ForeScout® Extended Module for McAfee® ePolicy Orchestrator®

Configuration Guide

Version 3.0.1
# Table of Contents

## About the McAfee ePolicy Orchestrator (ePO) Integration
- Use Cases .......................................................... 4
- Additional McAfee ePO Documentation ........................... 5

## About This Module

## Concepts and Components
- Concepts .............................................................. 5
- Components ........................................................... 7
- Considerations .......................................................... 7
- What to Do ............................................................. 7

## Requirements
- CounterACT Software Requirements ................................ 8
- ForeScout Module License Requirements ............................. 8
  - Requesting a License ................................................ 8
  - More License Information ............................................ 9
- Third-Party Requirements ............................................... 9

## Install the Module .................................................. 10

## Configure the Module ................................................ 10
- Configure the CounterACT ePO Extension .......................... 11
- Configure ePO Database Credentials ................................. 13
- Assign CounterACT Devices .......................................... 15

## Test the Module ...................................................... 16

## Install and Configure the CounterACT ePO Extension on the ePO Server ...
- Install the CounterACT ePO Extension ................................ 18
- Configure the ePO Detected System .................................. 19
  - Define Permission Sets ............................................. 19
  - Configure a User ..................................................... 22
- Automatic Responses Configurations .................................. 23
  - Define an ePO Registered Server .................................. 23
  - Configure the ePO Automatic Response Credentials .......... 25
  - Configure the Automatic Responses Module .................... 26

## Run McAfee ePO Policy Templates ................................ 28
- ePO Agent Communications Audit Policy Template .................. 28
- ePO Client Audit Policy Template ..................................... 33
- ePO Endpoint Test Policy Template .................................... 38

---

Version 3.0.1
ePO Event Received Policy Template ............................................. 43

Create Custom ePO Policies .......................................................... 48
  Detecting Endpoints with ePO Attributes – Policy Properties ........... 52
  ePO Agent Last Communication .................................................. 52
  ePO Agent Managed State ....................................................... 53
  ePO DB is UP ........................................................................... 53
  ePO Tags .................................................................................. 54
  ePO Events .............................................................................. 54
  ePO Point Product Properties .................................................... 55
  ePO Point Product Setting Boolean ......................................... 56
  ePO Point Product Setting Date ............................................... 57
  ePO Point Product Setting Integer ........................................... 57
  ePO Point Product Setting String ............................................. 58
  ePO RSD Detected System Linked Table Boolean ....................... 58
  ePO RSD Detected System Linked Table Date ............................. 59
  ePO RSD Detected System Linked Table Integer ....................... 59
  ePO RSD Detected System Linked Table String ......................... 60
  ePO RSD Detected System Table Boolean .................................. 60
  ePO RSD Detected System Table Date ....................................... 61
  ePO RSD Detected System Table Integer ................................... 61
  ePO RSD Detected System Table String .................................... 62

Managing ePO Endpoints – Policy Actions ..................................... 62
  Report Detected Hosts to the ePO Detected System ...................... 62

Display McAfee ePO Detections ..................................................... 63

Additional CounterACT Documentation ....................................... 65
  Documentation Portal .............................................................. 65
  Product Updates Portal ............................................................. 65
  CounterACT Console Online Help Tools ...................................... 65
About the McAfee ePolicy Orchestrator (ePO) Integration

The 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 McAfee ePO and ForeScout CounterACT® to offer greater coverage and control to more devices on the network.

Use Cases

This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About This Module.

Report New Endpoints to ePO

CounterACT offers real-time visibility and control over 100% of the devices on your network. When CounterACT 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

CounterACT 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, CounterACT verifies if the ePO Agent is installed and operational on devices. For more information, see Automatic Responses Configurations.

Run NAC actions on Suspicious Endpoints

If ePO detects that an endpoint on the network has become non-compliant, ePO can send CounterACT the non-compliant IP address and an event label. CounterACT 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 CounterACT orchestration capabilities

For more information, see ePO Event Received Policy Template.
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 CounterACT 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 CounterACT and carry out NAC (Network Access Control) actions based on events. See ePO Events for details.
- Instruct CounterACT to discover endpoints with an extensive range of ePO attributes, such as:
  - ePO Agent Managed State
  - ePO Agent Last Communication
  - ePO Events
  - ePO Point Product Properties

See Detecting Endpoints with ePO Attributes – Policy Properties for details.

