ForeScout Extended Module for FireEye® EX

Configuration Guide

Version 1.2

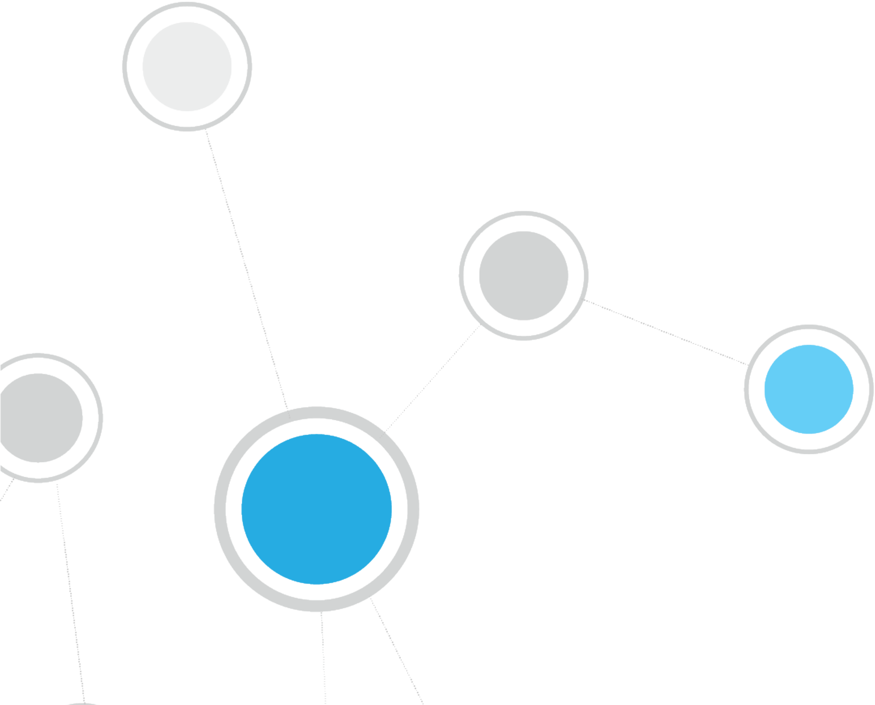


Table of Contents

About the FireEye EX Integration

Cyber criminals often use email spear phishing attacks, as well as malicious file attachments and URLs in emails, to launch advanced cyber-attacks. These email attacks routinely bypass conventional signature-based defenses such as antivirus and spam filters. The FireEye Email Security (EX) series protects against these email attacks on your corporate email accounts.

This integration combines the email threat detection mechanisms of FireEye EX with the network visibility and compliance enforcement capabilities of ForeScout CounterACT® to multiply the benefits of working with an Advanced Threat Detection (ATD) product. Integration with CounterACT helps corporate security teams identify, analyze and block advanced email-based cyber-attacks from both corporate and non-corporate email accounts.

Advanced Threat Detection with the IOC Scanner Plugin

This module works with the IOC Scanner Plugin – CounterACT's action center for Advanced Threat Detection (ATD) and response. The IOC Scanner Plugin provides:

- A centralized repository of all threats and their IOCs (indicators of compromise) reported to CounterACT by third-party ATD solutions, or added manually.
- Mechanisms that scan all Windows endpoints for threat and IOC information reported to CounterACT, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- FireEye EX instances in your environment report threats to this plugin as they are detected in emails.
- All threats reported by this module are automatically submitted to the IOC Scanner Plugin, which parses the threat to yield indicators of compromise (IOCs) - measurable events or state properties that can be used as a "fingerprint" to identify the threat. The IOC Scanner Plugin uses these IOCs to mount further scan/analyze/remediate stages of CounterACT's ATD response, as follows:
- ***ATD Stage 2 (IOC Scanner Plugin): Real-time hunt for endpoints of interest based on threats and IOCs:*** The IOC Scanner Plugin detects endpoints with IOCs associated with recently reported threats.
- ***ATD Stage 3 (IOC Scanner Plugin): Evaluation and remediation:*** The IOC Scanner Plugin evaluates the profile of IOCs on endpoints of interest to determine the likelihood that an endpoint is compromised, and applies appropriate blocking/remediation actions.

