ForeScout

CounterACT™ Invincea Plugin

Configuration Guide

Version 1.2.0 and Above

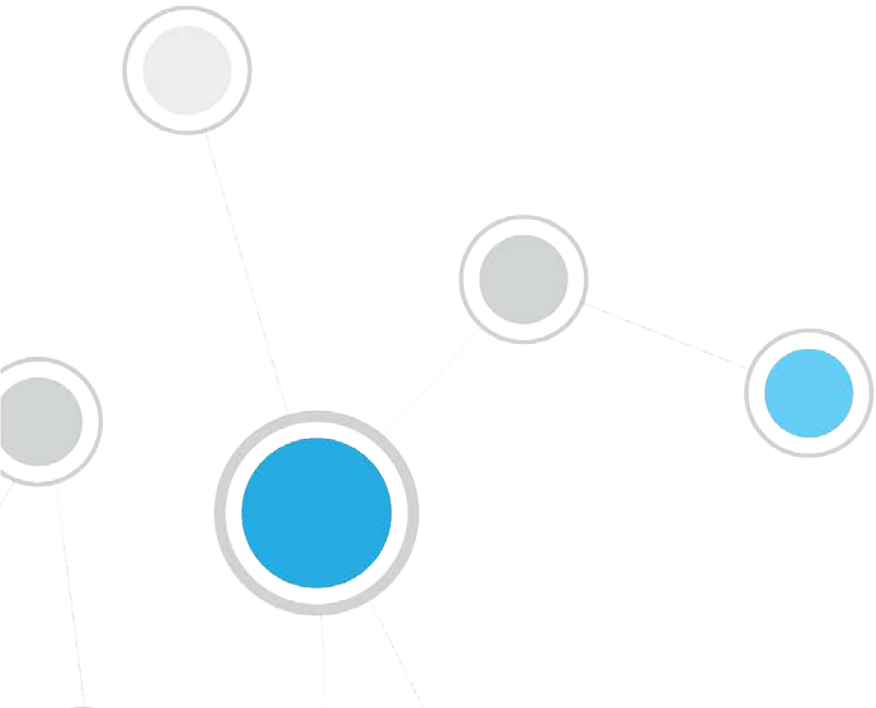


Table of Contents

About the Invincea Integration

The CounterACT Invincea Plugin helps IT administrators simplify the process of identifying, analyzing and blocking advanced cyber-attacks that threaten network security.

The CounterACT/Invincea integration protects against malware by moving the most highly targeted applications on endpoints, the web browsers, PDF reader and Office suite, into secure virtual containers on the user's device. When a user trips across a malicious website or content, whether via a spear-phish, web-based drive-by or watering hole, Invincea contains the attack, terminates the malware, collects forensics on the threat and forwards the information to the Invincea Management Server.

Advanced Persistent Threat (APT) engines have the capability to detect threats, but they may not have the network and endpoint visibility that CounterACT has. This may be because branch offices do not have an APT monitoring appliance on the network, or because it may be impractical to require APT detection product installation on guest machines and BYODs. Additionally, some APT detection products may be able to detect, but not remediate infected hosts.

To solve these problems, plugins in the Advanced Threat Detection Integration Module use the knowledge gained from the APT products to scan other hosts on the network.

Specifically, the CounterACT IOC Scanner Plugin combines the threat detection mechanisms of APT detection products with the network visibility and compliance enforcement capabilities of CounterACT to multiply the benefits of working with an APT detection product. The IOC Scanner Plugin serves as a centralized database and scanning hub for other plugins in ForeScout's Advanced Threat Detection Integration Module.

Additionally, CounterACT plugins provide the capability to remediate infected hosts where possible. The combined value of an APT product and CounterACT exceeds the sum of the benefits from the two products.

Additional Invincea Documentation

Refer to the following Invincea online documentation for more information:

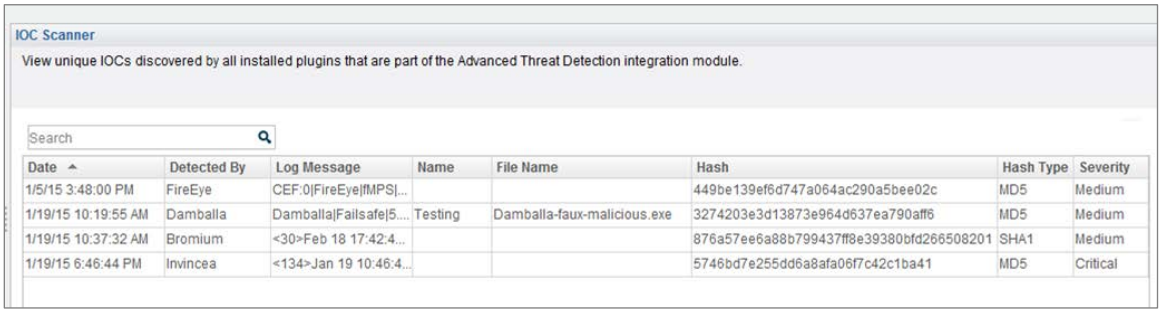
Invincea Management Server Installation and Configuration Guide, version 2.2

About This Plugin

The CounterACT Invincea Plugin, together with the CounterACT IOC Scanner Plugin, integrates CounterACT with the Invincea FreeSpace Advanced Persistent Threat (APT) engine.

Integration lets you:

- Use the CounterACT Invincea FreeSpace Compliance Policy Template to detect and handle endpoints not running Invincea FreeSpace. A policy template action can be used to trigger Invincea FreeSpace installation on non-compliant endpoints.
- Use the IOC Scanner Plugin to scan potentially compromised Windows endpoints for known Indicators of Compromise (IOCs) reported by the Invincea Plugin and other third party vendor integration plugins. The IOC Scanner Plugin converts the data into properties associated with the endpoint on which the threat was discovered. These properties can be used to trigger policy actions. See Detecting IOCs – Policy Properties for details.