Concepts and Components

This section provides a basic overview of McAfee ePO / CounterACT architecture:

- **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

There are two ways CounterACT integrates with McAfee ePO:

- Use the ForeScout CounterACT ePO Extension when integrating through the following module:
  - Automatic Response 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 the CounterACT devices mapped to that server. Using a proxy enables the module to control the query rate from CounterACT 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 the 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.

Considerations

**RSD Events:** The CounterACT 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 returns an ePO event to CounterACT. The ePO event uses the label defined in the ePO Automatic Responses window.

**Threat Events:** If an ePO Client is installed on the endpoint, RSD events and also threat events are 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 CounterACT 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:

- CounterACT Software Requirements
- ForeScout Module License Requirements
Third-Party Requirements

CounterACT Software Requirements

The module requires the following CounterACT releases:

- CounterACT version 7.0.0
- Service Pack 2.3.3 or above (Service Pack 3.0 recommended). It is recommended to install the latest service pack.
- HPS Inspection Engine version 10.2.3 or above
- CounterACT ePO Extension, version 1.3.0 or above. See Install and Configure the CounterACT ePO Extension on the ePO Server.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin you are provided with a 90-day demo module license.

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

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

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

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 CounterACT. 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 CounterACT, 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.

**More License Information**

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

**Third-Party Requirements**

- McAfee ePolicy Orchestrator (ePO) server version 5.3 or 5.9
- When working with the CounterACT ePO Extension:
  - Any of the following McAfee ePolicy Orchestrator (ePO) server versions: 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 CounterACT HPS Inspection Engine Plugin must already be installed or this module installation will fail.

The installation package for the module is in the form of a CounterACT plugin.

**To install the plugin:**

3. Navigate to the Product Updates Portal, ForeScout Modules page and download the plugin .fpi file.
4. Save the file to the machine where the CounterACT Console is installed.
5. Log into the CounterACT Console and select Options from the Tools menu.
7. Select Install. The Open dialog box opens.
8. Browse to and select the saved plugin .fpi file.
9. Select Install.
10. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.
11. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
12. When the installation completes, select Close. The plugin is displayed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.
13. Select the plugin and select Start. The Select Appliances dialog box opens.
14. Select the CounterACT devices on which to start the plugin.
15. Select OK. The plugin runs on the selected devices.

Configure the Module

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

**To configure the module:**

1. In the CounterACT Console, select Options from the Tools menu. The Options dialog box opens.
2. Navigate to and select the Plugins folder.
3. In the Plugins pane, select McAfee ePO, and select Configure. The McAfee ePO pane opens.
4. In the Device tab, select **Add**. The Add ePO Server wizard opens.

**Configure the CounterACT ePO Extension**

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

1. Select the **Enable ePO Extension Configuration** checkbox. Use the URL example shown next to the checkbox to locate the extension file.

2. In the **Server Address** field, enter the ePO server address.

3. In the **Server Port Number** field, enter the ePO server port.

**Configure the ePO Detected System Credentials**

Configure the options in the **ePO Detected System Credentials** section if you are using CounterACT to report rogue hosts to the ePO Detected System.

4. In the **ePO Detected System Credentials** section, enter the credentials of the user that is defined in the ePO Server with RSD (Rogue System Detection) permissions.
   - In the **CounterACT User Name** field, enter the user name defined in the ePO server.
   - In the **CounterACT Password** field, enter the password assigned to the user.
   - In the **Verify Password** field, retype the password to confirm.

5. 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.
   - In the **Detected System Threshold** field, define the maximum number of hosts that can be reported to the ePO server within the defined **Detected System Threshold Interval**.
   - In the **Detected System Threshold Interval (Seconds)** field, indicate the frequency with which the module will send reports to the ePO server.

