ForeScout

CounterACT™ FireEye EX Plugin

Configuration Guide

Version 1.1.0

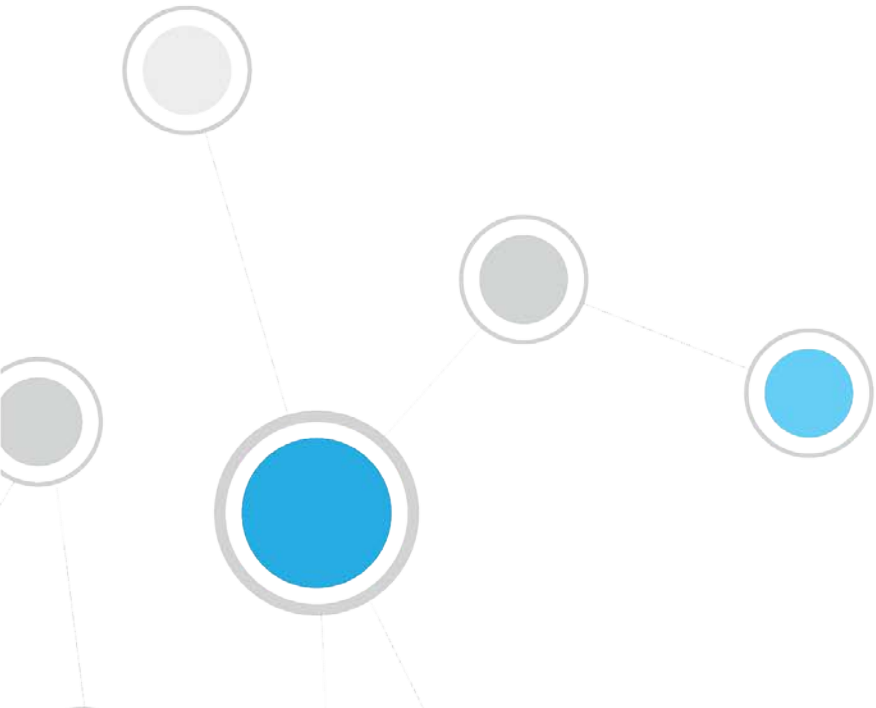


Table of Contents

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 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 plugin 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 plugin 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 *IOC Scanner Plugin Configuration Guide*.

Use Cases

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

- 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

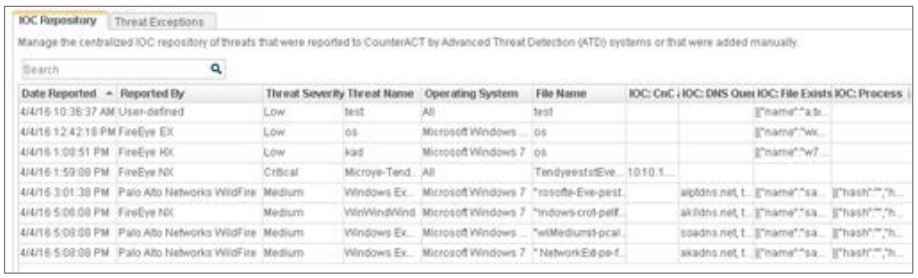
Refer to FireEye EX online documentation for more information about the FireEye EX solution:

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

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

About This Plugin

This plugin, 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.



To use the plugin, 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 plugin:

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 Plugin.
5. Configure the Plugin.
6. Configure the CounterACT Syslog Plugin.
7. Create Custom FireEye EX Policies (optional).

Requirements

This section describes system requirements, including:

CounterACT Software Requirements

The plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 7.0.0
- Service Pack 2.0.3 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- Syslog Plugin version 3.1.4 or above
- IOC Scanner Plugin version 2.0.0 or above

ForeScout Module License Requirements

This plugin is packaged as a ForeScout Module, and requires a module license. 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.

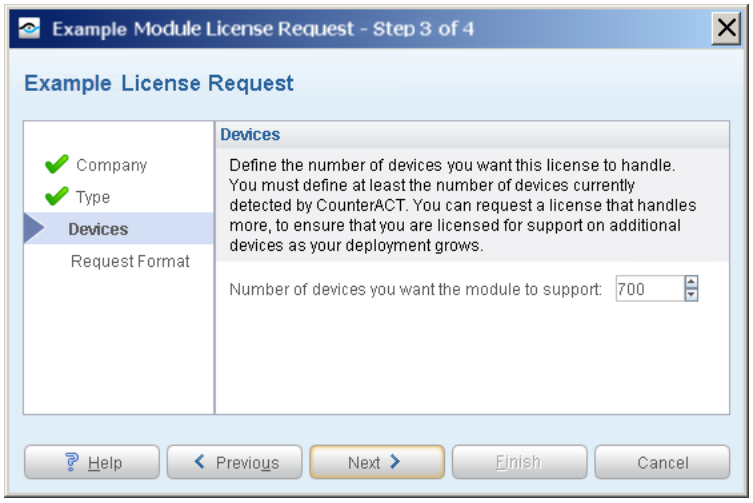
When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the plugin, you must purchase the license*.