For more information about IOC-based threat detection and remediation, refer to the *CounterACT IOC Scanner Plugin Configuration Guide*.

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.

- Identify threats delivered through emails, attachments and embedded URLs that may not have been delivered through corporate emails monitored by FireEye EX. For example, a file on an attached drive or an email attachment delivered to a personal email account. Once identified, you can use CounterACT polices to perform actions on potentially infected endpoints that immediately:
  - Contain infected endpoints, for example limit or block network access. This prevents lateral movement of the infection to other endpoints.
  - Remediate infected endpoints, for example by killing suspicious processes.
  - Notify stakeholders by, for example, sending an email to corporate security teams with details about which threats were detected on which endpoints.

  For more detailed information about this use case, refer to the section about use cases in the *CounterACT IOC Scanner Plugin Configuration Guide*.

Additional FireEye EX Documentation

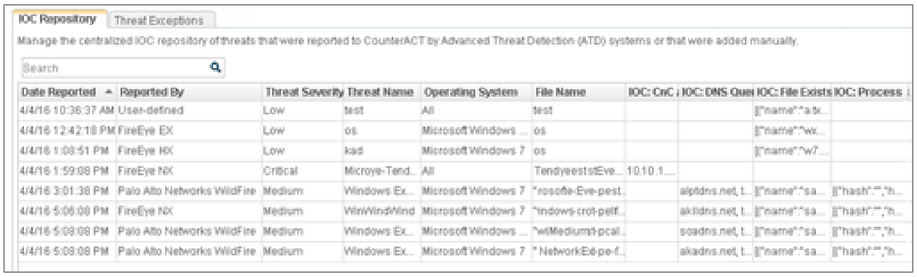
Refer to FireEye EX online documentation for more information about the FireEye EX solution:

- EX Series Threat Management Guide
- EX Series System Administration Guide

https://www.fireeye.com/products/ex-email-security-products.html

About This Module

This module, together with the IOC Scanner Plugin, lets you integrate CounterACT with FireEye EX so that you can view new threats of suspicious emails, attachments and embedded URLs reported by FireEye EX and automatically added to the IOC repository. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.



Manage the centralized IOC repository of threats that were reported to CounterACT by Advanced Threat Detection (ATD) systems or that were added manually.

Date Reported	Reported By	Threat Severity	Threat Name	Operating System	File Name	IOC: CnC	IOC: DNS Quer	IOC: File Exists	IOC: Process
4/4/16 10:36:37 AM	User-defined	Low	test	All	test			[{"name":"a.tx...	
4/4/16 12:42:18 PM	FireEye EX	Low	os	Microsoft Windows ...	os			[{"name":"wx...	
4/4/16 1:08:51 PM	FireEye HX	Low	kad	Microsoft Windows 7	os			[{"name":"w7...	
4/4/16 1:59:08 PM	FireEye NX	Critical	Microye-Tend...	All	TendyeeststEve...	10.10.1....			
4/4/16 3:01:38 PM	Palo Alto Networks WildFire	Medium	Windows Ex...	Microsoft Windows 7	"rosofte-Eve-pest...		alptdns.net, t...	[{"name":"sa...	[{"hash":"","h...
4/4/16 5:06:00 PM	FireEye NX	Medium	WinWindWind	Microsoft Windows 7	"indows-crot-pelf...		akildns.net, t...	[{"name":"sa...	[{"hash":"","h...
4/4/16 5:08:08 PM	Palo Alto Networks WildFire	Medium	Windows Ex...	Microsoft Windows ...	"wiMediumt-pcal...		soadns.net, t...	[{"name":"sa...	[{"hash":"","h...
4/4/16 5:08:08 PM	Palo Alto Networks WildFire	Medium	Windows Ex...	Microsoft Windows 7	" NetworkEd-pe-f...		akadns.net, t...	[{"name":"sa...	[{"hash":"","h...

