ForeScout® FireEye NX Module

Configuration Guide

Version 2.0.0 and Above

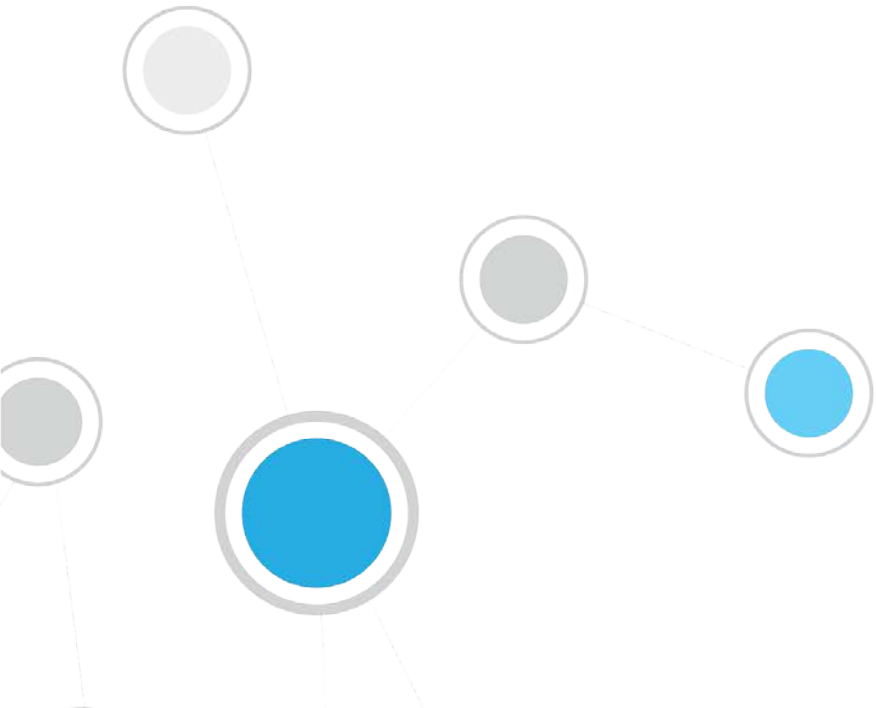


Table of Contents

About the FireEye NX Integration

The FireEye NX module helps corporate security teams simplify the process of identifying, analyzing and blocking advanced cyber-attacks that threaten network security. This integration combines the threat detection mechanisms of FireEye NX with the network visibility and compliance enforcement capabilities of CounterACT® to multiply the benefits of working with an Advanced Threat Detection (ATD) product.

The FireEye NX Module enables ForeScout CounterACT and FireEye NX to work together to quickly detect advanced threats and indicators of compromise (IOCs), contain infected endpoints, and disrupt the cyber kill chain preventing further lateral threat propagation and data exfiltration. The core of the FireEye NX platform is a virtual execution engine, complemented by dynamic threat intelligence that allows the security team to prevent, detect, analyze and respond to today's advanced attacks.

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.

- Receive alerts from FireEye NX of threats detected and immediately perform restrictive actions on the endpoints on which they were detected.
- Scan all Windows endpoints for IOCs reported to CounterACT by FireEye NX in order to identify potential threats and perform actions on potentially infected endpoints. For example, use CounterACT policies to run policy actions 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 NX Documentation

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

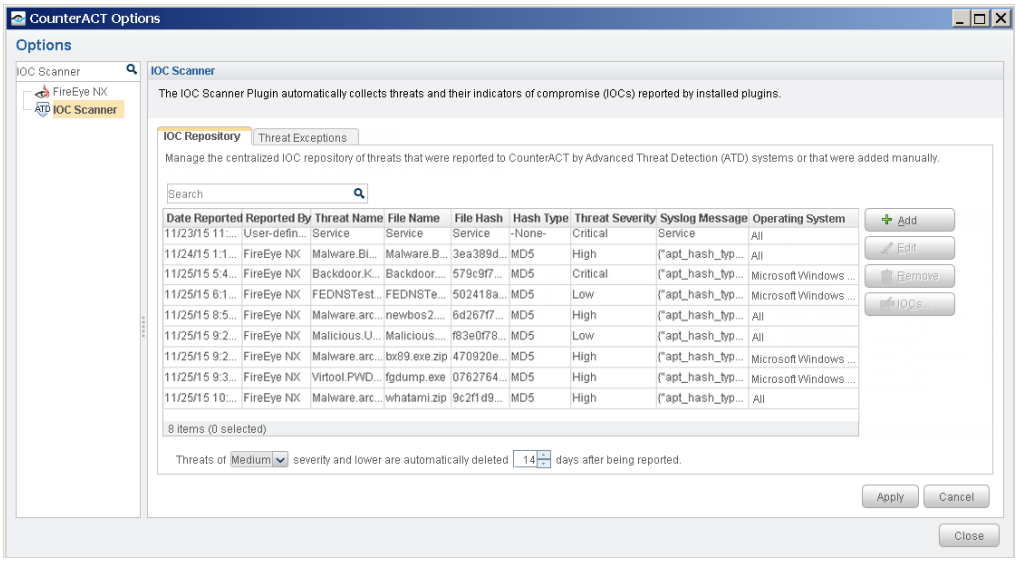
- NX Series Threat Management Guide
- NX Series System Administration Guide

https://www.fireeye.com/products/nx-network-security-products.html

About This Module

This module, together with the IOC Scanner Module, lets you integrate CounterACT with FireEye NX series so that you can:

- Use the FireEye NX Threat Detection Policy Template to create policies that immediately run actions, such as restrictive actions, on endpoints on which FireEye NX detected a Critical or High severity threat.
- Create Custom FireEye NX Policies that use FireEye NX – Policy Properties alongside bundled CounterACT properties and actions to deal with issues not covered in the FireEye NX Threat Detection policy template.
- View new threats reported by FireEye NX and automatically added to the IOC repository. The repository is a viewable table of all threats received from the FireEye NX Module, and is available in the IOC Scanner Module. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.