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

Requesting a License

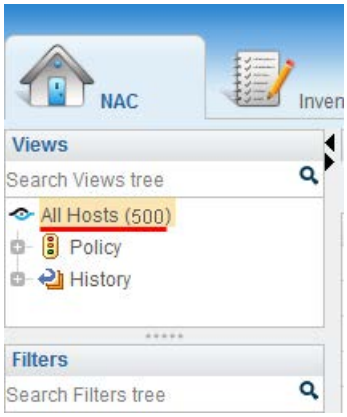
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that 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 **NAC** 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 for more information.

FireEye EX Requirements

The plugin requires the following FireEye EX components:

- FireEye Email Security (EX) Series version 7.8

Admin or Operator access to the EX Series appliance is required.

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 plugin.
- Notifications to CounterACT targets should use the following settings:

Format	JSON Extended
Delivery	Per Event
Notifications	All Events
Protocol	TCP

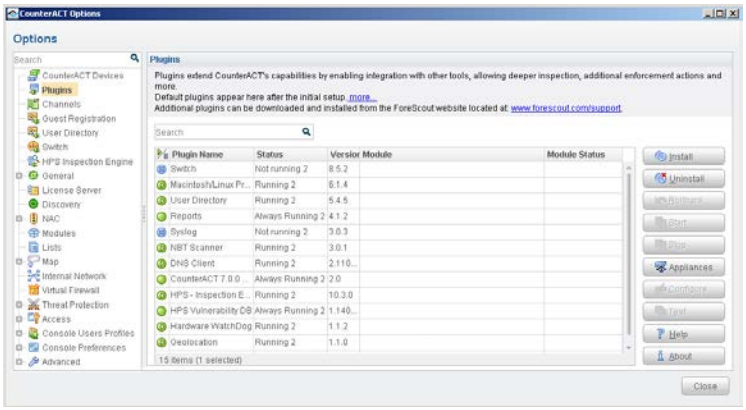
Install the Plugin

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

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

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   - If you are installing a Beta release of this plugin, acquire the plugin **`.fpi`** file from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support, ForeScout Modules page and download the plugin **`.fpi`** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.



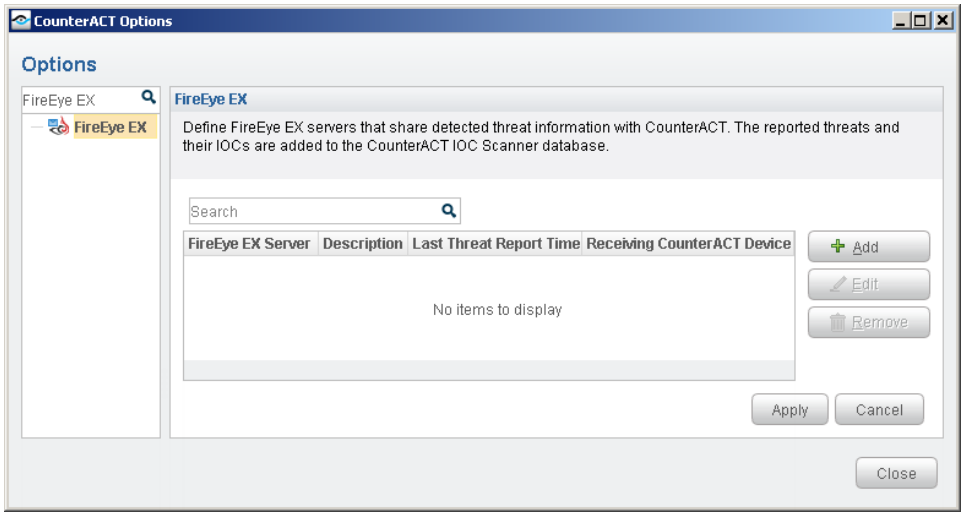
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and then select **Install**.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. 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 and the *CounterACT Console User Manual* for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select **Start**. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select **OK**. The plugin runs on the selected devices.

Configure the Plugin

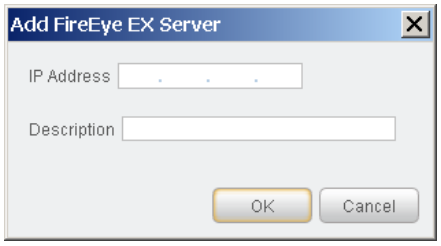
Configure the plugin to ensure that CounterACT can communicate with the FireEye EX service.

To configure the 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 **FireEye EX**, and select **Configure**. The FireEye EX pane opens.



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 plugin 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.