To use the module, you should have a solid understanding of FireEye EX concepts, functionality and terminology, and understand how CounterACT policies and other basic features work.

How It Works

FireEye EX detects spear phishing attacks as well as malicious file attachments and URLs in emails that are used to launch advanced cyber-attacks. When a threat is detected, the FireEye EX server sends a notification (rsyslog format) of the threat details to a pre-defined receiving CounterACT device. The notification includes:

- timestamp of the event
- threat name, file name, severity and hash
- IOC details identified throughout the lifecycle of the threat on different operating systems (according to how FireEye EX is configured in your environment), such as:
  - Process Names

    If the reported malicious process indication is an .exe file, the filename is stored in the IOC repository as both a *Process* IOC and a *File Exists* IOC. If the malicious process indication is a loaded .dll file, the filename is stored as a *File Exists* IOC only. CounterACT detects .dll or .exe Portable Executable file types only.
  - File Names
  - Registry Keys and Values
  - Service Names
  - Mutex Names
  - DNS Queries
  - Command and Control (CnC) URLs

CounterACT adds the data to its IOC repository, where it can be used to trigger policy actions.

Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for details.

What to Do

You must perform the following to work with this module:

1. Install the IOC Scanner Plugin
2. Verify that you have met system requirements. See Requirements.
3. Define Rsyslog Targets in FireEye EX.
4. Install the Module.
5. Configure the Module.
6. Configure the CounterACT Syslog Plugin.
7. Create Custom FireEye EX Policies (optional).

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- FireEye EX Requirements

CounterACT Software Requirements

This module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- Core Extensions Module version 1.0 with the following components running:
  - Syslog Plugin version 3.4
  - IOC Scanner Plugin version 2.2

ForeScout Extended Module License Requirements

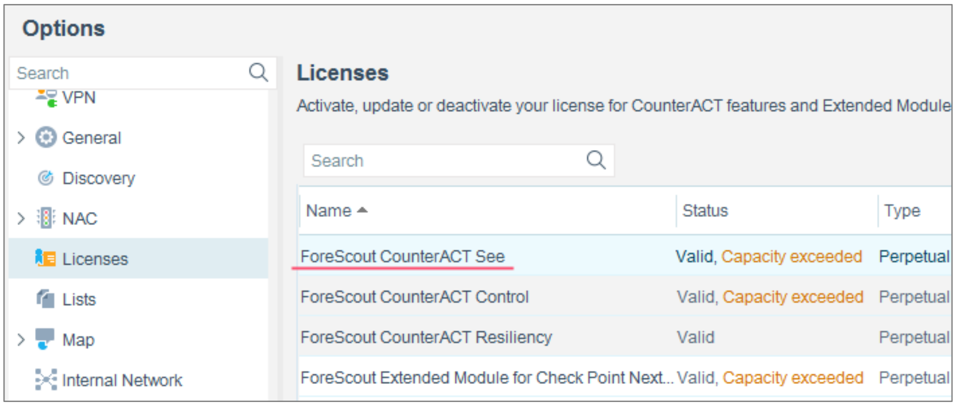
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

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

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

When installing the module you are provided with a 90-day demo module license.

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

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

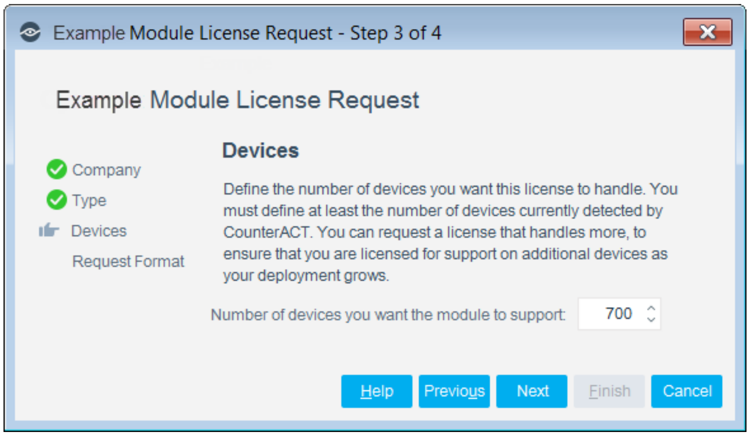
Demo license extension requests and permanent license requests are made from the CounterACT Console.