- Use the *Scan and Remediate Known IOCs* action to scan potentially compromised Windows endpoints for the same indicators of compromise (IOCs) reported by the FireEye NX Module to the IOC repository. For example, you can use the action to:
  - Scan all, or a subset of, Windows endpoints for IOCs used during a threat infection phase.
  - Trigger a threat remediation action to kill initiated processes.

  This action is provided by the IOC Scanner Module. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.
- Create policies that detect and remediate all Windows endpoints on which CounterACT detected specific IOCs reported by the FireEye NX Module. CounterACT provides *Advanced Threat Detection* properties and policy templates to help you work with the IOCs in the IOC repository.

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

- Use CounterACT inventory tools to display all threats reported by FireEye NX and the endpoints for which FireEye NX reported them. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how to handle the endpoints.

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

How It Works

When a threat is detected, the FireEye NX server sends an alert with the threat details to a pre-defined receiving CounterACT device. The alert includes:

- source/destination IP address
- 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 NX 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, and resolves the data as CounterACT properties associated with the endpoint on which the threat was discovered, as well as properties on other Windows endpoints. These properties can be used to trigger policy actions.

The IOC repository includes all the IOCs identified by Advanced Threat Detection systems throughout a threat's lifecycle. CounterACT can use this information to detect the same threat on other endpoints. For example, CounterACT can scan endpoints not monitored by FireEye NX, detect IOCs used during a threat infection phase, and trigger a threat remediation action.

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. Verify that you have met system requirements. See Requirements.
2. Install the Module.
3. Configure the Module.
4. Configure the CounterACT Syslog Module.
5. Configure FireEye NX.
6. Run the FireEye NX Policy Template (optional).
7. Create Custom FireEye NX Policies (optional).

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Module License Requirements
- FireEye NX Requirements

CounterACT continuously supports newly released FireEye NX versions. Refer to the Release Notes for the most updated list:

https://updates.forescout.com/support/files/plugins/fireeye/2.0.0/2.0.0-20000062/RN.pdf

CounterACT Software Requirements

The module 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 Module version 3.1.3
- IOC Scanner Module version 2.0.0 Beta 2 or above
- DNS Query Extension version 1.1.0 or above.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT module. 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.

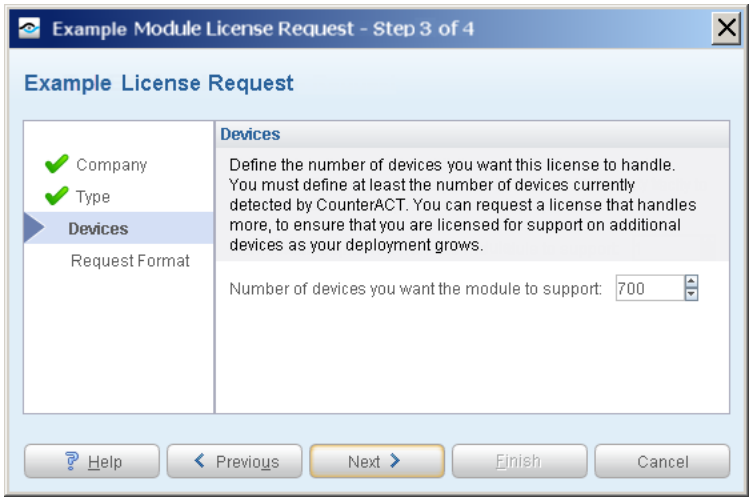
When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

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

Requesting a License

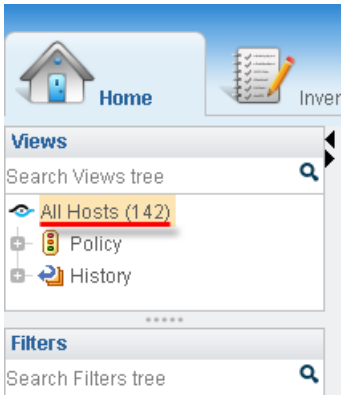
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

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



To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



More License Information

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

FireEye NX Requirements

The module requires the following FireEye NX components:

- FireEye Network Security (NX) Series version 7.5.3 through 7.9
- Admin or Operator access to the NX Series appliance

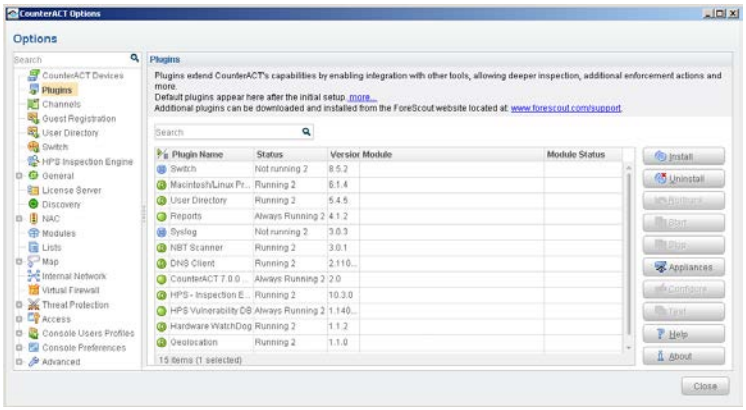
Install the Module

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

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.