IOC Scanner

View unique IOCs discovered by all installed plugins that are part of the Advanced Threat Detection integration module.

Search

Date	Detected By	Log Message	Name	File Name	Hash	Hash Type	Severity
1/5/15 3:48:00 PM	FireEye	CEF:0|FireEye|MPS|...			449be139ef6d747a064ac290a5bee02c	MD5	Medium
1/19/15 10:19:55 AM	Damballa	Damballa|Failsafe|5....	Testing	Damballa-faux-malicious.exe	3274203e3d13873e964d637ea790aff6	MD5	Medium
1/19/15 10:37:32 AM	Bromium	<30>Feb 18 17:42:4...			876a57ee6a88b799437ff8e39380bfd266508201	SHA1	Medium
1/19/15 6:46:44 PM	Invincea	<134>Jan 19 10:46:4...			5746bd7e255dd6a8afa06f7c42c1ba41	MD5	Critical

- Use information learned by Invincea to create custom policies that perform enforcement on endpoints with detected malware. For example:
  - Allow compliant and managed endpoints to join the network.
  - Limit network access to a subset of endpoints, blocking access to more sensitive corporate resources.
  - Block noncompliant endpoints or specific types of devices from your network.
- Enable unified supervision of APT-related threats from a single location.
- Use CounterACT inventory tools to display all IOCs reported by the Invincea Plugin and all other integrated third party vendor plugins, and the corresponding endpoints on which they were found.
- Create CounterACT reports that provide detailed information about:
  - Endpoints with IOCs found by Invincea or CounterACT.
  - IOCs detected during a recent period of time.

To use the plugin, you should have a solid understanding of Invincea FreeSpace concepts, functionality and terminology, and understand how CounterACT IOC Scanner Plugin policies and other basic features work.

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

How It Works

When an IOC is detected by Invincea, the Invincea Management Server (IMS) server sends a Syslog message (CEF format) containing details of the IOC to the configured CounterACT Appliance. This information includes the Source/Destination IP Address, a timestamp of the event, the file name, the severity, and the file hash value.

The CounterACT Invincea Plugin on that Appliance passes the parsed IOC information to the CounterACT IOC Scanner Plugin. The IOC Scanner Plugin converts the data into CounterACT properties associated with the endpoint on which the threat was discovered. An example of such a property is the IOCs Detected by Third Party property.

In addition, all endpoints in the CounterACT network are resolved with the date of the newest IOC received by the IOC Scanner Plugin. You can use this property in policies to trigger scans.

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

What to Do

To work with this plugin:

1. Install the CounterACT IOC Scanner Plugin and the CounterACT Syslog Plugin.
2. Verify that you have met system requirements. See Requirements.
3. Configure the Invincea Management Server.
4. Install the Plugin.
5. Configure the Plugin.
6. Test the Plugin.
7. Run Invincea Policy Templates (optional).
8. Create Custom Invincea Policies.

Requirements

This section describes:

- CounterACT Software Requirements
- Supported Vendor Requirements
- ForeScout Module License Requirements

CounterACT Software Requirements

Additional plugin requirements include:

- CounterACT version 7.0.0, running Hotfix version 1.6.3 or above.
- CounterACT IOC Scanner Plugin version 1.1.2.
- CounterACT Syslog Plugin version 3.0.3 or above.

Supported Vendor Requirements

The Invincea Plugin works with Invincea Enterprise version 2.2.

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*.

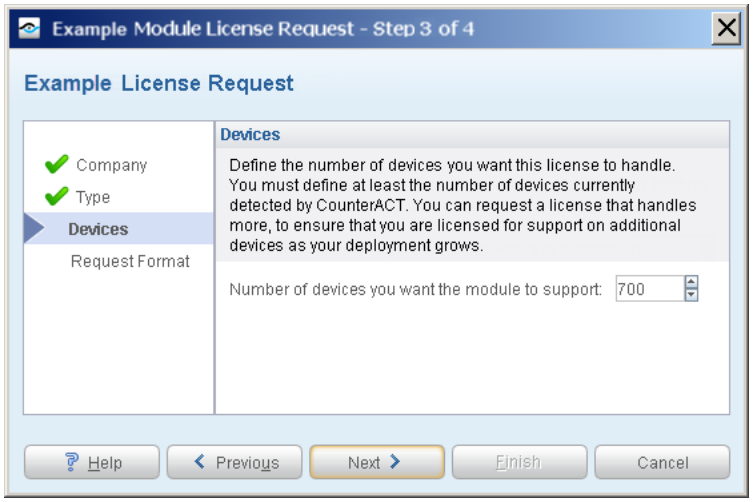
Demo license extension requests and permanent license requests are made from the CounterACT Console.

> *This plugin may have been previously packaged as a component of an Integration Module which contained additional plugins. If you already installed this plugin 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 Console User Manual 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.

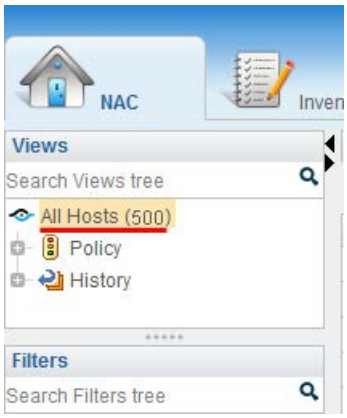
Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.