> *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 CounterACT 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 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.



Example Module License Request - Step 3 of 4

Example Module License Request

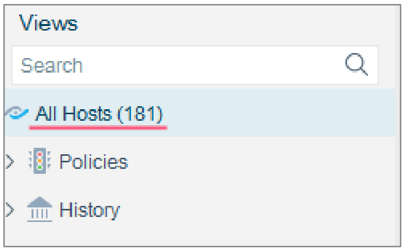
Devices

Define the number of devices 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.

Number of devices you want the module to support: 700

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.



Centralized Licensing Mode

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

🗎 *No demo license is automatically installed during system installation.*

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

Each Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

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

More License Information

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

FireEye EX Requirements

This module requires the following FireEye EX components:

- FireEye Email Security (EX) Series version 7.6
- Admin or Operator access to the EX Series appliance is required.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this component.*** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

Define Rsyslog Targets in FireEye EX

FireEye EX sends threat detections to CounterACT as rsyslog notification messages. To enable CounterACT to receive these notifications, you must define one or more CounterACT devices as rsyslog targets, and define the format of the notification message sent by FireEye EX.

- The EX Series appliance must have an established connection to the Internet.
- You must have Admin or Operator access to the EX Series appliance.
- Specify each Counteract connecting device by its IP address.
  - At least one CounterACT target must be enabled to work with the module.
- Notifications to CounterACT targets should use the following settings:

Format	JSON Extended
Delivery	Per Event
Notifications	All Events
Protocol	TCP

Install the Module

This section describes how to install the module. Before you install this module, first install the IOC Scanner Plugin.

Before you install this module, the CounterACT IOC Scanner Plugin and the CounterACT Syslog Plugin must already be running.

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 - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **.fpi** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **.fpi** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

🗎 *The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.*

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

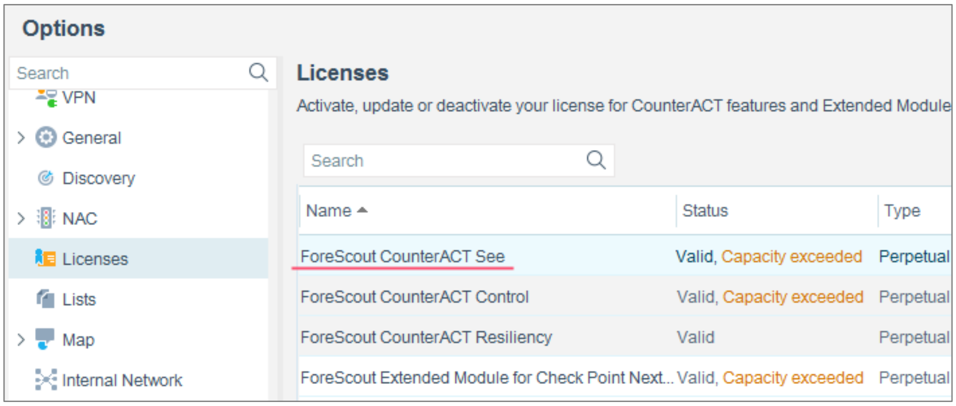
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    🗎 *Some components are not automatically started following installation.*

