ForeScout Extended Module for Bromium® Secure Platform

Configuration Guide

Version 1.3.0

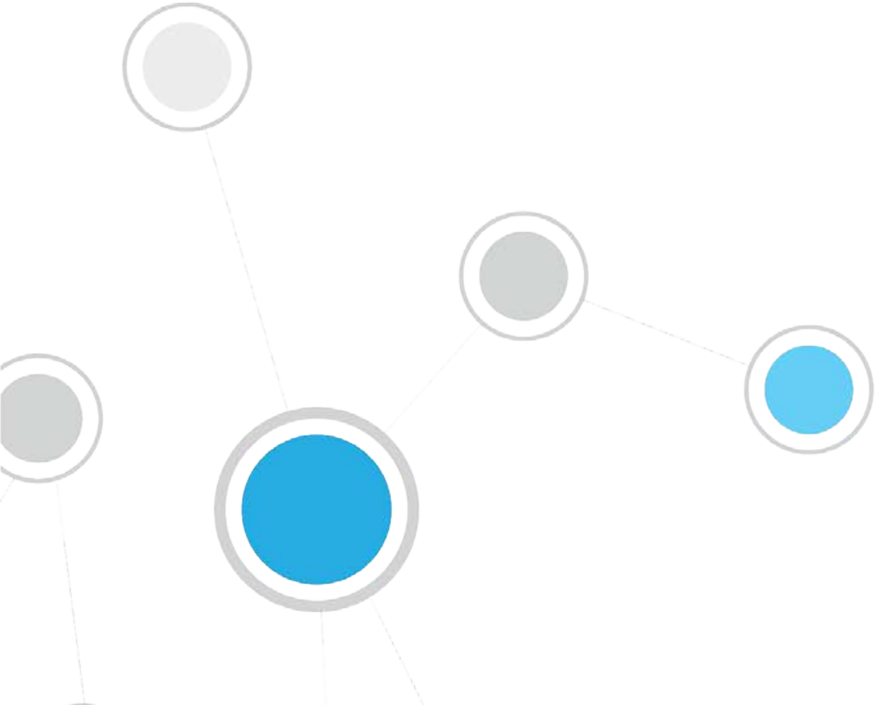


Table of Contents

About the Bromium Integration

The CounterACT® /Bromium integration helps IT administrators simplify the process of identifying, analyzing and blocking advanced cyber-attacks that threaten network security.

Advanced Persistent Threat (APT) solutions such as Bromium Secure Platform detects threats using a hardware-based isolation on modern-day hardware. For legacy hardware that does not support isolation there is a gap where the enterprise does not have network and endpoint visibility, CounterACT addresses this by providing full visibility across the entire enterprise.

CounterACT uses the knowledge gained from APT products such as Bromium Secure Platform to scan other hosts on the network.

Specifically, the CounterACT IOC Scanner Plugin combines the threat information from Bromium Secure Platform with the network visibility and compliance enforcement capabilities of CounterACT. The net result is complete visibility of threat behavior across the entire enterprise. The IOC Scanner Plugin serves as a centralized database and scanning hub for other plugins in ForeScout's Advanced Threat Detection Integration Module.

CounterACT modules 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.

The CounterACT/Bromium integration protects the enterprise from zero-day malware which is undetectable through traditional security layers, thereby eliminating the risk of a security compromise at the endpoint from key attacks vectors—Web, email, and USB. The cost of remediation and incidence response for endpoint infections is drastically reduced. The solution enables the security and IT teams to empower users with unrestricted access to the Web thereby increasing productivity.

Additional Bromium Secure Platform Documentation

Refer to the following Bromium documentation for more information:

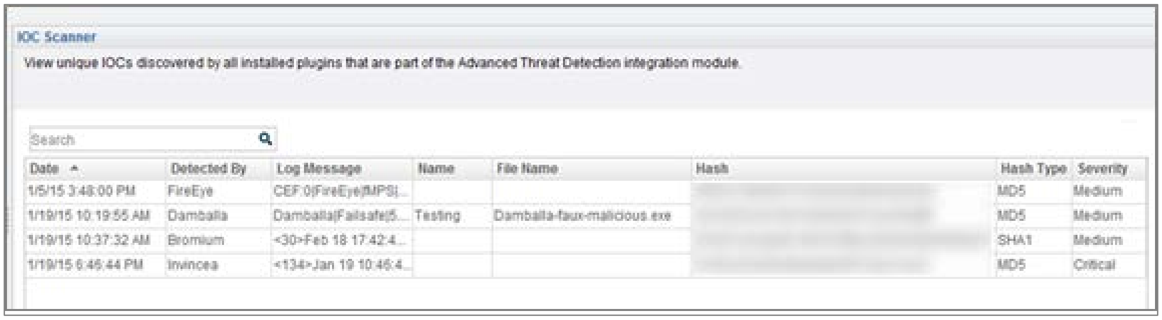
Bromium Advanced Endpoint Security 3.2 GA Update 3 Deployment Guide.