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

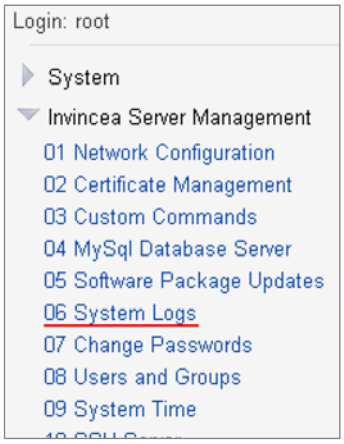
See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

Configure the Invincea Management Server

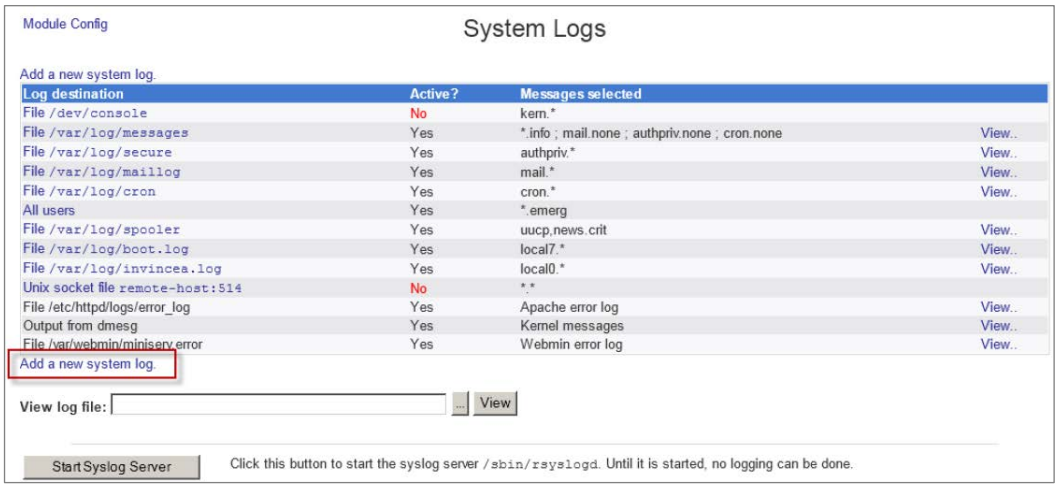
Verify that the Invincea Management Server (IMS) is running and add an IMS Syslog destination server for sending Syslog messages to CounterACT.

To configure the IMS:

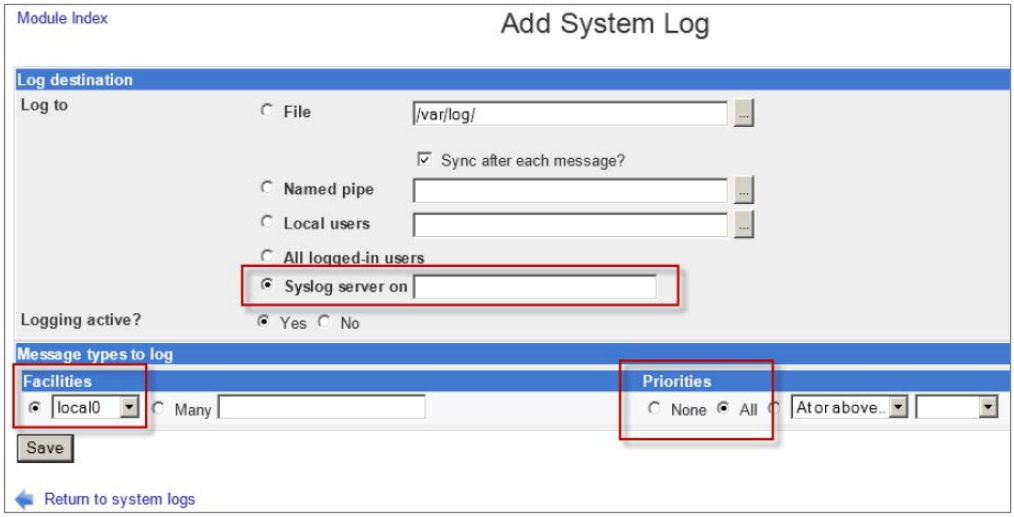
1. Open the Invincea Management Server menu.