Identifying Your Licensing Mode in the Console

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

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

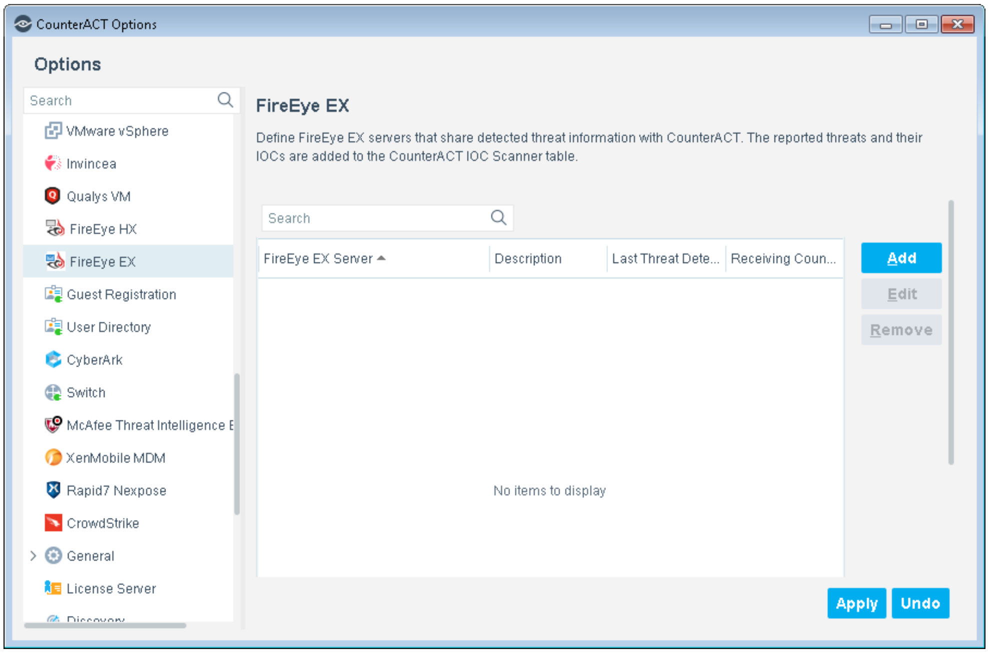
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

Configure the module to ensure that CounterACT can communicate with the FireEye EX service.

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 left pane, select **FireEye EX**, and select **Configure**. The FireEye EX pane opens.



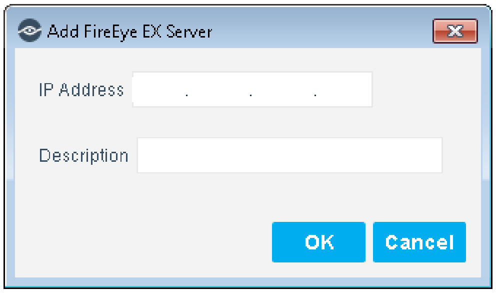
FireEye EX

Define FireEye EX servers that share detected threat information with CounterACT. The reported threats and their IOCs are added to the CounterACT IOC Scanner table.

FireEye EX Server ▲	Description	Last Threat Dete...	Receiving Coun...

No items to display

4. Select **Add** to define a FireEye EX server to communicate with CounterACT. The Add FireEye EX Server dialog box opens.



5. Enter the following information:
   – ***IP Address***. The IP address of the FireEye EX server that sends rsyslog notifications to CounterACT. See Define Rsyslog Targets in FireEye EX for details.
   – ***Description***. A textual description of the FireEye EX server.
6. Select **OK**. An entry for the FireEye EX server is added to the list in the FireEye EX pane.
7. In the FireEye EX pane, select **Apply**. A CounterACT Enterprise Manager Console dialog box opens.
8. Select **Yes** to save the module configuration.

The table in the FireEye EX pane has two additional display-only columns. These columns shown information on threats reported by FireEye EX appliances:

- ***Last Threat Report Time***. Indicates the latest date/time when CounterACT received a threat alert from this FireEye EX appliance.
- ***Receiving CounterACT Appliance***. The IP address of the connecting CounterACT device that received the last threat notification from this FireEye EX appliance. This is one of the CounterACT devices defined as rsyslog targets at the FireEye EX appliance. See Define Rsyslog Targets in FireEye EX.