About This Module

The ForeScout Extended Module for Bromium Secure Platform, together with the CounterACT IOC Scanner Plugin, lets you integrate CounterACT with Bromium so that you can:

- Use the Bromium Compliance Policy Template to detect and handle endpoints not running Bromium. A policy template action can be used to trigger Bromium 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 Bromium Module and other third-party vendor integration modules. 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.

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

- Use information learned by Bromium 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 Bromium Module and all other integrated third-party vendor modules, and the corresponding endpoints on which they were found.
- Create CounterACT reports that provide detailed information about:
  - Endpoints with IOCs found by Bromium or CounterACT.
  - IOCs detected during a recent period of time.

To use the module, you should have a solid understanding of Bromium isolation 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 Bromium, the Bromium Enterprise Controller sends a Syslog message (CEF format) containing details of the IOC to the configured CounterACT Appliance. This information includes:

- Source/Destination IP Address
- Timestamp of the event
- File name

- Severity level
- File hash value
- File exists
- Domain Name
- Command and Control

The Bromium Module on that CounterACT 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 Bromium Enterprise Controller.
4. Install the Module.
5. Configure the Module.
6. Run Bromium Policy Templates (optional).
7. Create Custom CounterACT Policies.

Requirements

This section describes:

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

CounterACT Software Requirements

This section describes system requirements:

- CounterACT version 7.0.0, running Service Pack 2.3.3.
- CounterACT IOC Scanner Plugin version 2.0.0 or above.

- CounterACT Syslog Plugin version 3.0.3 or above.
- CounterACT HPS Applications Plugin version 1.1.2 or above.

Supported Vendor Requirements

- Bromium Advanced Endpoint Security 3.2 GA Update 3.

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*.

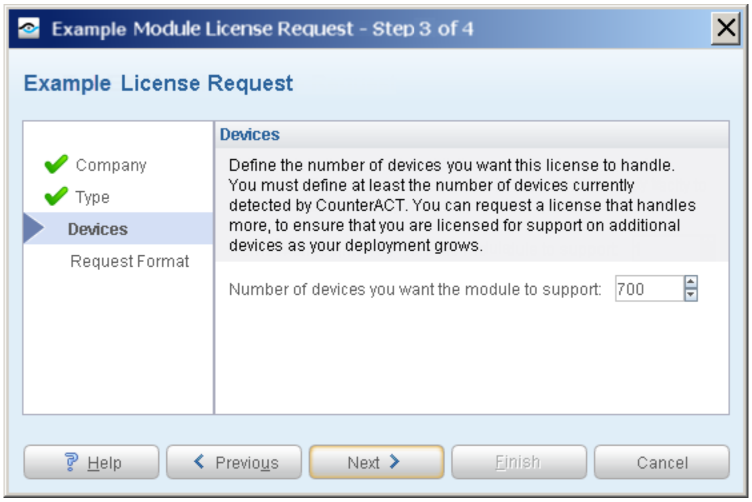
Demo license extension requests and permanent license requests are made from the CounterACT Console.

🗎 *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 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.



Example Module License Request - Step 3 of 4

Example License Request

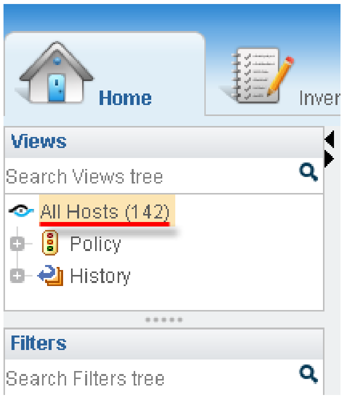
Devices

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.



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.

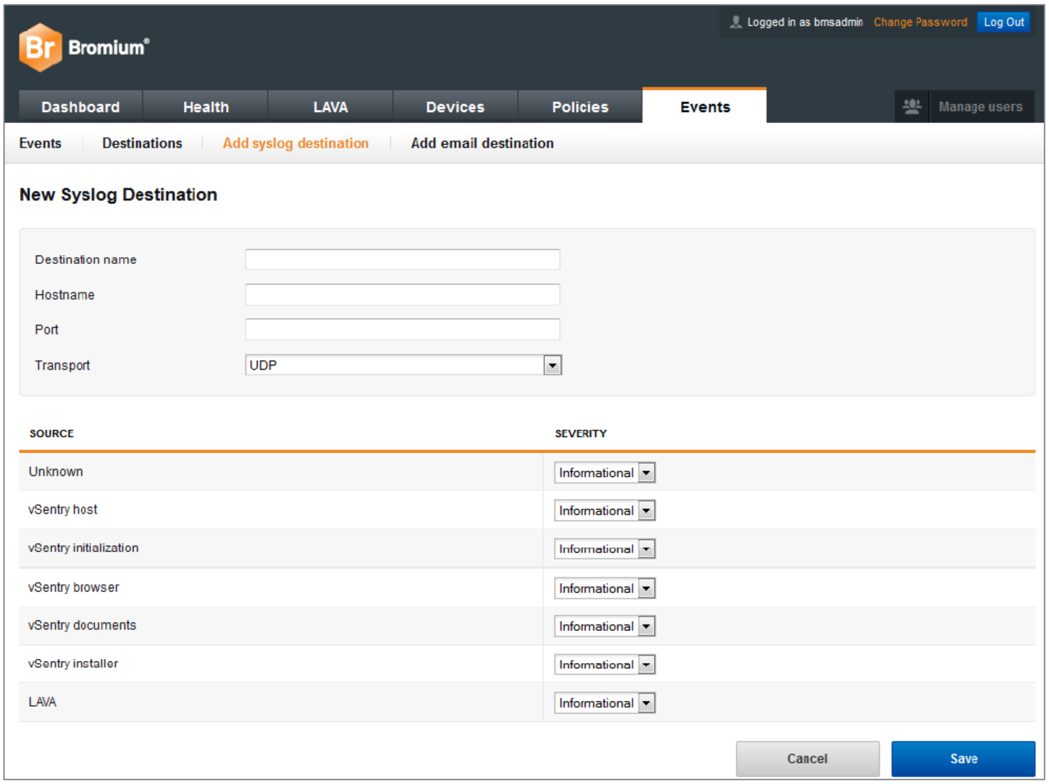
Configure the Bromium Enterprise Controller