2. Select **06 System Logs**.

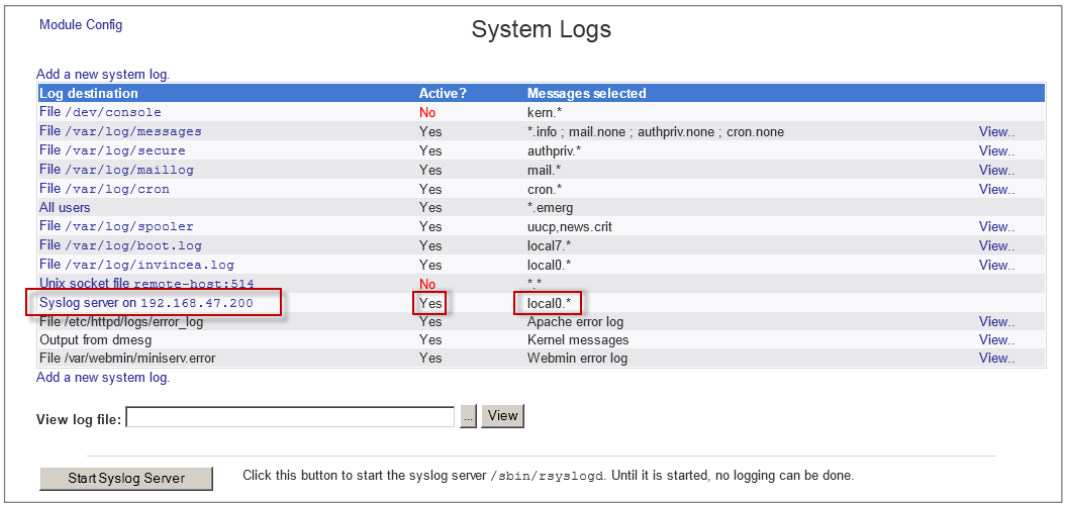


3. On the System Logs page, select **Add a new system log** from the bottom of the table. The Add System Log page opens.

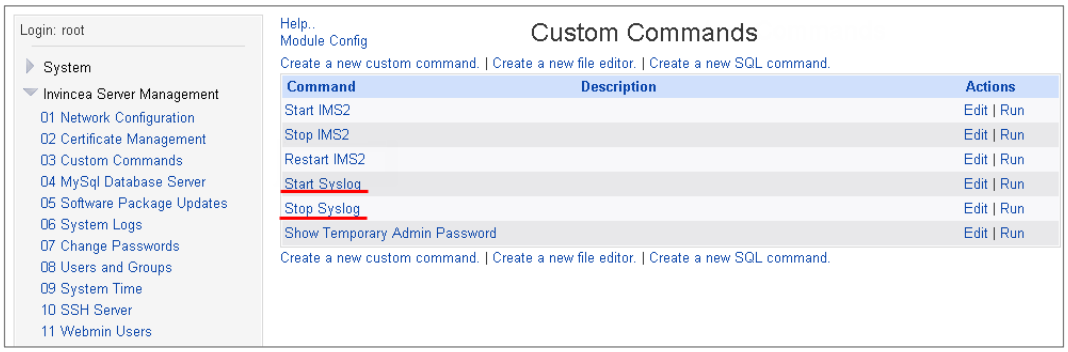


4. In Log Destination section, select **Syslog server on**, and in the field enter the IP address of the CounterACT Appliance that the event messages will be forwarded to.
5. In the Facilities section, select **local0** from the drop-down list.
6. In the Priorities section, select **All**.
7. Select **Save**.
8. In the System Logs page, verify the following:

- The syslog server must be listed as *Syslog server on <IP_ADDRESS>*.
- The syslog server must be *Active*.
- The *Messages selected* column must display *local0.**.



9. To complete the syslog configuration, the syslog service must be restarted (or started if it was not running).
In the Invincea Management Server menu, select **03 Custom Commands**.



10. Select **Stop Syslog** and then select **Start Syslog**.

Install the Plugin

This section describes how to install the CounterACT Invincea Plugin.

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

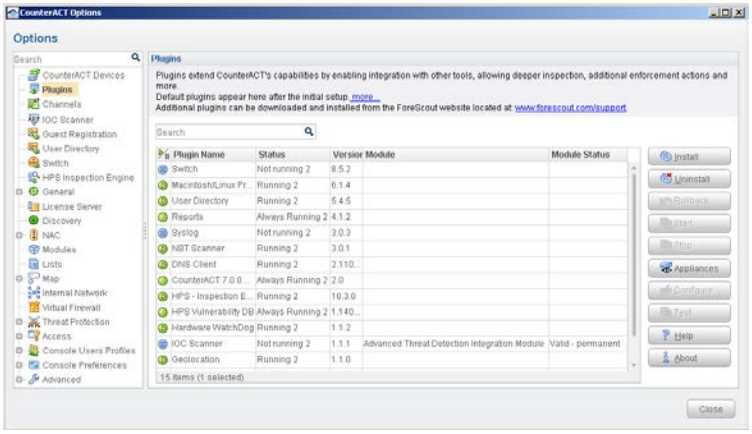
Once installed on the Enterprise Manager, the Invincea Plugin is automatically installed on all CounterACT Appliances.

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 a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
10. Once the installation is complete, select **Close**. The plugin is listed 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 information 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.

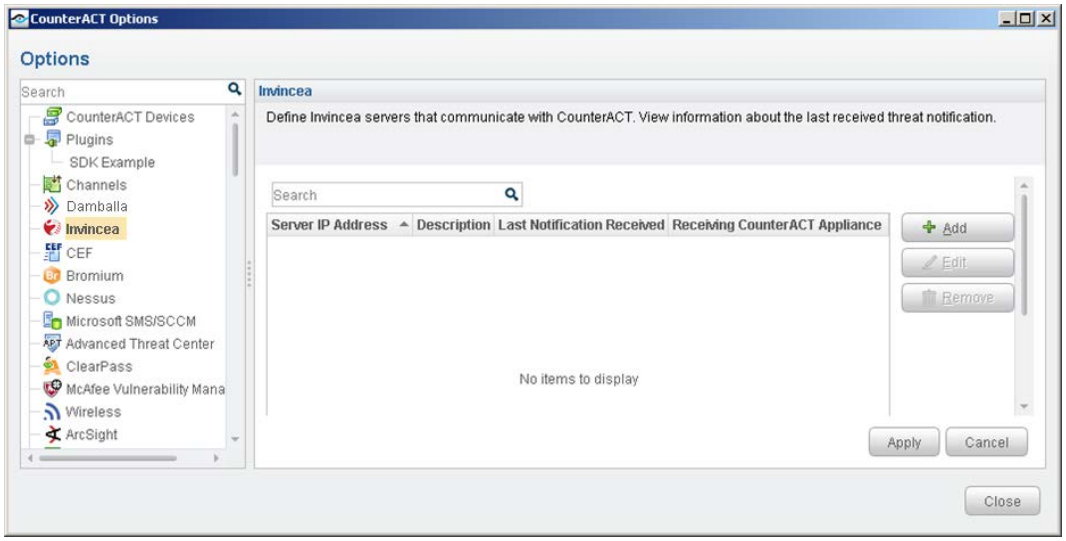
Configure the Plugin

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

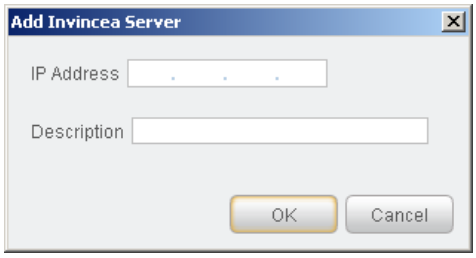
To configure the plugin:

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 **Invincea**, and select **Configure**. The Invincea pane opens.

