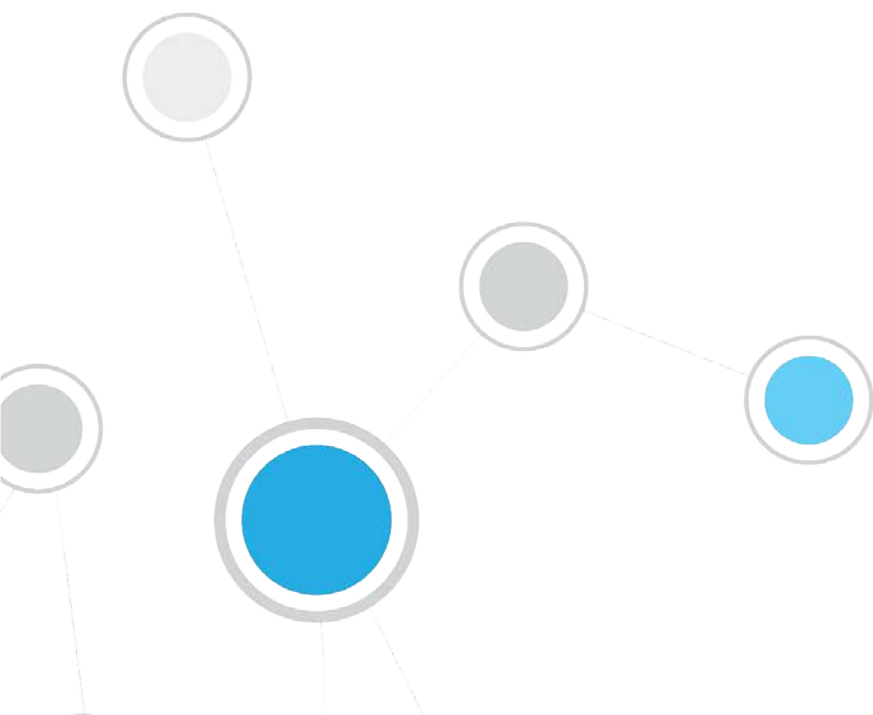




# CounterACT™ FireEye HX Plugin

## Configuration Guide

**Version 1.1.0**



## Table of Contents

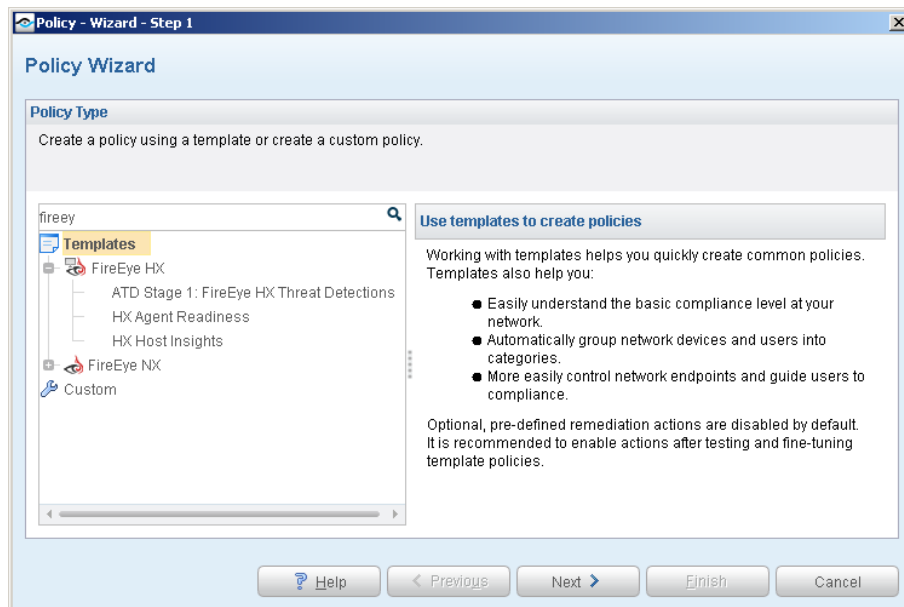
<b>About the FireEye HX Integration.....</b>	<b>3</b>
Advanced Threat Detection with the IOC Scanner Plugin .....	3
Use Cases .....	4
Additional FireEye HX Documentation .....	5
<b>About This Plugin .....</b>	<b>5</b>
How It Works.....	6
What to Do.....	6
<b>Requirements.....</b>	<b>7</b>
CounterACT Software Requirements .....	7
ForeScout Module License Requirements .....	7
Requesting a License .....	7
More License Information .....	8
FireEye HX Requirements .....	8
<b>Configure FireEye HX .....</b>	<b>9</b>
<b>Install the Plugin.....</b>	<b>9</b>
<b>Configure the Plugin.....</b>	<b>10</b>
Configure Additional FireEye HX Server Details .....	12
Restarting the Plugin - Traffic Throttling.....	13
<b>Run FireEye HX Policy Templates .....</b>	<b>14</b>
ATD Stage 1: FireEye HX Threat Detections Policy Template .....	14
HX Agent Readiness Policy Template.....	17
HX Host Insights Policy Template .....	21
<b>Create Custom FireEye HX Policies .....</b>	<b>25</b>
FireEye HX – Policy Properties.....	25
<b>Display Inventory Data .....</b>	<b>27</b>
<b>Additional CounterACT Documentation .....</b>	<b>29</b>
Documentation Portal .....	29
Customer Support Portal .....	29
CounterACT Console Online Help Tools.....	30