The Bromium Enterprise Controller is a Web-based, centralized service that manages and monitors the Bromium clients in the enterprise.

Verify that the Bromium Enterprise Controller server is running, and configure it to send Syslog messages to CounterACT.

To configure the Bromium Enterprise Controller:

1. In the Bromium Web interface, select the Events tab.
2. From the toolbar, select **Add syslog destination**. The New Syslog Destination pane opens.



New Syslog Destination

Destination name	
Hostname	
Port	
Transport	UDP

SOURCE	SEVERITY
Unknown	Informational
vSentry host	Informational
vSentry initialization	Informational
vSentry browser	Informational
vSentry documents	Informational
vSentry installer	Informational
LAVA	Informational

3. In the **Destination name** field, enter a name for the destination.
4. In the **Hostname** field, enter the IP address of the CounterACT Appliance that the event messages will be forwarded to.
5. In the **Port** field, enter **514**.
6. In the **Transport** drop-down list, select **UDP**.
7. Select the Severity of each BEC system alert from the drop-down list next to each alert source. The following severity levels are available:
   - Error
   - Warning
   - Informational
   - (Ignore)
8. Select **Save**.

Install the Module

This section describes how to install the ForeScout Extended Module for Bromium.

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

Once installed on the Enterprise Manager, the Bromium Module is automatically installed on all CounterACT Appliances.

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

To install the plugin:

1. 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 or 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.

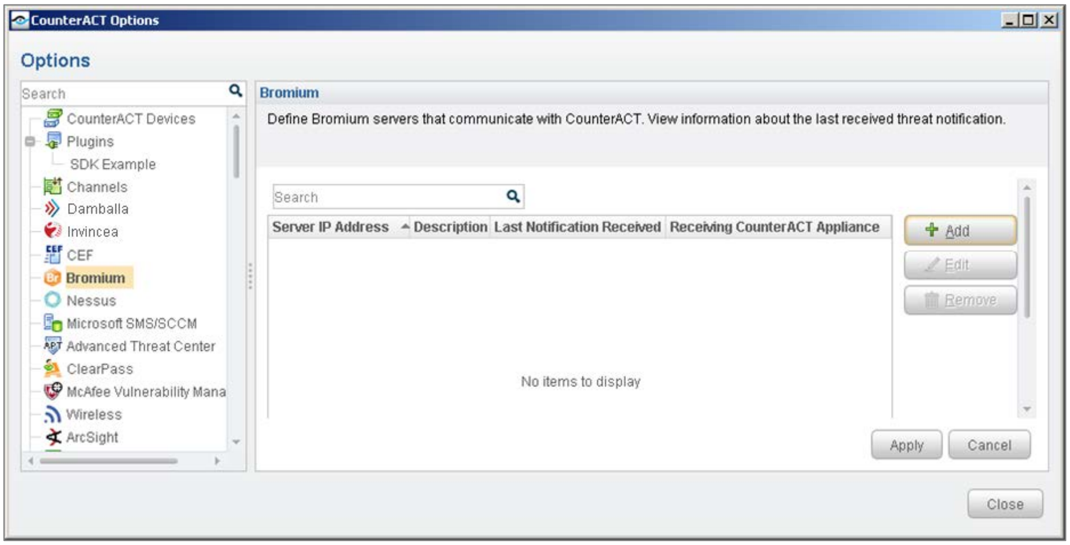
Configure the Module

Configure the module to ensure that CounterACT can communicate with the Bromium server.

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

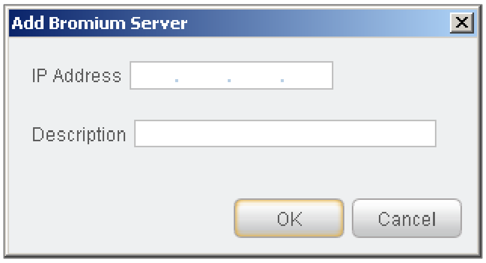


Define Bromium servers that communicate with CounterACT. View information about the last received threat notification.