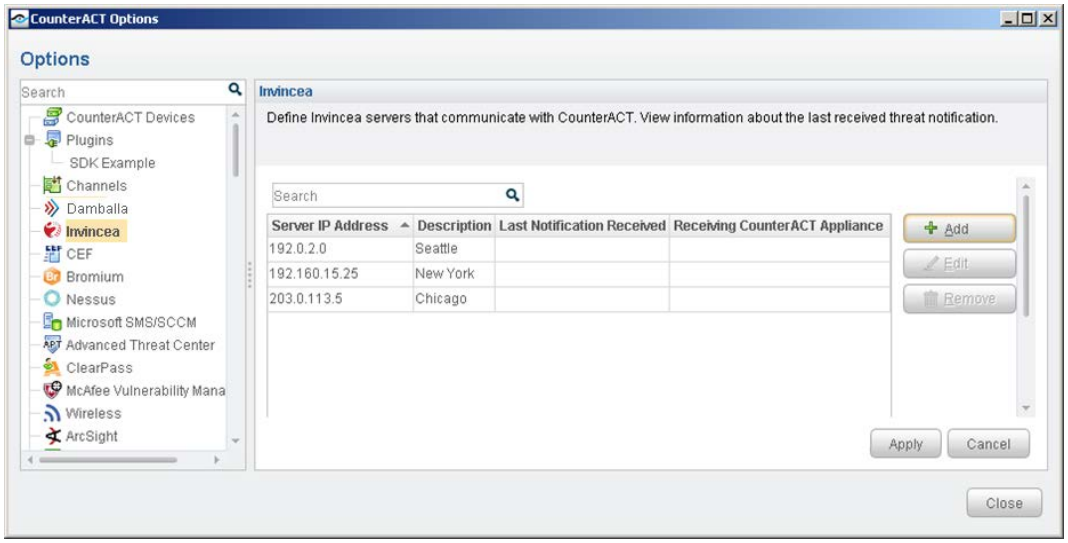


4. Select **Add**. The Add Invincea Server dialog box opens.



5. Enter the following information:
   - ***IP Address***. The IP address of the Invincea IMS server configured to send Syslog messages to CounterACT. See Configure the Invincea Management Server for details.
   - ***Description***. A textual description of the server.
6. Select **OK**. An entry for the Invincea server is added to the table in the Invincea pane.

   There are two additional display-only fields in the table:
   - ***Last Notification Received***. Indicates the latest date/time when CounterACT received an IOC from the particular Invincea server.
   - ***Receiving CounterACT Appliance***. The IP address of the CounterACT Appliance that received the latest IOC notification from the particular Invincea server.



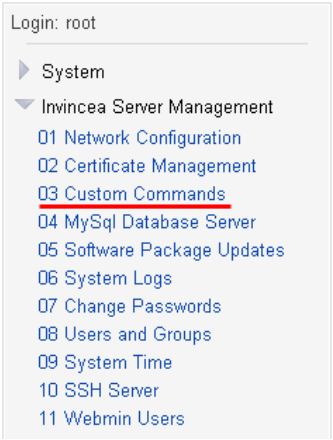
7. Select **Apply** and then select **Yes** to save the configuration changes.
8. Select **Close**.

Test the Plugin

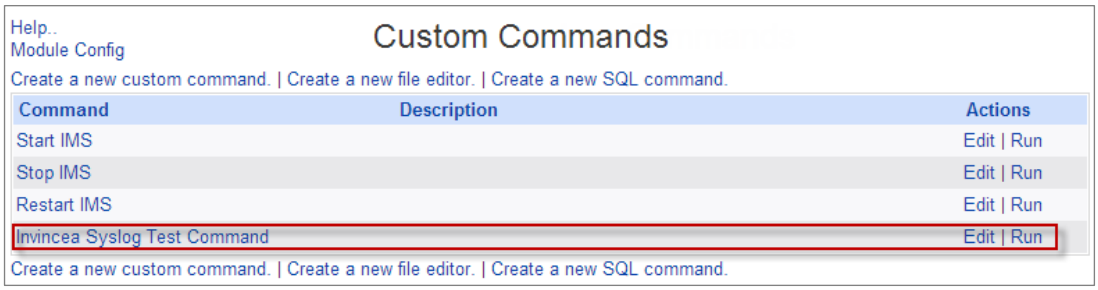
Test the plugin communication with the IMS.

To test the connection:

1. Open the Invincea Management Server menu.



2. Select **03 Custom Commands**.



3. Run **Invincea Syslog Test Command**.
4. Verify that the CounterACT Appliance receives a Syslog message reading ***Invincea Syslog Control Test***.

Run Invincea Policy Templates

This plugin provides the Invincea FreeSpace Compliance Policy Template which can be used to detect and handle endpoints not running Invincea FreeSpace.

Specifically, the template policy detects endpoints on which:

- Invincea FreeSpace is not installed.
- Invincea FreeSpace is installed but not running.
- Invincea FreeSpace is installed and running. These endpoints are compliant.

A policy template action can be used to trigger Invincea FreeSpace installation. This action is disabled by default.