## About the FireEye HX Integration

FireEye Endpoint Security (HX Series) offers threat detection capabilities from the network core to the endpoint, enhancing endpoint visibility and enabling a flexible and adaptive defense against known and unknown threats.

The FireEye HX - CounterACT integration helps security teams simplify the process of identifying, analyzing and blocking advanced cyber-attacks. FireEye HX, unlike other FireEye components, gets into the endpoint security space. This integration combines the threat detection mechanisms of FireEye HX with the network visibility and compliance enforcement capabilities of CounterACT to multiply the benefits of working with an endpoint threat detection and response (EDR) product.

This integration leverages the FireEye HX agent installed on Windows endpoints to provide threat and endpoint information that complements information detected by CounterACT (for example, information reported by SecureConnector). Endpoints suspected of infection can be isolated, and remediation actions can be initiated automatically instead of requiring human intervention, allowing corporate security teams to deal with other high profile issues.



## Advanced Threat Detection with the IOC Scanner Plugin

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

- A centralized repository of all threats and their IOCs (indicators of compromise) reported to CounterACT by third-party endpoint detection and response (EDR), and other threat prevention systems, or added manually.

- Mechanisms that scan all Windows endpoints for threat and IOC information reported to CounterACT, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- **ATD Stage 1 (this plugin): Detect and report threats on endpoints:** FireEye HX instances in your environment report threats to this plugin as they are detected on endpoints. Use the template provided with this plugin to create policies that apply block, quarantine, or other CounterACT actions based on the severity of detected threats.

In addition to this initial response, all threats reported by this plugin are automatically submitted to the IOC Scanner plugin, which parses the threat to yield indicators of compromise (IOCs) - measurable events or state properties that can be used as a "fingerprint" to identify the threat. The IOC Scanner Plugin uses these IOCs to mount further scan/analyze/remediate stages of CounterACT's ATD response, as follows:

- **ATD Stage 2 (IOC Scanner Plugin): Real-time hunt for endpoints of interest based on threats and IOCs:** The IOC Scanner Plugin detects endpoints with IOCs associated with recently reported threats.
- **ATD Stage 3 (IOC Scanner Plugin): Evaluation and remediation:** The IOC Scanner Plugin evaluates the profile of IOCs on endpoints of interest to determine the likelihood that an endpoint is compromised, and applies appropriate blocking/remediation actions.