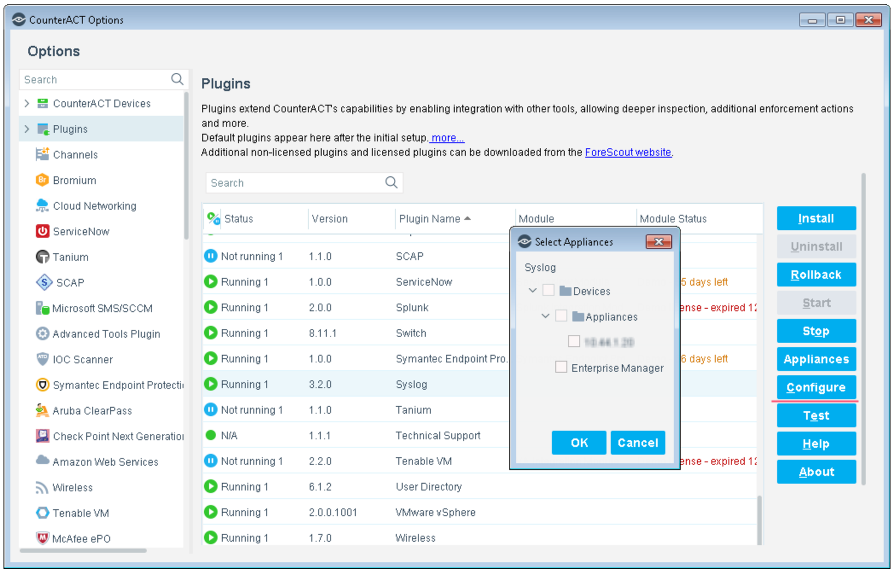
Configure the CounterACT Syslog Plugin

Configure the CounterACT Syslog Plugin to enable the receiving CounterACT device to connect to the FireEye EX server and receive notifications.

See the *CounterACT Syslog Plugin Configuration Guide* for more information about the Syslog Plugin configuration.

To configure the Syslog Plugin:

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 **Syslog**, and select **Configure**. The Select Appliances dialog box opens.



CounterACT Options

Options

Plugins

Plugins extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more.
Default plugins appear here after the initial setup. more...
Additional non-licensed plugins and licensed plugins can be downloaded from the ForeScout website.

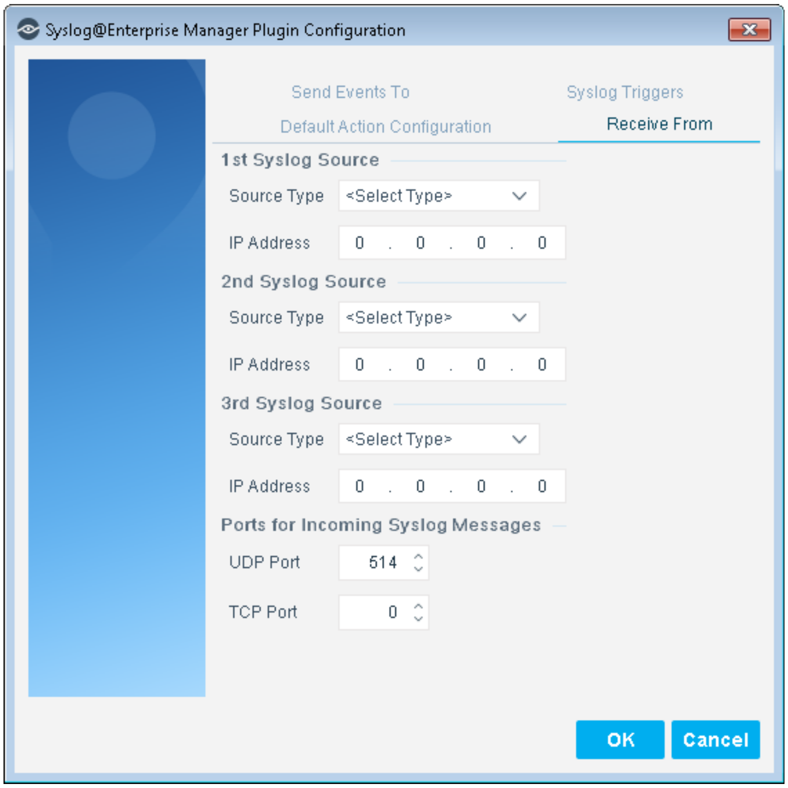
Status	Version	Plugin Name	Module	Module Status
Not running 1	1.1.0	SCAP		
Running 1	1.0.0	ServiceNow		5 days left
Running 1	2.0.0	Splunk		ense - expired 1
Running 1	8.11.1	Switch		
Running 1	1.0.0	Symantec Endpoint Pro.		6 days left
Running 1	3.2.0	Syslog		
Not running 1	1.1.0	Tanium		
N/A	1.1.1	Technical Support		
Not running 1	2.2.0	Tenable VM		ense - expired 1
Running 1	6.1.2	User Directory		
Running 1	2.0.0.1001	VMware vSphere		
Running 1	1.7.0	Wireless		