Prerequisites

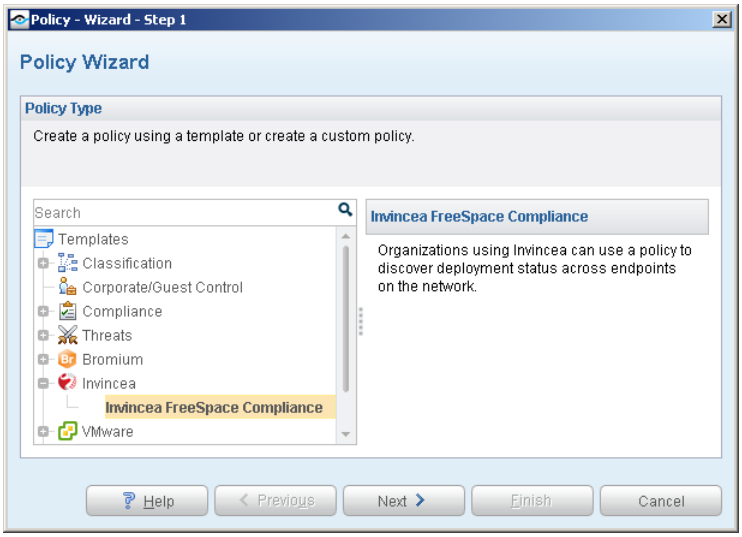
- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.
- Before you run a policy based on this template, verify that you have configured the plugin. See Configure the Plugin for details.

Run the Template

This section describes how to create a policy from the policy template.

To run the 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 **Invincea** folder and select **Invincea FreeSpace Compliance**. The Invincea FreeSpace Compliance pane opens.

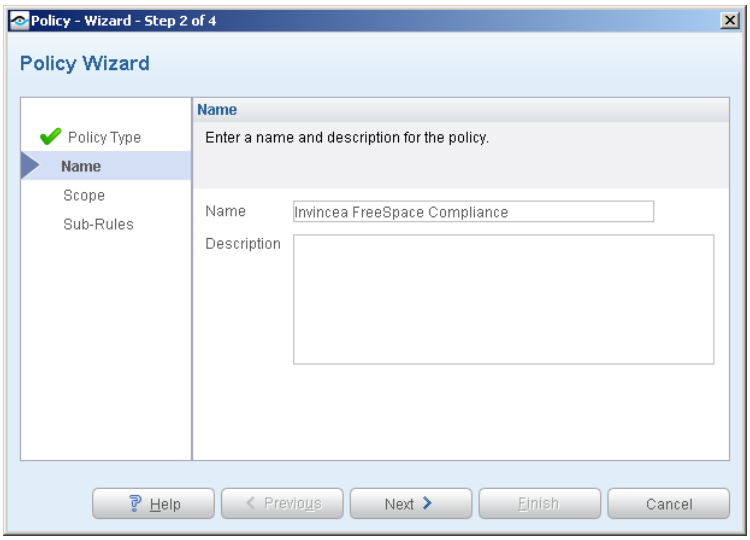


4. Select **Next**. The Name pane opens.

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.

1. Define a unique name for the policy you are creating based on this template, and enter a description.



Naming Tips

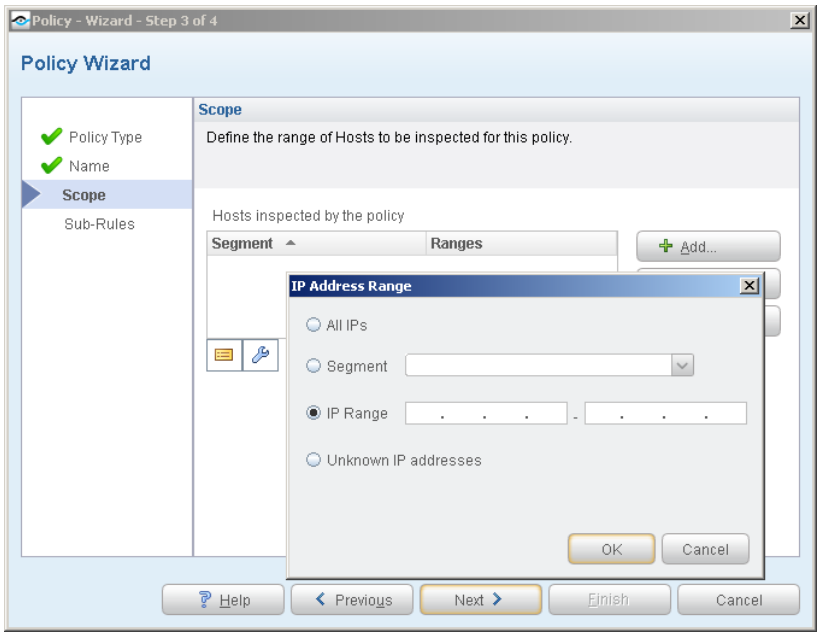
- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.

– Avoid having another policy with a similar name.

2. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Hosts 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.



1. 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 page.
   – **IP Range**: Define a range of IP addresses. These addresses must 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.