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

## Use Cases

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

### Evaluate Endpoint Readiness

Use the HX Agent Readiness template to create a CounterACT policy that:

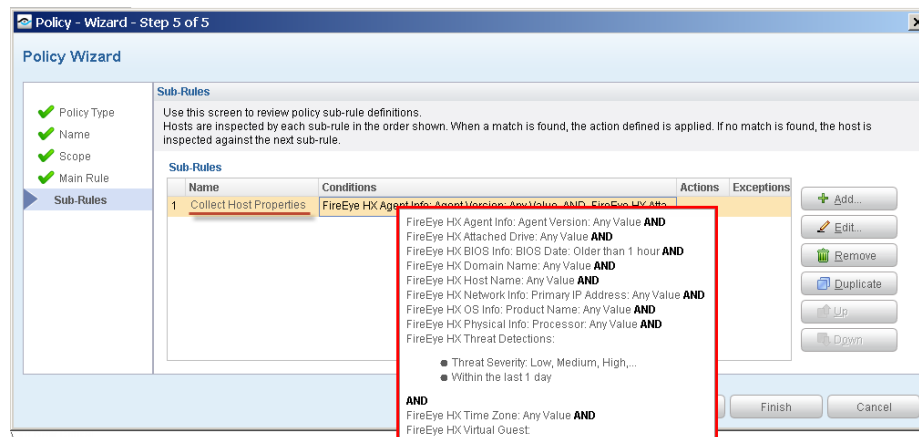
- Ensures that the FireEye HX agent is installed on all Windows endpoints supported by FireEye HX.
- Ensures that the FireEye HX agent is running on all Windows endpoints supported by FireEye HX.
- Ensures that the FireEye HX agent can communicate with the defined FireEye HX server.

### Retrieve Endpoint Insights from FireEye HX

Leverage the presence of installed FireEye HX agents to receive the following endpoint information in situations where SecureConnector is not installed or Remote Inspection is not used:

- Threat information detected by FireEye HX on specific endpoints.

- Information of all endpoints monitored by the FireEye HX agent. For example, network and host BIOS information.



## Prevent Lateral Threat Propagation

Use a policy-based workflow to automatically handle endpoints on which FireEye HX detected specific threats. For example, by isolating the compromised endpoint so that no other machine can communicate with the endpoint.

## Additional FireEye HX Documentation

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

<https://www.fireeye.com/products/hx-endpoint-security-products.html>

## About This Plugin

This plugin lets you integrate CounterACT with FireEye HX series so that you can:

- Use the [HX Agent Readiness Policy Template](#) to create policies that determine the readiness of the FireEye HX agent on Windows endpoints.
  - If the agent is not installed, the policy can redirect users to a URL from which to install the agent.
  - If the agent is not running, the policy can run a script to start the agent.
  - If the agent is running but is not communicating with the defined FireEye HX server, the policy can notify the administrator.
- Use the CounterACT [HX Host Insights Policy Template](#) to create policies that collect endpoint information using the FireEye HX agent.
- Use the [ATD Stage 1: FireEye HX Threat Detections Policy Template](#) policy template to create policies that immediately run appropriate actions, such as restrictive actions, on endpoints on which FireEye HX detected a threat. You can apply different actions to endpoints based on the severity of the detected threat.

- [Create Custom FireEye HX Policies](#) that use properties provided by this plugin, and other CounterACT properties and actions, to deal with issues not covered in the ATD Stage 1: FireEye HX Threat Detections Policy Template policy template.
- View new IOCs related to threats reported by FireEye HX and automatically added to the IOC repository. These IOCs are used by the IOC Scanner Plugin for Advanced Threat Detection (ATD) and recovery. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.
- Use CounterACT inventory tools to display all threats and the corresponding endpoints on which they have been found.

To use the plugin, you should have a solid understanding of FireEye Endpoint Security (HX Series) concepts, functionality and terminology, and understand how CounterACT policies and other basic features work. Additionally, you should have a solid understanding of how to leverage threat intelligence distributed by IOCs.

## How It Works

### CounterACT Queries FireEye HX for Endpoint Information

When the FireEye HX agent runs on corporate endpoints, it provides the FireEye HX server with endpoint information, such as the host time zone. This plugin presents this endpoint information in CounterACT as host properties, which can be included in CounterACT policy conditions. To evaluate these properties, CounterACT queries the FireEye HX server.

### Threat Notifications from FireEye HX

When FireEye HX detects suspicious activity on an endpoint, the FireEye HX server sends an alert notification in syslog format to a pre-defined connecting CounterACT device. When the alert notification indicates a threat, the FireEye HX Plugin queries the FireEye HX server for more details. CounterACT presents the threat detection event as a host property, and passes detailed threat information to the IOC repository maintained by the IOC Scanner Plugin.