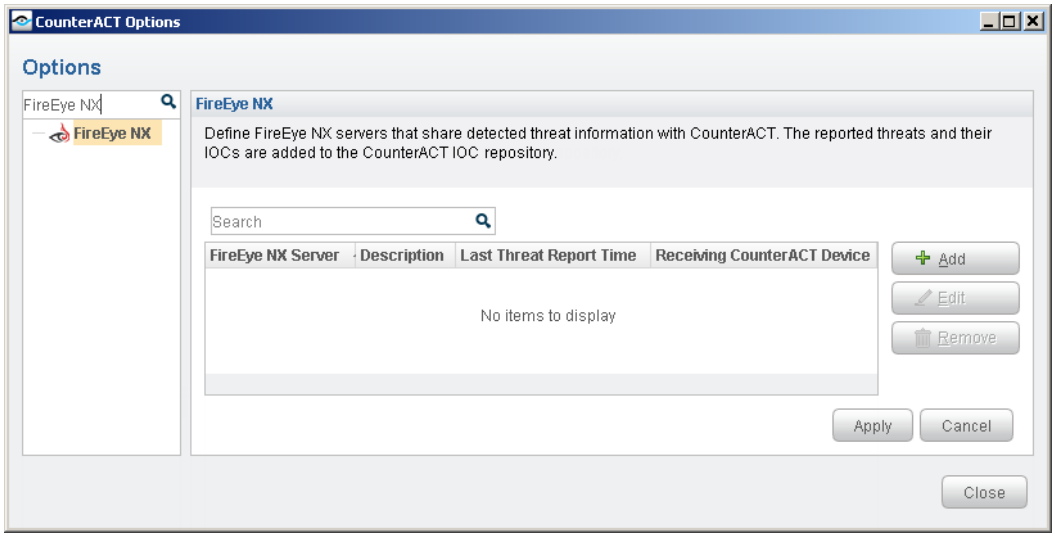
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and 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 FireEye NX service.

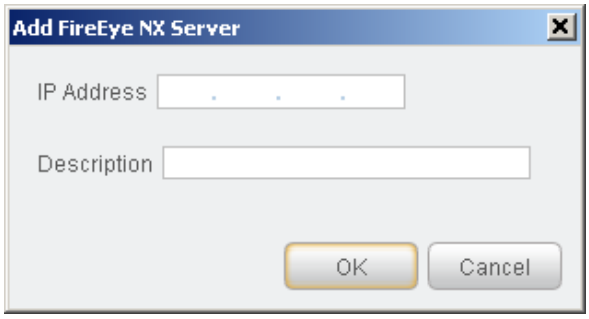
To configure the module:

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 **Plugins** pane, select **FireEye NX**, and select **Configure**. The FireEye NX pane opens.



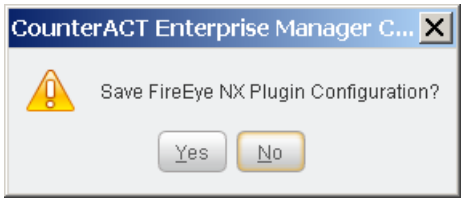
4. Select **Add** to define a FireEye NX server to communicate with CounterACT. The Add FireEye NX Server dialog box opens.

   FireEye EX series servers need to be configured separately in the CounterACT FireEye EX Module.



5. Enter the following information:
   - ***IP Address***. The IP address of the FireEye NX server configured to send rsyslog notifications to CounterACT. See Configure FireEye NX for details.
   - ***Description***. A textual description of the FireEye NX server.
6. Select **OK**. An entry for the FireEye NX server is added to the list in the FireEye NX pane.

   There are two additional display-only fields in the FireEye NX pane:
   - ***Last Threat Report Time***. Indicates the latest date and time when CounterACT received a threat notification from the listed FireEye NX server.
   - ***Receiving CounterACT Device***. The IP address of the CounterACT device that received the latest threat notification from the listed FireEye NX server. Receiving CounterACT devices must be defined to FireEye as rsyslog servers. See Configure FireEye NX for details.
7. In the FireEye NX pane, select **Apply**. A CounterACT Enterprise Manager Console dialog box opens.