2. Select **OK**. The added range appears in the Scope pane.
3. Select **Next**. The Sub-Rules pane opens.

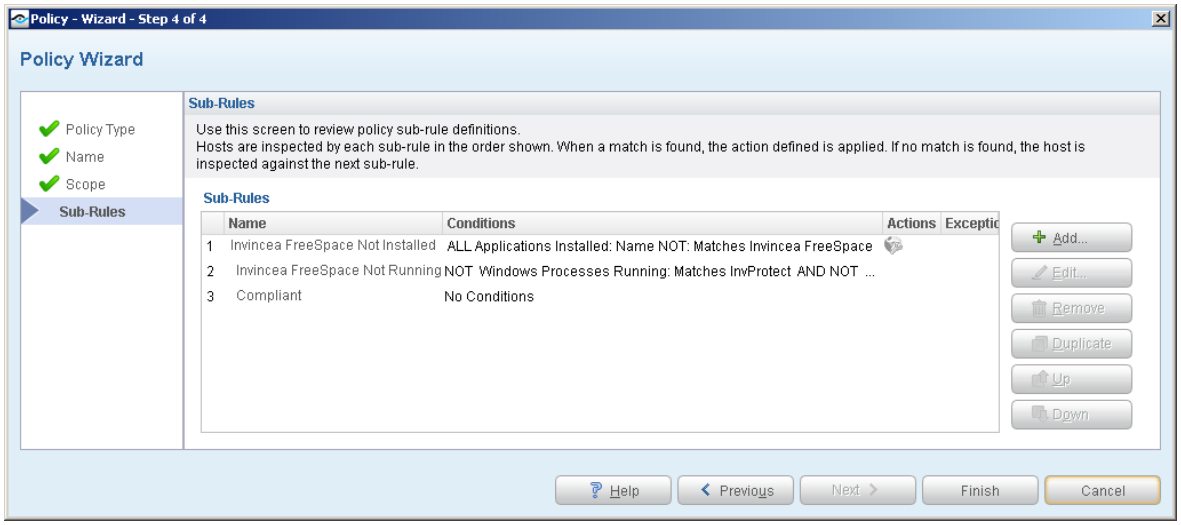
Review Sub-Rules

1. Review the sub-rules.

Sub-rules let you streamline separate detections and actions into one automated sequence.

Sub-rules are predefined to detect common conditions on the endpoints you defined in the policy scope.

Sub-rules are evaluated in numeric order. If the endpoint does not match the requirements of the first sub-rule, the next sub-rule in the list is evaluated. When a sub-rule condition match is found, the policy evaluation stops. If an action is associated with the matching sub-rule, that action is applied to the endpoint.



When an endpoint matches one of these rules, the policy evaluation of the endpoint ends.

The sub-rules are:

- **Invincea FreeSpace Not Installed** – Invincea FreeSpace is not installed on the endpoint.
- The policy wizard includes an optional action to install Invincea FreeSpace when this condition is detected. By default, this action is disabled. You can double-click the sub-rule and enable the action.
- **Invincea FreeSpace Not Running** – Invincea FreeSpace is not running on the endpoint.
- **Compliant** – Invincea FreeSpace is installed and running on the endpoint.

2. Select **Finish**. The policy is created.

Create Custom Invincea Policies

You may need to create a custom policy to deal with issues not covered in the Invincea policy templates.

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.

Use the IOC Scanner Plugin to scan potentially compromised Windows endpoints for known Indicators of Compromise (IOCs) reported by the Invincea Plugin.

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.

Invincea Properties and Actions

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with Invincea and IOC Scanner Plugin properties and actions to create custom policies. These items are available when you install the plugin.

For more information about working with policies, select **Help** from the policy wizard.

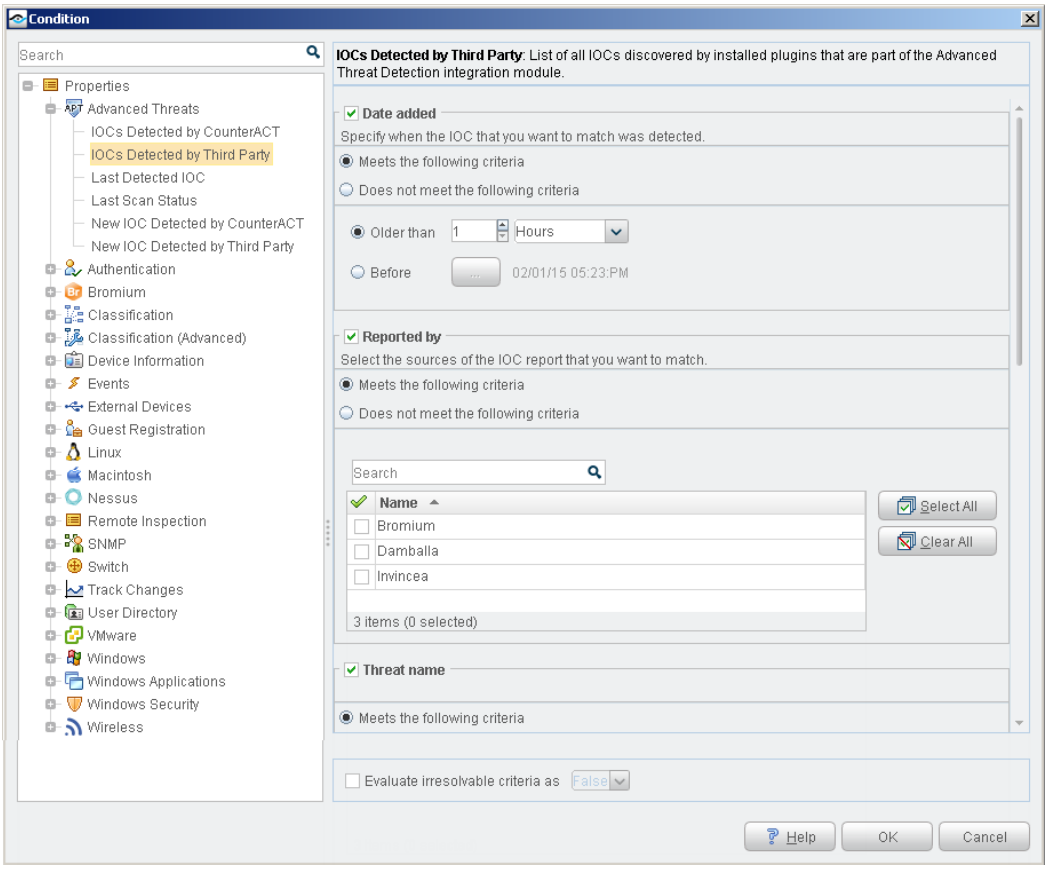
To create a custom policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select **Add** to create a policy.

Detecting IOCs – Policy Properties

The following properties contain IOC data reported by the CounterACT Invincea Plugin. These properties are available when you install the CounterACT IOC Scanner Plugin.