## What to Do

You must perform the following to work with this plugin:

1. Verify that you have met system requirements. See [Requirements](#).
2. [Configure FireEye HX](#).
3. [Install the Plugin](#).
4. [Configure the Plugin](#).
5. [Run FireEye HX Policy Templates](#).
6. [Create Custom FireEye HX Policies](#) (optional).

# Requirements

This section describes system requirements, including:

- [CounterACT Software Requirements](#)
- [ForeScout Module License Requirements](#)
- [FireEye HX Requirements](#)

## CounterACT Software Requirements

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

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

## ForeScout Module License Requirements

This plugin is packaged as a ForeScout Module, and requires a module license. When installing the plugin you are provided with a 90-day demo module license.

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

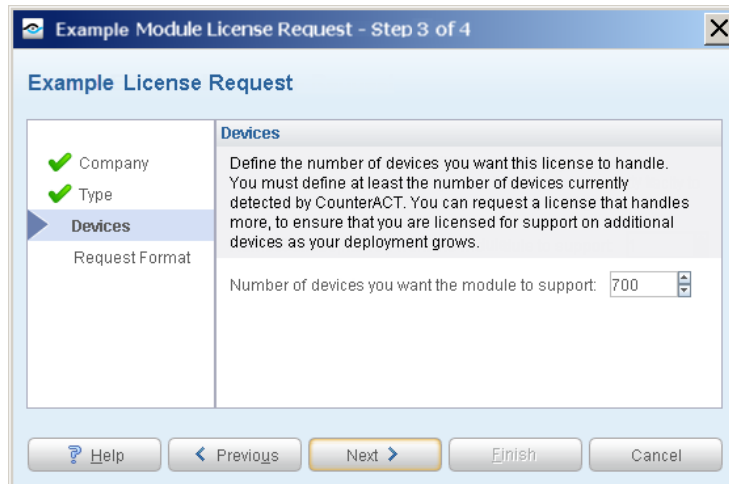
When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the plugin, you must purchase the license.*

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

### Requesting a License

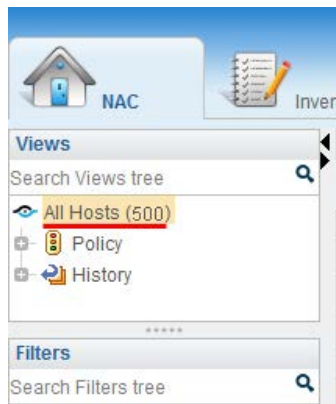
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that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

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



**To view the number of currently detected devices:**

1. Select the **NAC** tab.
2. In the Views pane, 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](mailto:license@forescout.com) for more information.

## FireEye HX Requirements

The plugin requires the following FireEye HX components:

- FireEye Endpoint Security (HX Series) version 3.0.x or 3.1.x with an appliance that is running and that has an established connection to the Internet.
- A user defined on the appliance with the following roles:
  - The *admin* or *fe\_services* role for initial appliance configuration
  - The *api\_analyst* or *fe\_services* role for access to the appliance



## Configure FireEye HX

For each FireEye HX server, designate a CounterACT device to receive FireEye HX syslog notifications. In the HX Series appliance, define the connecting CounterACT device as a remote syslog server, and configure the notification settings. Refer to the *FireEye HX & HXD Series System Administration Guide* for more information about configuring event notifications.

### To define a connecting CounterACT device as a remote syslog server:

1. Log in to the HX Series appliance CLI (command-line interface) as a user assigned the *admin* or *fe\_services* role for the HX Series appliance.

2. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

3. Add a remote syslog server destination:

```
hostname # logging <remote-IP-address> trap none
hostname # logging <remote-IP-address> trap override class cef
priority info
```

where **<remote-IP-address>** is the connecting CounterACT device IP address

4. Save your settings:

```
hostname # write mem
```

When the operation completes, the following message is displayed:

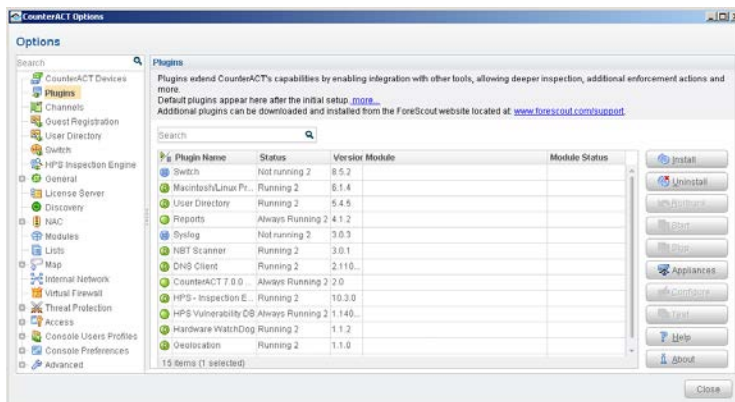
```
Saving configuration file ... Done!
```

## Install the Plugin

This section describes how to install the plugin. Before you install this plugin, first install the IOC Scanner Plugin. See [CounterACT Software Requirements](#).

### 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](mailto:beta@forescout.com).
  - Otherwise, navigate to the [Customer Support, ForeScout Modules](#) page and download the plugin **.fpi** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.



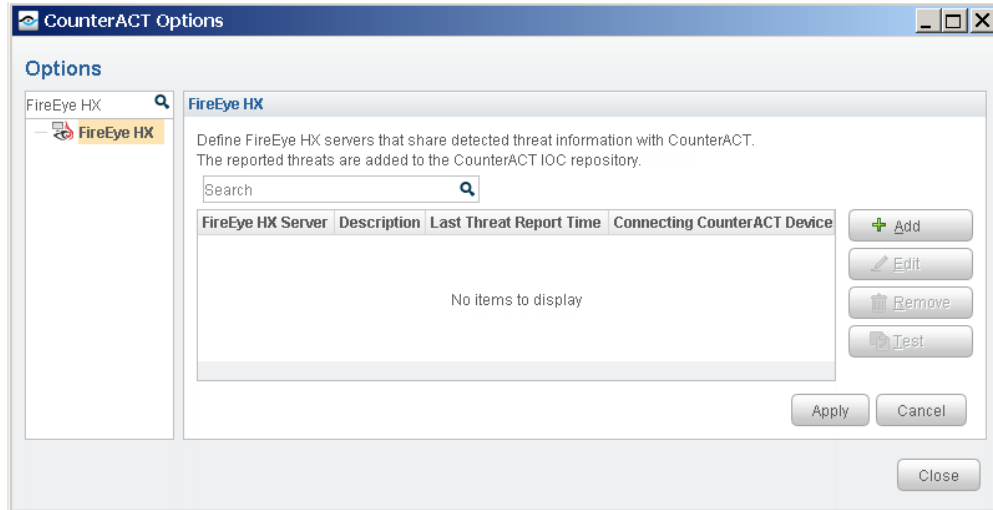
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **.fpi** file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and then select **Install**.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. 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

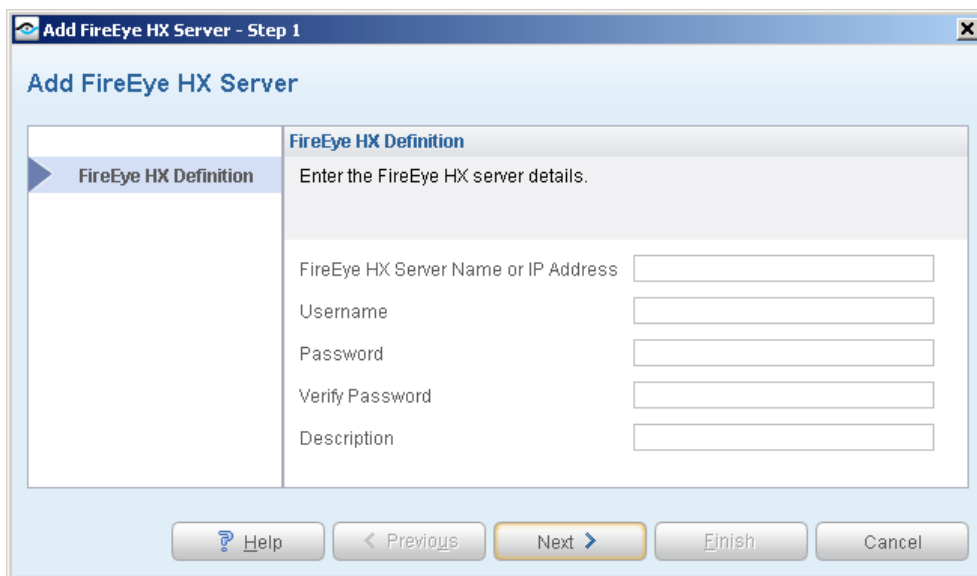
Configure the plugin to ensure that CounterACT can communicate with the FireEye HX service.