8. Select **Yes** to save the module configuration.

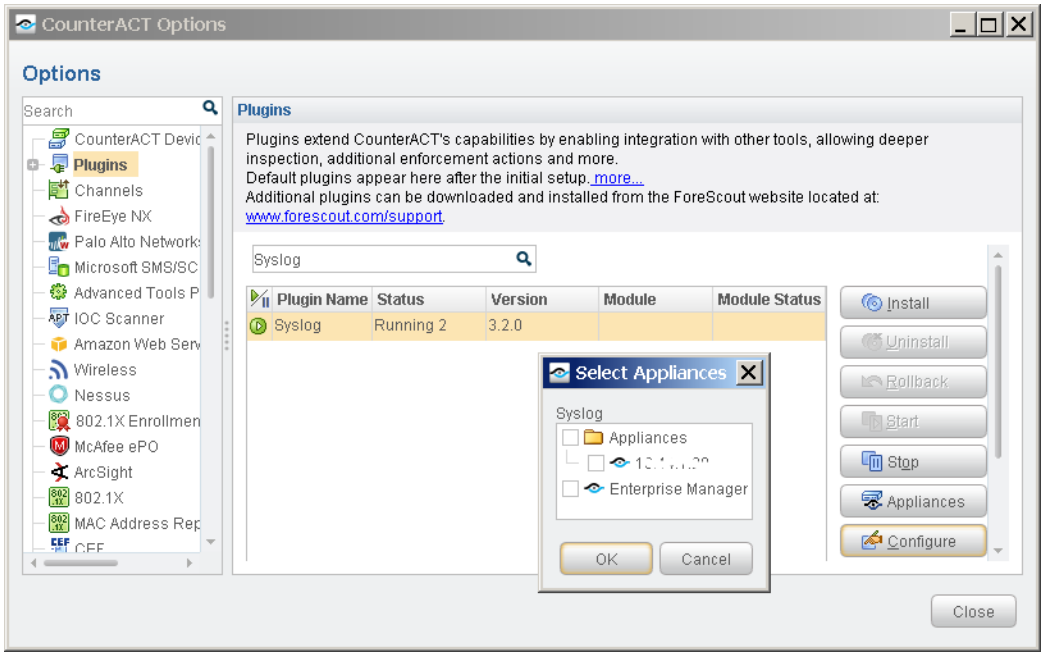
Configure the CounterACT Syslog Module

Configure the CounterACT Syslog Module to enable the receiving CounterACT device to connect to the FireEye NX server and receive notifications.

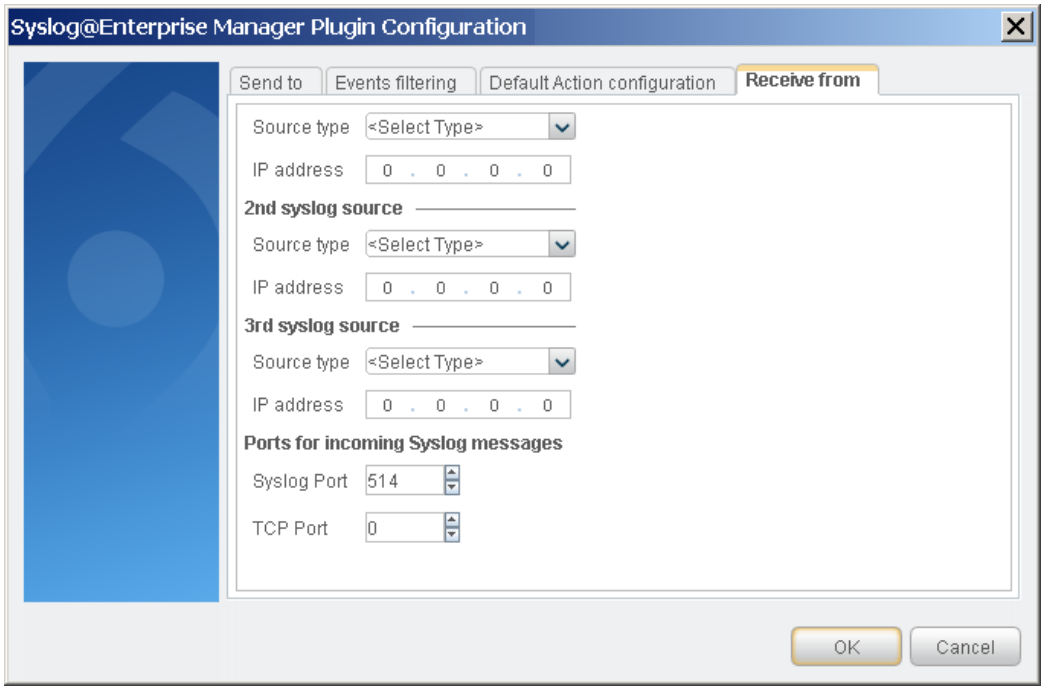
See the *CounterACT Syslog Plugin Configuration Guide* for more information about the Syslog Module configuration.

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



4. Select the CounterACT device defined as an rsyslog server in the Configure FireEye NX section, and select **OK**. The Plugin Configuration window opens.
5. Select the *Receive from* tab.



6. In the first syslog source field that is not yet configured, select the source type **NTSyslog security log**, and enter the IP address of the FireEye NX server.
7. Set the TCP Port to **514**.
8. Select **OK** to save the configuration.