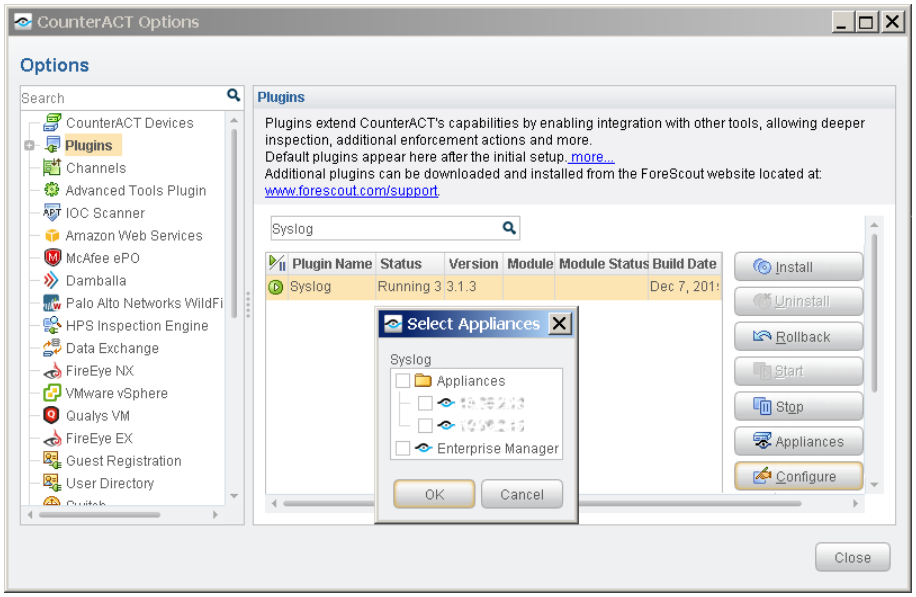
Configure the CounterACT Syslog Plugin

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

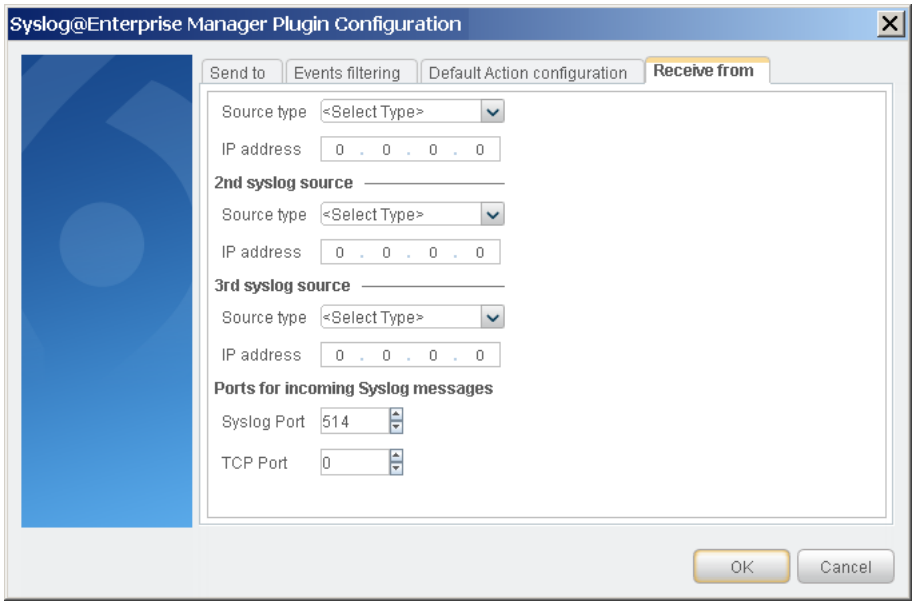
See the *CounterACT Syslog Plugin Configuration Guide* for more information about the Syslog Plugin configuration.

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.



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



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 Plugin.
- 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.

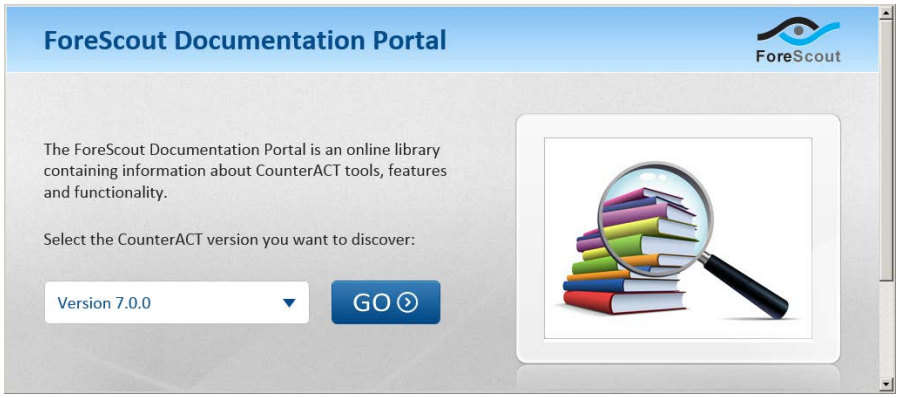
Additional CounterACT Documentation

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

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



To access the Documentation Portal:

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

Customer Support Portal

The Customer Support 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 Customer Support Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
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

1. 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**.

Documentation Portal

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

Legal Notice

2016-08-09 15:00