Server IP Address	Description	Last Notification Received	Receiving CounterACT Appliance

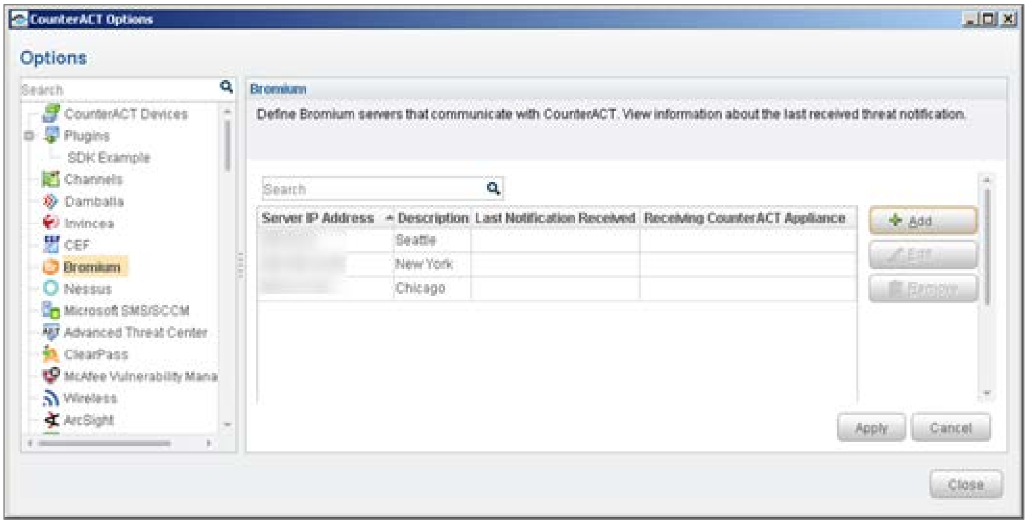
No items to display

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



5. Enter the following information:
   - ***IP Address***. The IP address of the BEC server configured to send Syslog messages to CounterACT in the Configure the Bromium Enterprise Controller section.
   - ***Description***. A textual description of the server.
6. Select **OK**. An entry for the BEC server is added to the table in the Bromium 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 BEC server.
   - ***Receiving CounterACT Appliance***. The IP address of the CounterACT Appliance that received the latest IOC notification from the particular BEC server.



Define Bromium servers that communicate with CounterACT. View information about the last received threat notification.

Server IP Address	Description	Last Notification Received	Receiving CounterACT Appliance
[redacted]	Seattle		
[redacted]	New York		
[redacted]	Chicago		

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

Run Bromium Policy Templates

This module provides the Bromium Compliance Policy Template which can be used to detect and handle endpoints not running Bromium.

Specifically, the template policy detects endpoints that:

- are not CPU virtualization ready.
- are CPU virtualization ready, but do not have Bromium installed.
- have Bromium installed but not running.
- have Bromium installed and running. These endpoints are compliant.

A policy template action can be used to trigger Bromium 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 module. See Configure the Module for details.

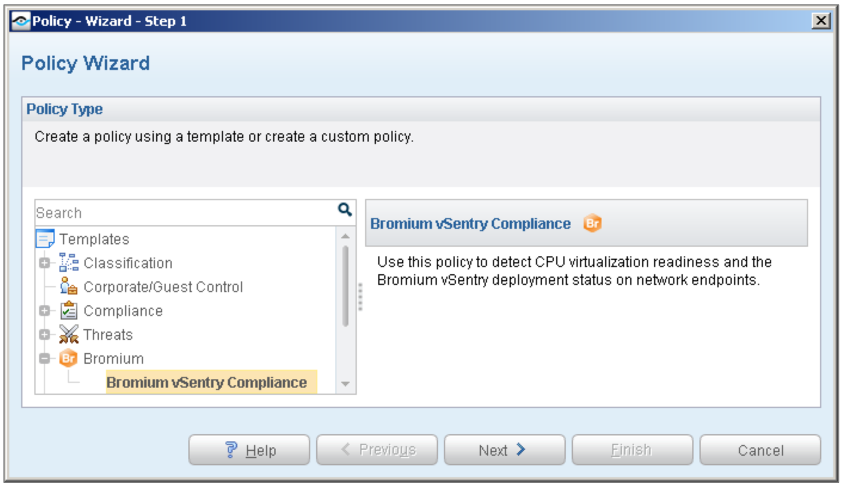
Run the Template

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 **Bromium** folder and select **Bromium vSentry Compliance**. The Bromium vSentry Compliance pane opens.