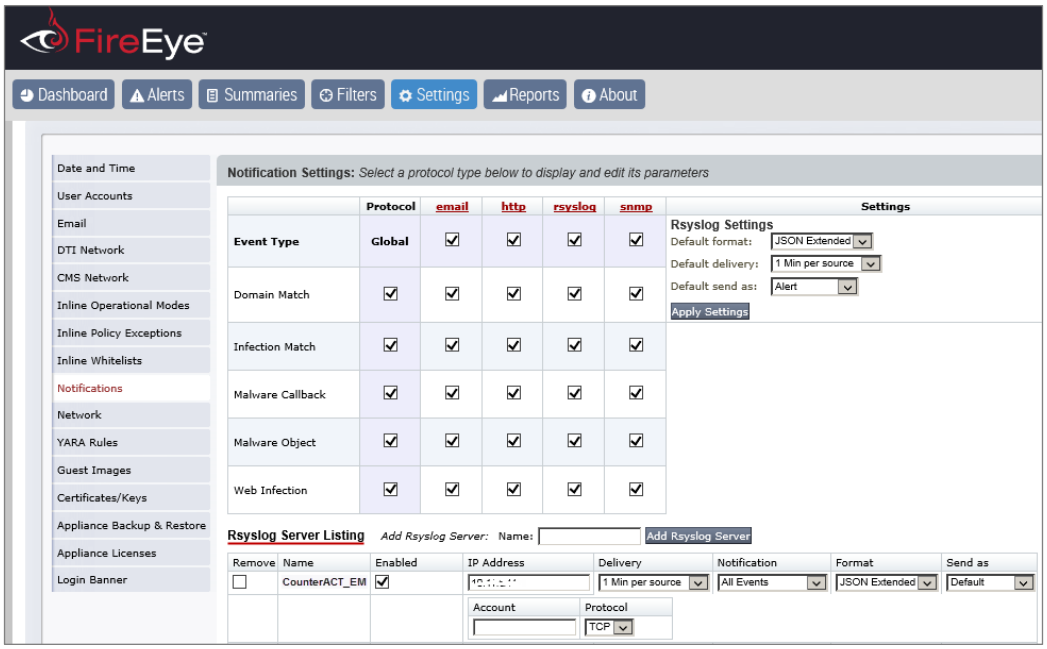
Configure FireEye NX

For each FireEye NX server, designate which CounterACT device will receive the FireEye NX rsyslog notifications. In the FireEye Web UI, define the receiving CounterACT device as an rsyslog server that can receive FireEye rsyslog notifications, and configure the notification settings. Refer to the *NX Series Threat Management Guide* for more information about configuring event notifications.

If your FireEye NX environment was configured for an earlier version of the CounterACT FireEye Module, ensure that the settings match those described in this section.

To define a receiving CounterACT device as an rsyslog server:

1. In the FireEye NX Web UI, select the **Settings** tab.
2. On the side bar, select **Notifications**.
3. Select the **rsyslog** column heading. The **Rsyslog Server Listing** options are displayed at the bottom.



4. In the **Name** box, enter a name for the new rsyslog server, and select **Add Rsyslog Server**. The server is added.
5. Select the **Enabled** checkbox for the new rsyslog server. You can select the **Enable All** checkbox to enable all listed servers to receive rsyslog notifications.
6. In the **IP Address** box of the new rsyslog server, enter the IP address of the receiving CounterACT device.
7. In the **Delivery** dropdown list, select the delivery frequency.
8. In the **Notification** dropdown list, select the event type or **All Events** to send rsyslog notifications to CounterACT when the specified events are detected.
9. In the **Format** dropdown list, select **JSON Extended**.
10. In the **Send as** dropdown list, select the severity classification for the rsyslog notification.
11. Leave the **Account** box blank. This option will be deprecated.
12. In the **Protocol** dropdown list, select **TCP**.
13. Select **Update** to save the new rsyslog server definition.

Run the FireEye NX Policy Template

This module provides the following policy template which you can use to manage and restrict threats in a FireEye NX environment.

- FireEye NX Threat Detection Policy Template

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

FireEye NX Threat Detection Policy Template

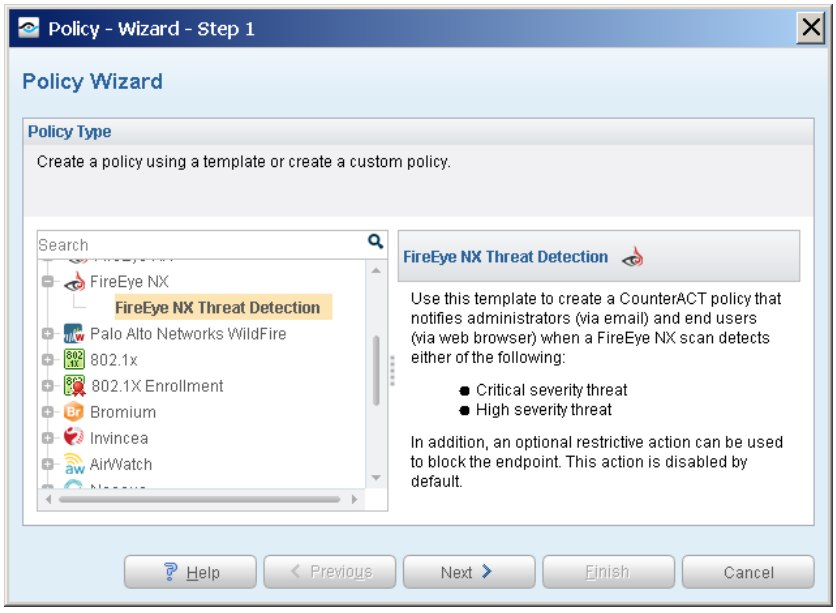
Use this policy to notify administrators (via email) and end users (via web browser) when FireEye NX alerts CounterACT of a *malware-callback* Event Type, and when this event is reported as a Critical or High severity threat. This indicates that the threat has a high probability of infection on the endpoint. In addition, an optional restrictive action can be used to block the endpoint. This action is disabled by default.

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 **FireEye NX** folder and select **FireEye NX Threat Detection**. The FireEye NX Threat Detection pane opens.

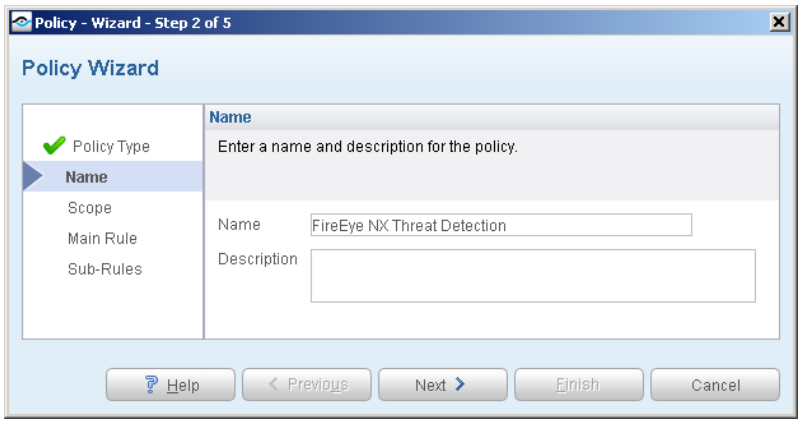


4. Select **Next.** The **Name** page opens.

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.