6. From the **ePO Extension Version** dropdown menu, select the CounterACT ePO Extension version that is installed on the ePO server. By default, **Version 1.3.X** is selected.
   - *It is recommended to install the latest version of the CounterACT ePO Extension.*

7. The **Event Polling Interval** defines how often (in seconds) the module queries the ePO Database for ePO Events. A value of 0 disables this feature (i.e., the ePO Database is never queried for ePO Events.)

8. By default, the checkbox **Create unique NetBIOS Hostname when required** is selected.

   If this option is selected and CounterACT 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.
9. By default, the checkbox **Create unique DNS Name when required** is selected.

If this option is selected and CounterACT 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.

10. Select **Next**. The ePO Database Configuration pane displays.

**Configure ePO Database Credentials**

Configure ePO database credentials if you are resolving CounterACT ePO properties, including the ePO Events property. See Detecting Endpoints with ePO Attributes – Policy Properties for details about these properties. This configuration allows you to access the ePO MSSQL database, which is required for retrieving properties.

To configure ePO database credentials:

1. The **Enable ePO database access** checkbox is selected by default.
2. In the **Server Address** field, enter the IP Address of the McAfee ePO database server.
3. Select one of the following options:
   - In the **Server Instance** field, enter the name of the database.
   - In the **Port** field, enter the port configured on the server to access the ePO database.

4. The **Use encrypted connection** checkbox is selected by default. This indicates the SQL connection to the ePO database must be encrypted.

5. In the **Name** field, enter the ePO database name.

6. In the **User Name** field, 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.

7. In the **Password** field, enter the password assigned to the user.

8. In the **Verify Password** field, retype the password to confirm.

9. Define the maximum number of query requests the connecting CounterACT device can send to the ePO database during a given time span. 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.
   - In the **Request Threshold** field, define the maximum number of query requests to the ePO database within the defined **Request Threshold Interval**. The default is 20.
   - In the **Request Threshold Interval (Seconds)** field, indicate the frequency with which the module will query the database. It is recommended that you have this set to the default setting (1 second.)

10. Select **Finish** and then select **Apply**.
Assign CounterACT Devices

This section covers selecting a connecting CounterACT device.

To configure CounterACT devices:

1. In the CounterACT Devices pane, select the Connecting CounterACT device to communicate with the ePO server. This device will handle 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 back to CounterACT.

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*. 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 displays in the McAfee ePO pane.

Test the Module

After the McAfee ePO Module 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 CounterACT 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 CounterACT Console, select Options from the Tools menu. The Options dialog box opens.
2. Navigate to and select the Plugins folder.
3. In the Plugins 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.
6. The **Add this Host to the ePO Detected System** checkbox is selected by default. This adds the host to the RSD table on the ePO server.

7. The **Display ePO Agent Managed State** checkbox is selected by default. This displays whether the ePO Agent is managed or not.

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

9. Select **Display Point Product Setting for Specific Point Product** and enter the **Point Product Family Name** into the field provided. Select this to collect additional information as needed for troubleshooting to a specific McAfee point products.

10. Select **Display Detected System Table Properties** - select this to enumerate the System Table Properties detected on the remote ePO.

11. Select **Apply**.

12. Select the **Device** tab.

13. Select a Connecting CounterACT Device and then select the **Test** button. The test is performed, and results are displayed in the Test dialog box.

14. When testing is complete, select **Close**.
Install and Configure the CounterACT ePO Extension on the ePO Server

This section describes how to install the CounterACT ePO Extension onto the ePO server. Use the extension when using CounterACT 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 CounterACT policies. The extension lets you integrate with the *Automatic Responses Module*.

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

Install the CounterACT ePO Extension

This section describes how to install the CounterACT ePO Extension.

To install the extension:

1. Download the CounterACT 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 server as an administrator.
4. Select *Menu > Software > Extensions*.

5. The Extensions screen opens. Select the **Install Extension** button. The Install Extension dialog box opens.
6. Navigate to the location where you saved the CounterACT ePO Extension file and select OK to install the file. The ForeScout CounterACT extension appears in the Extensions pane.