Policy - Wizard - Step 1

Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

Bromium vSentry Compliance

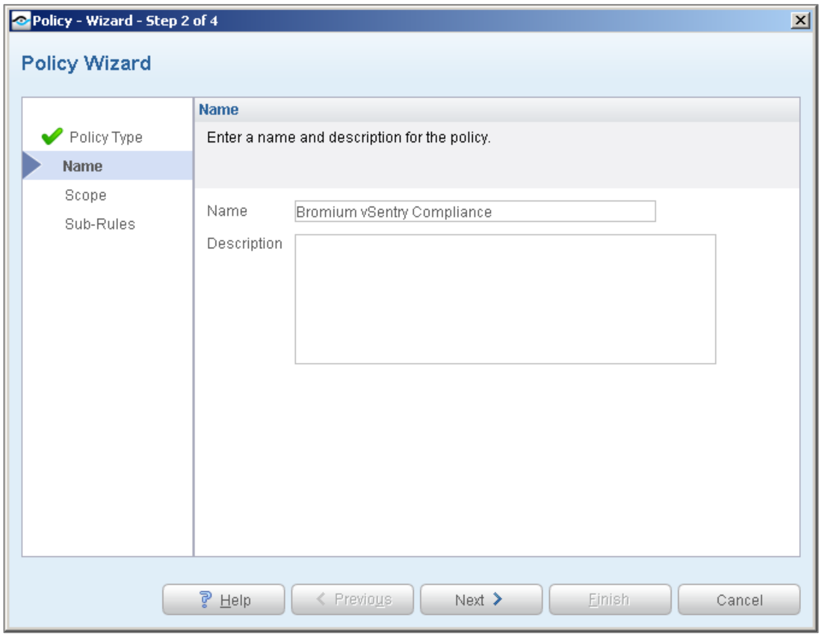
Use this policy to detect CPU virtualization readiness and the Bromium vSentry deployment status on network endpoints.

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.



Policy - Wizard - Step 2 of 4

Policy Wizard

Name

Enter a name and description for the policy.

Name: Bromium vSentry Compliance

Description:

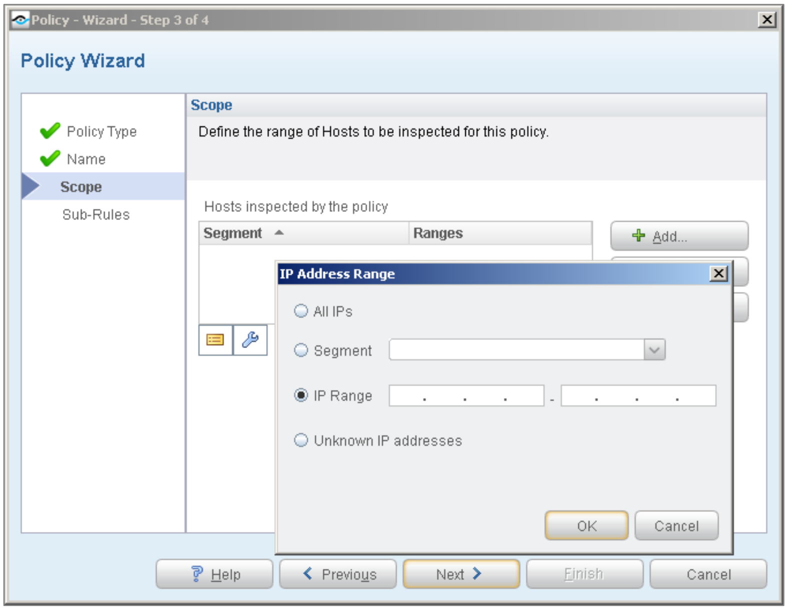
Naming Tips

- 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.

6. 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.



Define the range of Hosts to be inspected for this policy.

○ All IPs
○ Segment
● IP Range
○ Unknown IP addresses

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 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.*

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

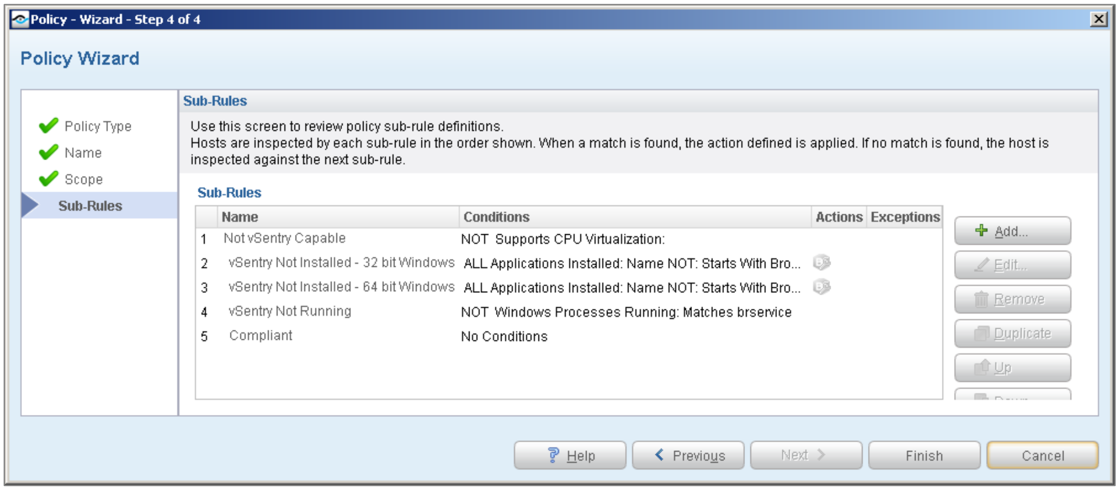
Review Sub-Rules

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.

