audit Policy Template**

Use this template to create a policy that detects the last time the ePO Agent communicated with the ePO server. The policy organizes hosts into groups based on how long since the most recent communication.
Optional 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

**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**.
5. Enter a name for the policy. Optionally, enter a description.

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**.
In the Condition section, the predefined criteria is ePO Agent Managed State. The main rule of this policy checks if this host is managed by the McAfee ePO server.

10. (Optional) To add another condition, select Add in the Condition section. See Detect Endpoints with ePO Attributes – Policy Properties for details.

11. (Optional) To add an action, select Add in the Actions section. See Manage ePO Endpoints – Policy Actions for details.

12. Select Next.
In the Sub-Rules pane, the predefined sub-rules for the policy are displayed. The sub-rules of the ePO Agent Communications Audit policy detects when the ePO Agent last communicated with the ePO server.

13. (Optional) Select a sub-rule and then select **Edit** to modify its settings or select **Add** to add a sub-rule.

14. Select **Finish**.

15. In the Policy Manager, select **Apply** to save the policy.

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

---

**ePO Client Audit Policy Template**

Use this template 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 used 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**.

5. Enter a name for the policy. Optionally, enter a description.

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**.
In the Condition section, the predefined criteria is Member of Group - Windows. The main rule of this policy checks if the endpoint is a member of the group Windows.

10. (Optional) To add another condition, select Add in the Condition section. See Detect Endpoints with ePO Attributes – Policy Properties for details.

11. (Optional) To add an action, select Add in the Actions section. See Manage ePO Endpoints – Policy Actions for details.

12. Select Next.
In the Sub-Rules pane, the predefined sub-rules for the policy are displayed. The sub-rules of the ePO Client Audit policy detects several types of managed states.

13. (Optional) Select a sub-rule and then select Edit to modify its settings or select Add to add a sub-rule.


15. In the Policy Manager, select Apply to save the policy.

16. Select Start to execute the policy.

**ePO Endpoint Test Policy Template**

Use this template to create a policy that verifies at least one communication has been received from the ePO Agent within the given time period. The policy puts failed hosts into the group: ePO Agent Endpoint Test Failures.

Optional remediation actions can be used to:

- Notify the Forescout administrator that the Agent endpoint test failed
- Send a Syslog message that the endpoint test failed

**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. Enter a name for the policy. Optionally, enter a description.

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**.
In the Condition section, the predefined criteria is ePO Agent Last Communication – Older than 8 hours. The main rule of this policy checks if the most recent communication with the ePO Agent is older than 8 hours.

10. (Optional) To add another condition, select Add in the Condition section. See Detect Endpoints with ePO Attributes – Policy Properties for details.

11. (Optional) To add an action, select Add in the Actions section. See Manage ePO Endpoints – Policy Actions for details.

12. Select Next.
By default, there are no sub-rules in the ePO Endpoint Test policy.

13. (Optional) Select **Add** to add a sub-rule.

14. Select **Finish**.

15. In the Policy Manager, select **Apply** to save the policy.

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

**ePO Event Received Policy Template**

Use this template to create a policy that categorizes ePO Events received. The policy puts hosts into a group based on key words in the event matching the key word of a specific sub-rule. If none of the key words are found in any of the sub-rules, the Forescout platform puts the host into an Un-categorized group.

Optional remediation actions can be used to:

- Notify the Forescout administrator that a key word from an ePO Event has matched a key word defined in a sub-rule
- Send a Syslog message that a key word from an ePO Event has matched a key word defined in a sub-rule

**To create an ePO Event Received 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 Event Received**.

![Policy - Wizard - Step 1](image)

4. Select **Next**.

![Policy - Wizard - Step 2 of 5](image)

5. Enter a name for the policy. Optionally, enter a description.

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 listed in the Scope pane.

9. Select Next.
In the Condition section, the predefined criteria is ePO Events – Any Value Within the last 30 weeks. The main rule of this policy checks for ePO Events that have occurred within the last 30 weeks.

10. (Optional) To add another condition, select Add in the Condition section. See Detect Endpoints with ePO Attributes – Policy Properties for details.

11. (Optional) To add an action, select Add in the Actions section. See Manage ePO Endpoints – Policy Actions for details.

12. Select Next.
In the Sub-Rules pane, the predefined sub-rules for the policy are displayed.

Each sub-rule of the ePO Events Received policy detects a specific key word or phrase in an ePO Event received within the last week. For example, the first sub-rule in the image below matches if the keyword EICAR (European Institute for Computer Antivirus Research) was an ePO Event Received in the last week.

13. (Optional) Select a sub-rule and then select Edit to modify its settings or select Add to add a sub-rule.


15. In the Policy Manager, select Apply to save the policy.

16. Select Start to execute the policy.

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**.

2. In the Policy Manager, select **Add**. The Policy Wizard opens.

3. Select **Custom**.

4. Select **Next**.
5. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
6. Enter a policy scope and select **Next**.
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 Events
   - 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) 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 an ePO database.

![Image of ePO DB is UP condition](image)

ePO Tags

Use this property to detect endpoints with specific ePO tags.

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

![Image of ePO Tags condition](image)

ePO Events

Use this property to detect endpoints on which specific ePO Events occurred. When ePO events are detected, the Forescout platform creates an admission event, which initiates a policy recheck. You can carry out NAC actions based on the ePO Events detected.

The value entered is case-sensitive.

Use of this property requires that you configure the Forescout ePO extension (see Install and Configure the Forescout ePO Extension) and configure ePO Extension parameters in the module (see Configure the Forescout ePO Extension).
**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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) 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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database for details.

![ePO Point Product Setting String Diagram]

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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database for details.

![ePO RSD Detected System Linked Table Boolean Diagram]
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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) for details.

![Image of ePO RSD Detected System Linked Table Date](image)

---

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 `NaCHostStatus`), **Host ID**, and the integer value.

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

![Image of ePO RSD Detected System Linked Table Integer](image)
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 an ePO database. To ensure access, verify that you have configured ePO database credentials in the Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) for details.

![Image of ePO RSD Detected System Linked Table String](image)

---

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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See [Configure Primary ePO Database](#) for details.

![Image of ePO RSD Detected System Table Boolean](image)
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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database for details.

![ePO RSD Detected System Table Date](image)

---

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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database for details.

![ePO RSD Detected System Table Integer](image)
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 an ePO database. To ensure access, verify that you have configured ePO database credentials in Forescout eyeExtend for McAfee ePolicy Orchestrator. See Configure Primary ePO Database 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 Audit 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 Columns.
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](#), 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 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 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.

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 access information about tasks and topics quickly.

Forescout Administration Guide

- Select Forescout Help from the Help menu.
Plugin Help Files

- After installing the plugin, 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).