Configure the ePO Detected System

This section lists 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 CounterACT ePO Add to Detected System action.

To define a new permission set and add extension permissions:

1. Log on to the ePO server as an administrator.
2. Select Menu > User Management > Permission Sets.
3. Select the **New** button. The New Permission Set dialog box opens.

4. Create a Permission Set **Name** and select one or more **Users** other than the **admin** or **system** users.

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

5. Select **Save**. The Permission Set is saved.
6. Select the newly created permission set, Permissions_for_West_Coast in our example, and then select ForeScout CounterACT > Edit.

7. The Edit Permission Set dialog box opens.

8. 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 CounterACT module ePO Database Configuration parameters. See Configure ePO Database Credentials.

To configure a user:

1. Log on to the ePO server as an administrator.
2. Select Menu > User Management > Users.
3. Create a user or select a user. Do not select the admin or system users.
4. Verify that the **Permission sets** value includes the correct Permission Set.

**Automatic Responses Configurations**

To use CounterACT to retrieve *ePO Events*, configure Automatic Responses parameters.

- Define an *ePO Registered Server*
- Configure the *ePO Automatic Response Credentials*
- Configure the Automatic Responses Module

You'll also need to configure the authentication key in the CounterACT module ePO Extension Configuration, ePO Automatic Response Credentials section. See **Configure the CounterACT ePO Extension**.

**Define an ePO Registered Server**

Register access from the ePO server to CounterACT.

To define an ePO registered server:

1. Select **Menu > Configuration > Registered Servers**.
2. Select the **New Server** button. The Registered Server Builder wizard opens.

![Registered Servers](image1)

3. In the **Server Type** dropdown menu, select **CounterACT**. Enter a **Name** and enter **Notes** (optional).

![Registered Servers](image2)

4. Select **Next**.

![Registered Servers](image3)

5. In the **Server Name** field, enter the hostname or IP address of the connecting CounterACT device.
6. Enter and confirm an authentication key. This key must be copied to the CounterACT plugin ePO Extension Configuration, ePO Automatic Response Credentials section. See Configure the CounterACT ePO Extension.

7. Select Test Connection to test the connection.

8. 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 CounterACT to retrieve EPO_Events. (The extension configuration lets you integrate with the Automatic Responses Module which delivers Events information.)

1. 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 Menu > Registered Servers > Details tab when the ePO server was added.

Use the ePO Events property in a CounterACT policy to retrieve the information. See ePO Events for details.
Configure the Automatic Responses Module

To configure the Automatic Responses:

1. Select **Menu > Automation > Automatic Responses**.

2. Select the **New Response** button.

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

5. In the **What actions** dropdown menu, select **Forward Event to ForeScout CounterACT**.

6. In the **ePO Event Label** section, enter a name for the event that you want the CounterACT policy to detect. This name will be displayed in the ePO Events property when the event occurs. To view an example of how to instruct CounterACT to detect this event, select the **See example** button.

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.
Run McAfee ePO Policy Templates

This module provides the following policy template 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 CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

**ePO Agent Communications Audit Policy Template**

This template is used to create a CounterACT policy that detects the last time the ePO Agent communicated with the ePO server. Remediation actions can be used to:

- Notify the CounterACT 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 CounterACT groups based on how long since the most recent communication.

9. Select **Save**.
To use the ePO Agent Communications Audit policy template:

1. Log in to the CounterACT Console and select the Policy tab.

2. Select Add from the Policy Manager. The Policy Wizard opens.

3. Expand the McAfee ePO folder and select ePO Agent Communications Audit. The ePO Agent Communications Audit pane displays.

4. Select Next. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear 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.


**Define which Endpoints will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

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

> Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select OK. The added range appears in the Scope pane.


**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 CounterACT 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.

10. The Condition Criteria section is populated by default.
11. Select **Next**. The Sub-Rules pane opens.
**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 displays all the Sub-Rules associated with the ePO Agent Communications Audit policy.

- See the CounterACT Console User Guide to understand the symbols listed in the Actions column.

12. Select **Finish**

13. In the CounterACT Policy Manager, select **Apply** to save the policy. The Policy Manager refreshes with the ePO Agent Communications Audit rule and all the sub-rules.