10. Review the sub-rules.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Not vSentry Capable	NOT Supports CPU Virtualization:		
2	vSentry Not Installed - 32 bit Windows	ALL Applications Installed: Name NOT: Starts With Bro...	⚙	
3	vSentry Not Installed - 64 bit Windows	ALL Applications Installed: Name NOT: Starts With Bro...	⚙	
4	vSentry Not Running	NOT Windows Processes Running: Matches brservice		
5	Compliant	No Conditions		

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

- **Not vSentry Capable** – The endpoint CPU cannot, or is not configured to, support CPU virtualization. As a result, Bromium vSentry cannot be installed.
- **vSentry Not Installed - 32 bit Windows** – Bromium vSentry is not installed on an endpoint in a 32-bit Windows environment.
  - The policy wizard includes an optional action to install Bromium vSentry when this condition is detected. By default, this action is disabled. You can double-click the sub-rule and enable the action.
- **vSentry Not Installed - 64 bit Windows** – Bromium vSentry is not installed on an endpoint in a 64-bit Windows environment.
  - The policy wizard includes an optional action to install Bromium vSentry when this condition is detected. By default, this action is disabled. You can double-click the sub-rule and enable the action.
- **vSentry Not Running** – Bromium vSentry is not running on the endpoint.
- **Compliant** – Bromium vSentry is installed and running on the endpoint.

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

Create Custom CounterACT Policies

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

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.

Bromium Properties and Actions

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with Bromium and IOC Scanner Plugin properties and actions to create 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** to create a policy.

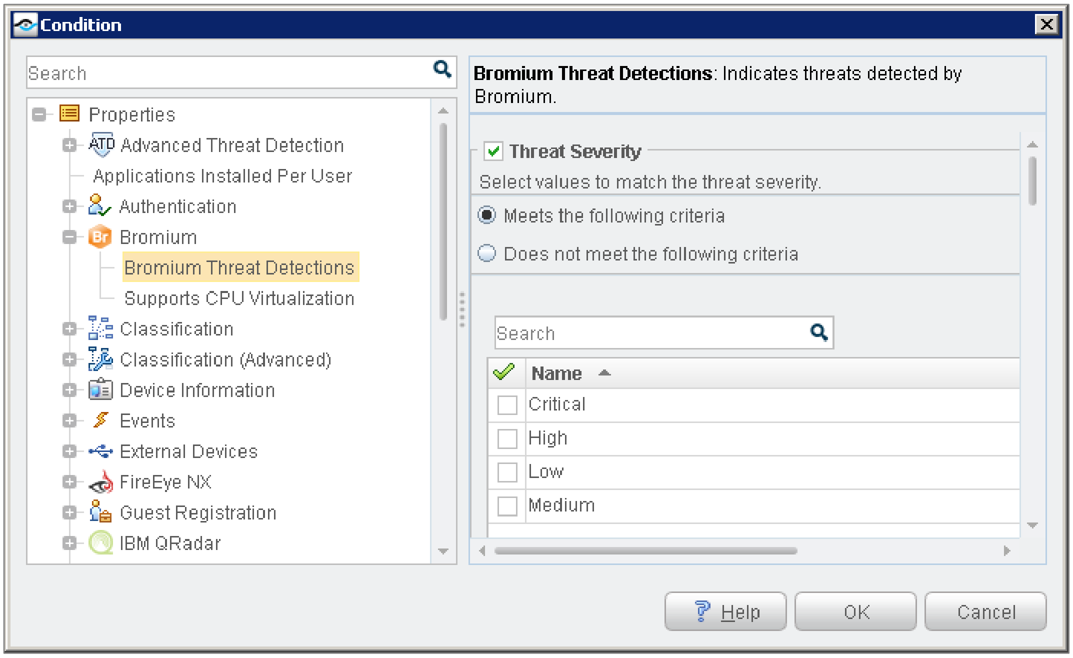
Detecting Bromium Properties – Policy Properties

This section describes the properties that are made available when the Bromium Module is installed.

To access Bromium properties:

1. Open the policy Conditions dialog box.

2. Expand the Bromium folder in the Properties tree.
3. Select **Bromium Threat Detections**.



Condition

Bromium Threat Detections: Indicates threats detected by Bromium.

☑ Threat Severity

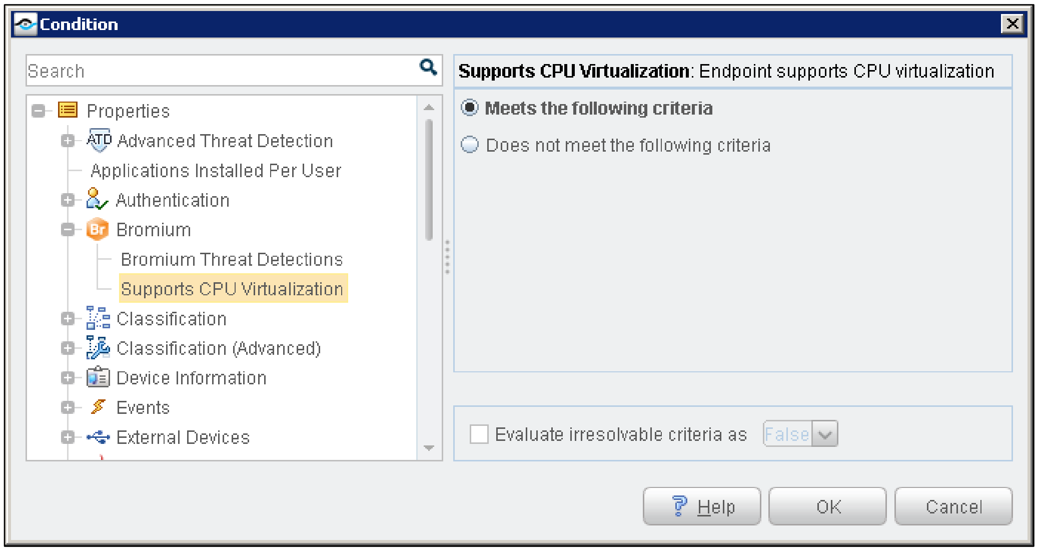
Select values to match the threat severity.