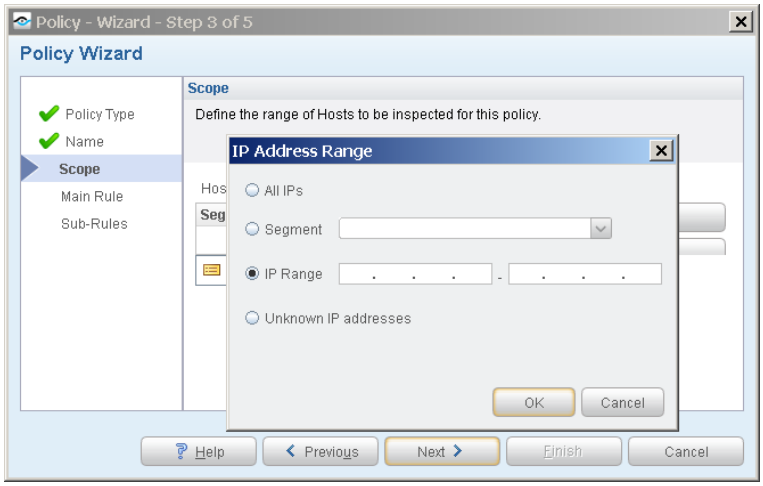
Naming Tips

- 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.



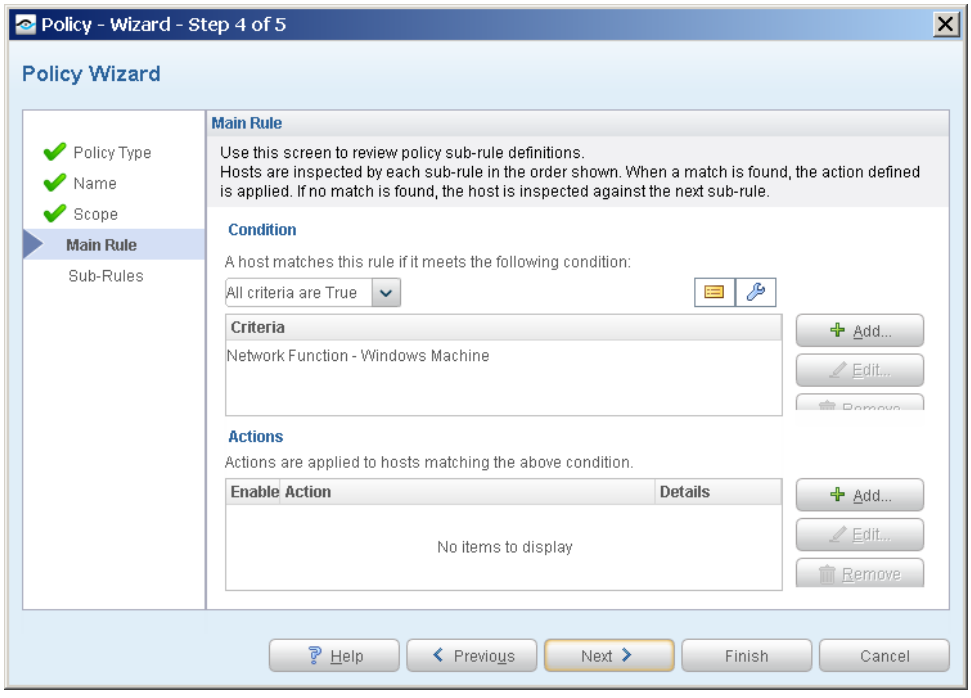
3. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:
   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously 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.

4. Select **OK**. The added range appears in the Scope pane.
5. Select **Next**. The Main Rule pane opens.

Main Rule

The main rule of this policy detects if the endpoint is a Windows machine.



When an endpoint matches the Main Rule, the policy notifies the IT administrator (via email) and the end user (via web browser). In addition, an optional restrictive action can be used to block the endpoint. This action is disabled by default.

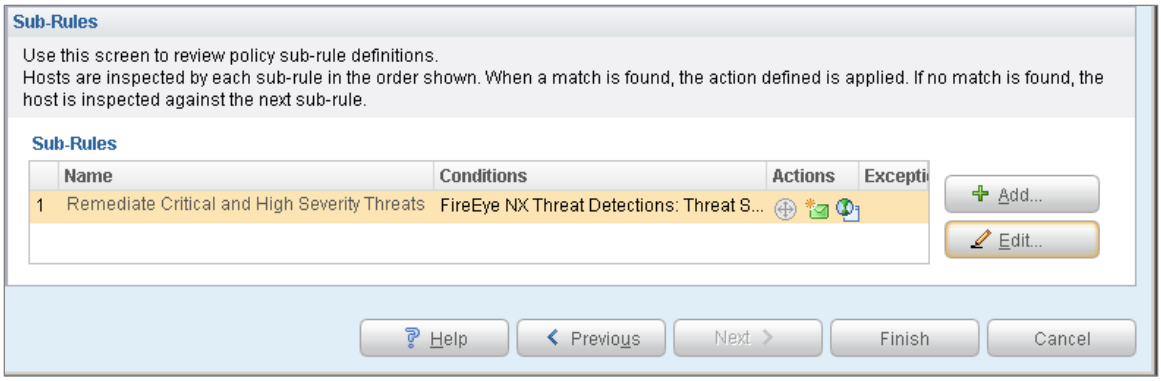
6. Select **Next** to add sub-rules to the policy, or select **Finish** to create the policy.

Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy*.

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. The sub-rule of this policy detects endpoints on which FireEye NX detected a threat severity of Critical or High. The policy template searches for Event Types with a value of *malware-callback*, indicating that FireEye NX explicitly detected this threat on the endpoint with a high probability of infection. When a match is found, the policy notifies the IT administrator (via email) and the end user (via web browser). In addition, an optional restrictive action can be used to block the endpoint. This action is disabled by default.



7. Select **Finish** to create the policy.
8. On the CounterACT Console, select **Apply** to save the policy.

Create Custom FireEye NX Policies

CounterACT policies are powerful tools used for automated endpoint access control and management. You may need to create a custom policy to deal with issues not covered in the FireEye NX policy template.

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 work with FireEye NX related properties to create the custom policies. These items are available when you install the module.

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 NX Module.
- Remediate infected endpoints.

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

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.

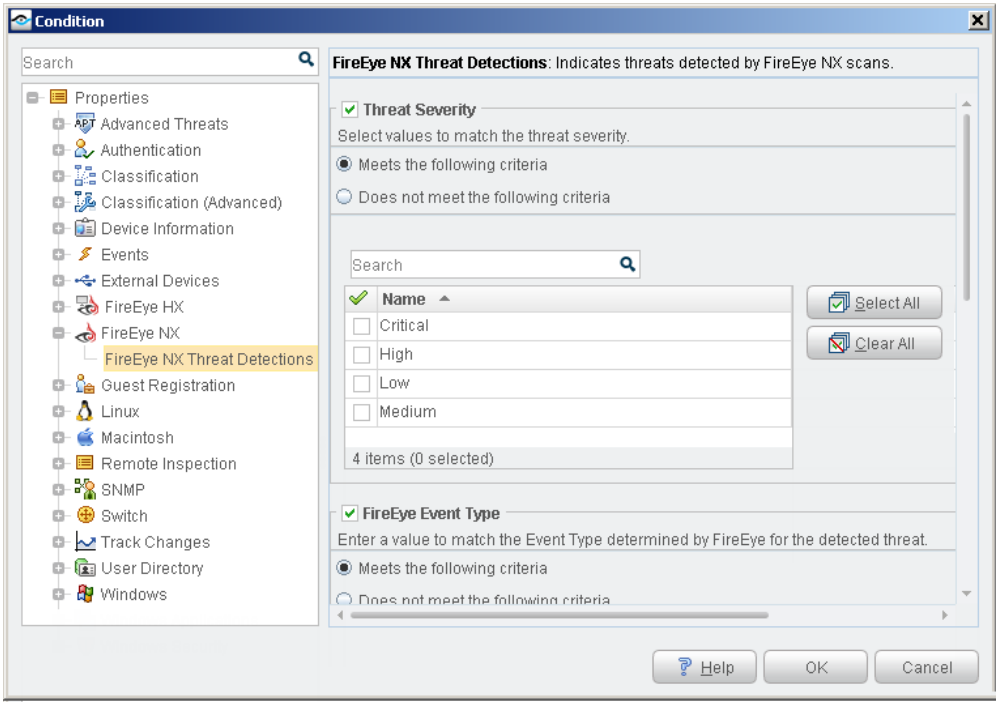
FireEye NX – Policy Properties

This section describes the property that is available when you install the FireEye NX Module.

- FireEye NX Threat Detections

FireEye NX Threat Detections

Use the *FireEye NX Threat Detections* property in CounterACT policies to detect threats reported by FireEye NX. For example, create a policy that detects if FireEye NX has detected a Critical severity threat, and trigger remediation when an endpoint meets this condition.



To access FireEye NX properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the FireEye NX folder in the Properties tree, and select **FireEye NX Threat Detections**. The following information is available:
   - Threat Severity
   - FireEye Event Type. See Best Practices for Working with FireEye NX Event Notifications for more information.
   - Threat Name
   - Threat File Name
   - Threat File Hash
   - Threat Hash Type
   - Syslog Message (rsyslog notification)

Display Inventory Data

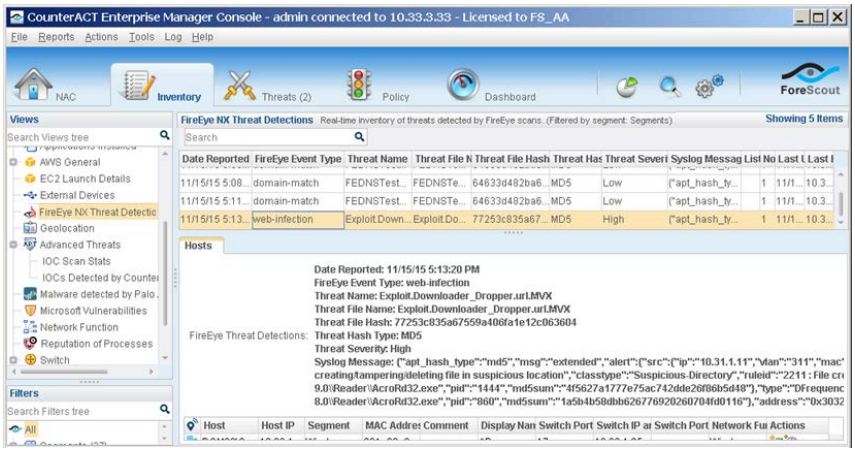
Use the CounterACT Inventory to view a real-time display of threats detected by FireEye NX.

The inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoints that have been detected with specific threats. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how to handle the endpoints.
- Incorporate inventory detections into policies.

To access the inventory:

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to **FireEye NX Threat Detections**.



The following information, based on the FireEye NX Threat Detections property, is available:

- FireEye Event Type
- Threat Name
- Threat File Name
- Threat File Hash
- Threat Hash Type
- Threat Severity
- Last Update

Refer to *Working at the Console>Working with Inventory Detections* in the *CounterACT Console User's Manual* or the Console Online Help for information about working with the CounterACT Inventory.

Best Practices for Working with FireEye NX Event Notifications

Event notifications inform you when specific events occur, alerting you of potential threats so that you can protect the security of your network.

This section describes best practices that help you:

- Analyze the threat severity of FireEye NX event notifications received by CounterACT.
- Decide how to respond to these notifications using CounterACT policies.

There are five event notification categories, listed according to the typical threat severity associated with the event:

- Malware Callback
  - Critical Severity
- Web Infection and Malware Object
  - High Severity
- Domain Match and Infection Match
  - Low and Medium Severity

These notifications are detected by CounterACT as *FireEye Event Type* criteria via the FireEye NX Threat Detections property.

The FireEye NX Threat Detection Policy Template provided by the module searches for Malware Callback event types since these have the highest probability of infection. You can create custom FireEye NX policies that search for other event types. See Create Custom FireEye NX Policies.

Malware Callback

A *malware callback* notification on an endpoint indicates that there is an established connection between the infected endpoint and a command and control (CnC) server. This event is typically categorized by CounterACT with a threat severity of Critical.

If you identify one or more malware callback notification on an endpoint that also received a web infection notification (see Web Infection and Malware Object), there is a very high probability that the endpoint is infected.

At this point, FireEye recommends immediately patching or otherwise remediating the infected system, as well as preventing the CnC server from communicating with all endpoints in your network.

Respond Using CounterACT Policies

- Create a policy to automatically trigger restrictive actions (Switch Block, Assign to VLAN or Virtual Firewall) on the potentially infected endpoint.
- If you have other ForeScout Modules installed in your environment, various orchestration actions may be available to trigger vulnerability scanning or patch management.
- In addition, the IOC Scanner Module allows you to monitor communications to the CnC server across all endpoints in your network. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.

Web Infection and Malware Object

A *web infection* notification on an endpoint indicates that a web browser initiated an outbound connection to a website that was ultimately determined to be malicious. These attacks usually penetrate the firewall and other perimeter security devices.

A *malware object* notification indicates the presence of a file attachment with a malicious executable payload. Both of these events are typically categorized as High severity threats.

FireEye recommends confirming the infection by scanning the endpoint to verify that the IOC found matches that of the endpoint. Viewing the IOC details associated with a web infection or malware object event shows registry changes, file system changes, and processes that have been started as a result of the infection. If suspicious changes in the FireEye analysis match changes on the actual endpoint, then the infection can be confirmed.

Respond Using CounterACT Policies

- Create a custom policy that scans the potentially infected endpoint (*Scan and Remediate Known IOCs* action) when such a notification is received (*IOCs Detected by CounterACT* condition). Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.
- In addition, you can create a policy to automatically trigger restrictive actions (Switch Block, Assign to VLAN or Virtual Firewall) on the potentially infected endpoint when such a notification is received.

Domain Match and Infection Match

A *domain match* notification indicates that the website domain has been identified as the source of malicious behavior. An *infection match* notification refers to the process of identifying a URL pointing to the initial web infection. Both of these events are typically categorized as Low or Medium severity threats.

Respond Using CounterACT Policies

- When these types of notifications are received on their own, they likely do not represent an infection. It is recommended to avoid running policies that automatically trigger restrictive actions.
- When these types of notifications are received alongside other, higher risk notifications listed above, follow the best practices listed for each notification type.

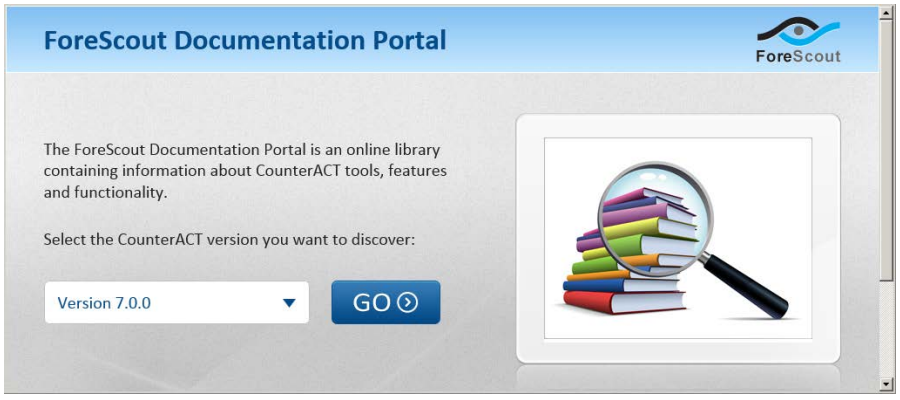
Additional CounterACT Documentation

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 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

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

2017-01-19 12:41