14. Select the **Start** button to execute the policy.

**ePO Client Audit Policy Template**

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

- It is a known limitation that the ePO Module does not support dual-homed hosts.

You can set optional remediation actions to:

- Notify the CounterACT 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 use the ePO Client Audit policy template:

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

4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear 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.


**Define which Endpoints will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

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

   Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range appears 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.
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 CounterACT 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*.

10. The Condition Criteria section is populated by default.
11. Select **Next**. The Sub-Rules pane opens.
Sub-Rules

The sub-rules of the ePO Client Audit policy detects several types of managed states.

The Sub Rules pane displays all the Sub-Rules associated with the ePO Client Audit policy.

See the CounterACT Console User Guide to understand the symbols listed in the Actions column.

12. Select Finish

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

14. Select the Start button to execute the policy.

ePO Endpoint Test Policy Template

This template is for creating a CounterACT policy that verifies at least one communication has been received from the ePO Agent within the given time period.

To use the ePO Endpoint Test policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the McAfee ePO folder and select ePO Endpoint Test. The ePO Endpoint Test pane opens.
4. Select **Next**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear 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.


**Define which Endpoints will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

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

&gt; **Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.**

8. Select **OK**. The added range appears 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.

**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 CounterACT 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.

10. The Condition Criteria section is populated by default.
**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 displays all the Sub-Rules associated with the ePO Endpoint Test policy.

- See the CounterACT Console User Guide to understand the symbols listed in the Actions column.

12. Select **Finish**

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

14. Select the **Start** button to execute the policy.

**ePO Event Received Policy Template**

This template is used to create a CounterACT policy that categorizes ePO Events received. The policy puts hosts into a CounterACT 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, CounterACT puts the host into an Un-categorized group. Optional remediation actions can be used to:

- Notify the CounterACT 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. These actions are disabled by default.

**To use the ePO Event Received policy template:**

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the McAfee ePO folder and select **ePO Event Received**. The **ePO Event Received** pane displays.

4. Select **Next**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear 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**. The Scope pane and IP Address Range dialog box opens.

**Define which Endpoints will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

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

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select OK. The added range appears in the Scope pane.


**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 CounterACT 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 for ePO Events that have occurred within the last 30 weeks.

10. The Condition Criteria section is populated by default.

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

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.

![Sub-Rules Image]

The Sub Rules pane displays all the Sub-Rules associated with the ePO Events Received policy.

- See the CounterACT Console User Guide to understand the symbols listed in the Actions column.

12. Select Finish

13. In the CounterACT Policy Manager, select Apply to save the policy. The Policy Manager refreshes with the ePO Events Received policy rule and all the sub-rules.

14. Select the Start button to execute the policy.

Create Custom ePO Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct CounterACT 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 CounterACT actions to handle hosts detected by your McAfee ePO policy.
Properties
CounterACT policy properties let you instruct CounterACT to detect hosts with specific attributes. For example, create a policy that instructs CounterACT to detect hosts running a certain Operating System or having a certain application installed.

Actions
CounterACT policy actions let you instruct CounterACT 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 bundled CounterACT properties and actions 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 CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select Add from the Policy Manager. The Policy Wizard opens.
4. Select Custom.
5. Select Next. The Policy Wizard, Name pane opens.
6. Enter a policy name and select **Next**. The policy Scope pane opens.

7. Enter a policy Scope and select **Next**. The Main Rule pane opens.
8. Create policy rules. You can incorporate ePO rules as main rules or sub-rules. Select the Help button for details about working with rules.

9. In either the Main Rule or Sub-Rules panes, select the Add button from the Condition section. The Properties list opens. Navigate to and expand the McAfee ePO folder. The ePO properties appear. For a description of the properties, see Detecting Endpoints with ePO Attributes – Policy Properties.

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

11. Select Finish, saving the new policy.
Detecting Endpoints with ePO Attributes – Policy Properties

The following properties describe ePO attributes that can be discovered by working with CounterACT McAfee ePO policies. These properties are available when you install the ForeScout Extended Module for McAfee ePO.