● Meets the following criteria

○ Does not meet the following criteria

✓	Name
□	Critical
□	High
□	Low
□	Medium

4. Make selections based on criteria for detecting threats.
5. Select **Supports CPU Virtualization**.



Condition

Supports CPU Virtualization: Endpoint supports CPU virtualization

● Meets the following criteria

○ Does not meet the following criteria

□ Evaluate irresolvable criteria as False

Search
Properties
Advanced Threat Detection
Applications Installed Per User
Authentication
Bromium
Bromium Threat Detections
Supports CPU Virtualization
Classification
Classification (Advanced)
Device Information
Events
External Devices
Help
OK
Cancel

6. Indicate if the condition detects endpoints on which CPU virtualization is enabled, or on which CPU virtualization is not available or is disabled and select **OK**.

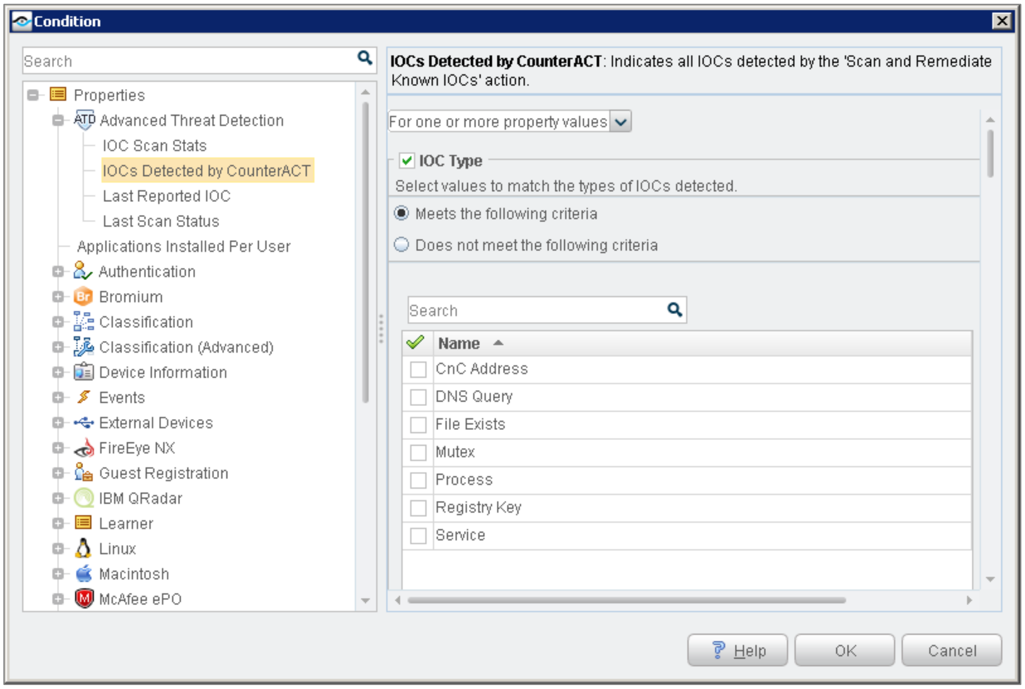
Detecting IOCs – Policy Properties

The following properties contain IOC data reported by the Bromium Module.

- Bromium Threat Detections

The following properties are also available when you install the CounterACT IOC Scanner Plugin.

- Last Reported IOC
- IOCs Detected by CounterACT



IOCs Detected by CounterACT: Indicates all IOCs detected by the 'Scan and Remediate Known IOCs' action.

For one or more property values

☑ IOC Type

Select values to match the types of IOCs detected.

● Meets the following criteria

○ Does not meet the following criteria

Search

✓	Name
□	CnC Address
□	DNS Query
□	File Exists
□	Mutex
□	Process
□	Registry Key
□	Service

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

Bromium – Policy Actions

This section describes the actions that are made available when the Bromium Module is installed.