Select Appliances

Syslog
- □ Devices
  - □ Appliances
    - □ [redacted]
  - □ Enterprise Manager

4. Select the CounterACT device(s) defined as an rsyslog server in the Define Rsyslog Targets in FireEye EX section, and select **OK**. The Module Configuration window opens.

5. Select the *Receive from* tab.



Syslog@Enterprise Manager Plugin Configuration

1st Syslog Source

Source Type: <Select Type>

IP Address: 0 . 0 . 0 . 0

2nd Syslog Source

Source Type: <Select Type>

IP Address: 0 . 0 . 0 . 0

3rd Syslog Source

Source Type: <Select Type>

IP Address: 0 . 0 . 0 . 0

Ports for Incoming Syslog Messages

UDP Port: 514

TCP Port: 0

6. If necessary, set the TCP Port to **514**.

7. Select **OK** to save the configuration.

Create Custom FireEye EX Policies

CounterACT policies are powerful tools used for automated endpoint access control and management.

Policies and Rules, Conditions and Actions

CounterACT policies contain a series of rules. Each rule includes:

- Conditions based on host property values. CounterACT detects endpoints with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.
- Actions can be applied to endpoints that match the conditions of the rule.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can use the *Scan and Remediate Known IOCs* action and *Advanced Threat Detection* properties to create custom policies that:

- Scan potentially compromised Windows endpoints for IOCs reported by the FireEye EX Module.
- Remediate infected endpoints.

These items are available when you install the IOC Scanner Plugin.

To create a custom policy:

1. In the CounterACT Console, select the **Policy** tab. The Policy Manager opens.
2. Select **Add** to create a policy, or select **Help** for more information about working with policies.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

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

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

🗎 *Software downloads are also available from these portals.*

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

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

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

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.

2. Select the plugin and then select **Help**.

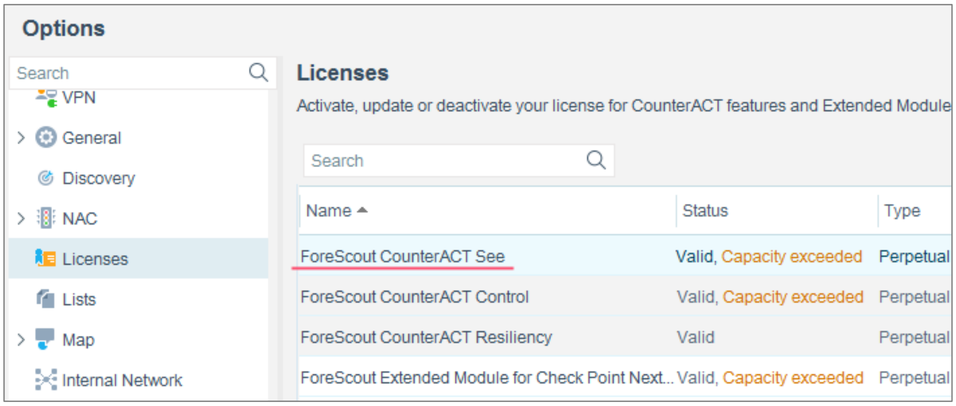
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

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

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21