To access McAfee ePO properties:
1. Navigate 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 Events
   - 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 the McAfee ePO Module. 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 the McAfee ePO Module. 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 that the McAfee ePO module 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 the McAfee ePO Module. 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 the McAfee ePO Module. See Configure ePO Database Credentials for details.

The value entered is case-sensitive.

Use of this property requires that you configure the following:

ePO Events

Use this property to detect endpoints on which specific ePO Events occurred. When ePO events are detected, CounterACT 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 following:
- CounterACT ePO extension (see Install and Configure the CounterACT ePO Extension)
- ePO Extension parameters in the CounterACT module (see Configure the CounterACT ePO Extension).
- Database credentials (see Configure ePO Database Credentials)

**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 the McAfee ePO Module. 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 the McAfee ePO Module. 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 the McAfee ePO Module. 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 the McAfee ePO Module. 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 the McAfee ePO Module. See Configure ePO Database Credentials for details.

![ePO Point Product Setting String Property](image1)

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 the McAfee ePO Module. See Configure ePO Database Credentials for details.

![ePO RSD Detected System Linked Table Property](image2)
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 the McAfee ePO Module. See [Configure ePO Database Credentials](#) for details.

---

**Table Example**

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Column Name</th>
<th>Host ID</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>SampleTable</code></td>
<td><code>Column1</code></td>
<td><code>Host1</code></td>
<td><code>2023-01-01</code></td>
</tr>
</tbody>
</table>

---

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 the ePO database. To ensure access, verify that you have configured ePO database credentials in the McAfee ePO Module. See [Configure ePO Database Credentials](#) for details.

---

**Table Example**

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Column Name</th>
<th>Host ID</th>
<th>Integer Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>SampleTable</code></td>
<td><code>Column1</code></td>
<td><code>Host1</code></td>
<td><code>10</code></td>
</tr>
</tbody>
</table>

---
**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 McAfee ePO Module. 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 the `RSDDetectedSystemProperties` table. Enter the **Column Name**.

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

---

**Condition**

- **Value**
  - **RSDDetectedSystemProperties**
  - **Type** Date
  - **Use**
  - **Does not meet the following criteria**
  - **Column Name**
  - **Older than**
    - **1** Hours
  - **Before**
    - **2018-02-01 07:06 PM**
  - **Evaluate Irresolvable criteria as**
    - **False**

---

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 the McAfee ePO Module. See [Configure ePO Database Credentials](#) for details.

---

**Condition**

- **Value**
  - **RSDDetectedSystemProperties**
  - **Type** Integer
  - **Use**
  - **Does not meet the following criteria**
  - **Column Name**
  - **Enter a single, list or range of numbers. Example: 10, 20, 100-200**
  - **Evaluate Irresolvable criteria as**
    - **False**
**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 the McAfee ePO Module. See [Configure ePO Database Credentials](#) for details.

---

**Managing ePO Endpoints – Policy Actions**

CounterACT 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. Navigate 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 CounterACT policies to report endpoints detected by CounterACT to the **ePO Detected System**.

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

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

1. Right-click a table column header at the Console, **Detections** pane.

   ![Table Column Headers](image)

   - **Segment**
   - **Policy ePO**
   - **MAC Address**

   - Add/Remove Columns
     - Remove Column
     - Best Fit Column

   - **Fit table columns to view**

2. Select **Add/Remove Column**. The Add/Remove column dialog box opens.

   ![Add/Remove Column Dialog](image)

   - **Available Columns**
     - General
     - Policies
     - Policy Actions
     - Properties

3. In the left pane, under **Properties**, expand **McAfee ePO**.

4. Select the required columns in the left pane and select **Add**. The columns are displayed in the right pane.

5. Select **OK**.

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

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

- Documentation Portal
- Product Updates Portal
- CounterACT Console Online Help Tools

Documentation Portal

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

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

Product Updates Portal

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

To access the Product Updates Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

Console User Manual

Select CounterACT Help from the Help menu.

Plugin Help Files

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

2019-04-29 10:28