The following Invincea action is available:

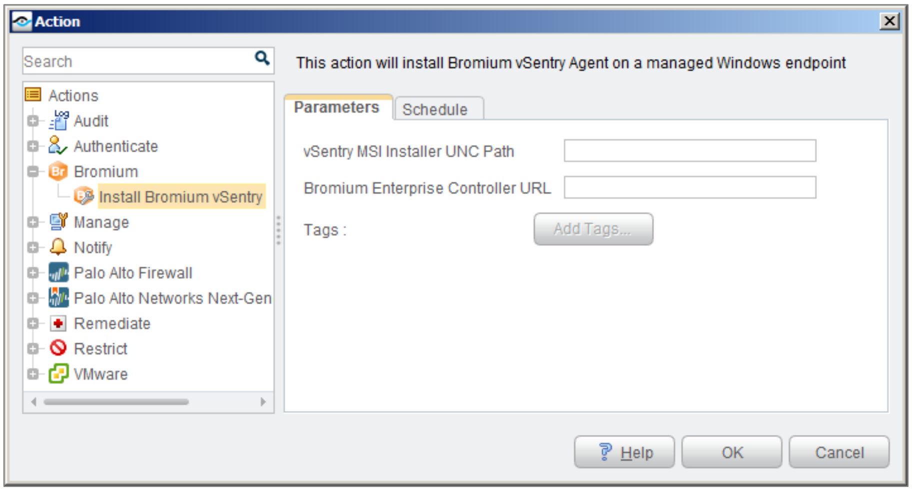
- Install Bromium vSentry

Install Bromium vSentry

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

To apply the Install Bromium vSentry action:

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



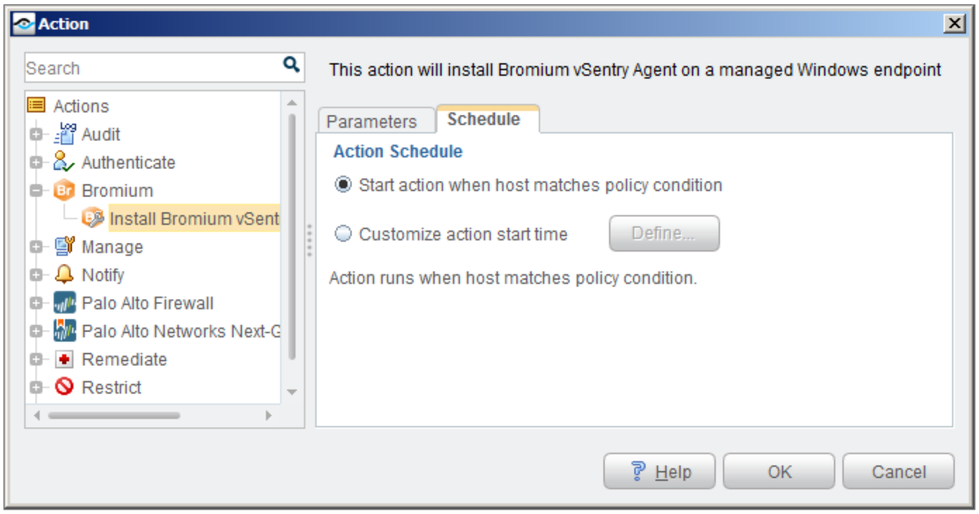
This action will install Bromium vSentry Agent on a managed Windows endpoint

vSentry MSI Installer UNC Path

Bromium Enterprise Controller URL

Tags :

4. In the Parameters tab, enter the following:
   - **vSentry MSI Installer UNC Path**: Enter the path to the vSentry installation file, including the filename.
   - **Bromium Enterprise Controller URL**: Enter the Bromium Enterprise Controller URL.



This action will install Bromium vSentry Agent on a managed Windows endpoint

Action Schedule

● Start action when host matches policy condition

○ Customize action start time

Action runs when host matches policy condition.

5. In the Schedule tab, select one of the following schedules:
   - **Start action when host matches policy condition**: Bromium 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.

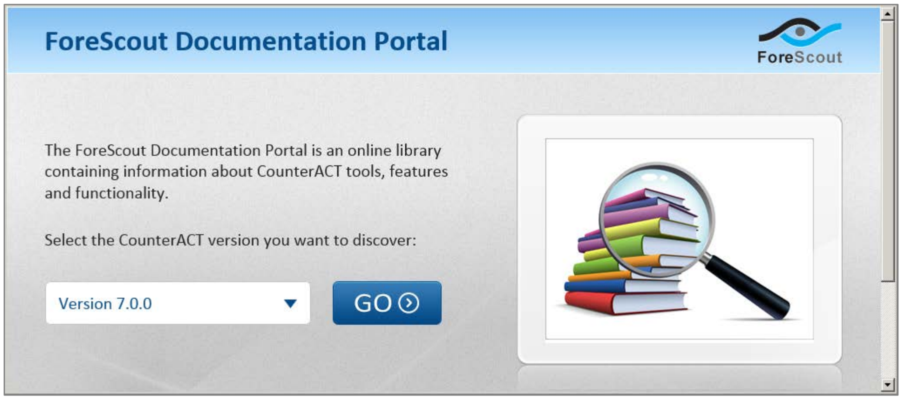
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, 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, functionality and integrations.



ForeScout Documentation Portal

The ForeScout Documentation Portal is an online library containing information about CounterACT tools, features and functionality.

Select the CounterACT version you want to discover:

Version 7.0.0

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

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

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

Legal Notice

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-03-30 14:03