- IOCs Detected by Third Party
- Last Detected IOC
- New IOC Detected by Third Party



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

Invincea FreeSpace– Policy Actions

This section describes the actions that are made available when the Invincea plugin is installed.

The following Invincea action is available:

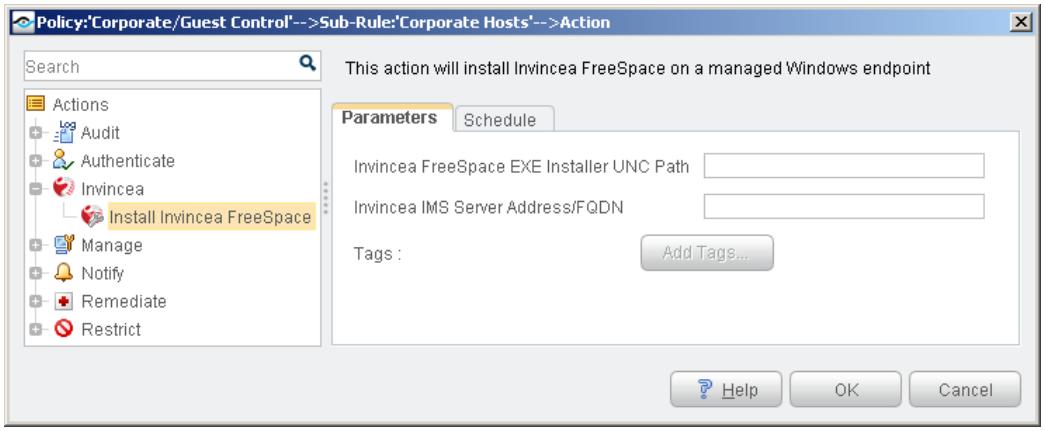
- Install Invincea FreeSpace

Install Invincea FreeSpace

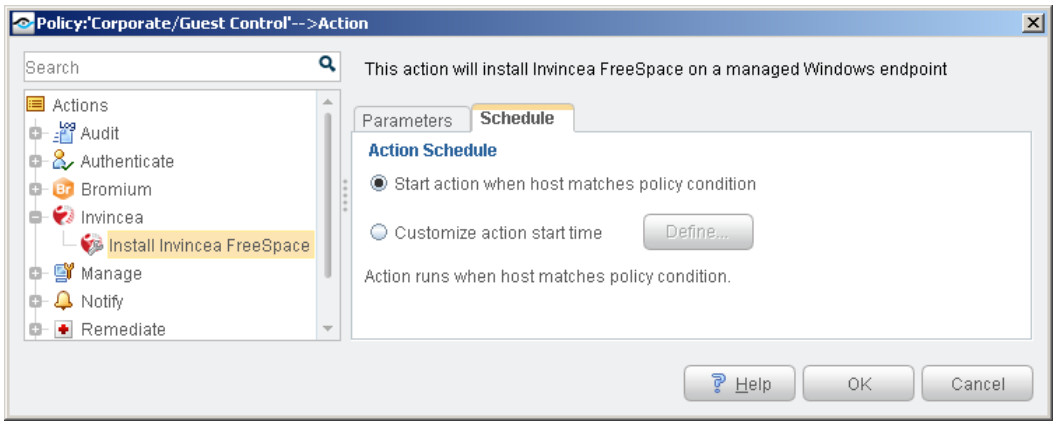
Use the *Install Invincea FreeSpace* action in CounterACT policies to install Invincea FreeSpace when certain policy conditions are met. For example, create a policy that detects if Invincea FreeSpace has not yet been installed on an endpoint, and trigger installation when an endpoint meets this condition.

To apply the Install Invincea FreeSpace action:

1. Open the policy Actions dialog box.
2. Expand the Invincea folder in the Actions tree.
3. Select **Install Invincea FreeSpace**.



4. In the Parameters tab, enter the following:
   - **Invincea FreeSpace EXE Installer UNC Path**: Enter the path to the Invincea FreeSpace EXE installation file, including the filename.
   - **Invincea IMS Server Address/FQDN**: Enter the address or fully qualified domain name of the IMS server.



5. In the Schedule tab, select one of the following schedules:
   - **Start action when host matches policy condition**: Invincea FreeSpace is installed on the endpoint immediately upon a condition sub-rule match.
   - **Customize action start time**: Define when installation on the endpoint should begin following a condition sub-rule match.

You can identify action success or failure at the CounterACT Console Detections pane.

Additional CounterACT Documentation

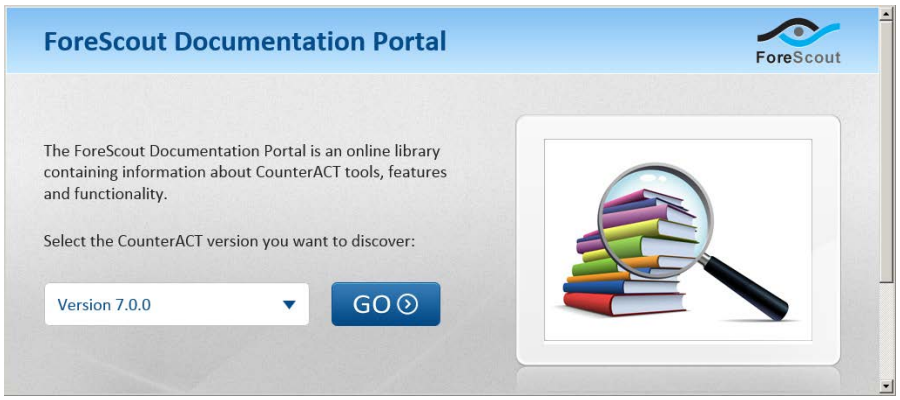
For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources:

- 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