### To configure the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Plugins** folder.
3. In the **Plugins** pane, select **FireEye HX**, and select **Configure**. The FireEye HX pane opens.



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



5. Enter the following information:
  - **FireEye HX Server Name or IP Address.** The name or IP address of the FireEye HX server that sends notifications to CounterACT. See [Configure FireEye HX](#) for details.

The server prefix (HTTP/HTTPS) and the port number are configurable via an install.properties file that comes with the plugin. See [Configure Additional FireEye HX Server Details](#).

- **Username.** A username assigned the *api\_analyst* or *fe\_services* role for access to the HX Series appliance.
- **Password** and **Verify Password.** The password for the above user. Retype the password to confirm it.

- **Description.** Textual description of the FireEye HX server or a relevant comment.
6. Select **Next**. The Advanced pane opens.



7. Select the CounterACT device that will handle all communication between FireEye HX and CounterACT devices.
8. Select **Finish**. An entry for the FireEye HX server is added to the list in the FireEye HX pane.
9. (Optional) Repeat these steps to define additional FireEye HX appliances as message sources.
10. To test communication with FireEye HX servers, select a server, and select **Test**. After viewing the test results, select **Close**.
11. In the FireEye HX pane, select **Apply**. A CounterACT Enterprise Manager Console dialog box opens.
12. Select **Yes** to save the plugin configuration, and then select **Close**.

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

- **Last Threat Report Time.** Indicates the latest date/time when CounterACT received a threat alert from this FireEye HX appliance.
- **Receiving CounterACT Appliance.** The IP address of the connecting CounterACT device that received the last threat notification from this FireEye HX appliance. This is one of the CounterACT devices defined as rsyslog targets at the FireEye HX appliance. See [Configure FireEye HX](#).

## Configure Additional FireEye HX Server Details

The server prefix (HTTP/HTTPS) and the port number are configurable via an install.properties file that comes with the plugin.

### To configure additional server details:

1. Log in to the connecting CounterACT device as root.

2. Access the **Install.Properties** file in the folder where the plugin is installed.
3. To change the server prefix, edit the property **config.rest\_api\_prefix.value** with one of the following values:
  - (1) http
  - (2) https
4. To change the port value, edit the **config.rest\_api\_port.value** property with a positive integer value. The default value is 3000.

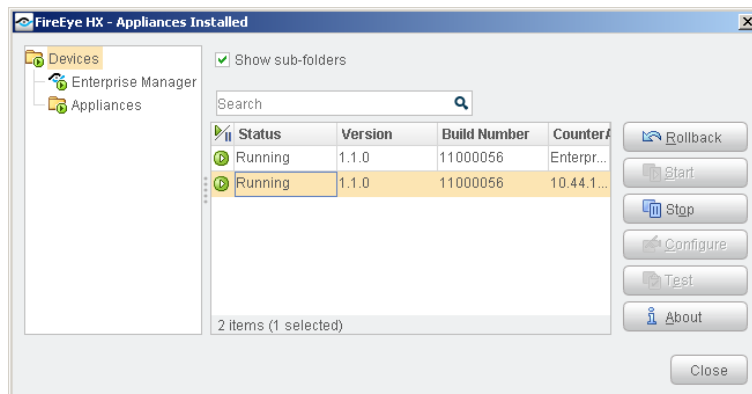
## Restarting the Plugin - Traffic Throttling

Typically, the plugin is started and runs after installation. During operation, the plugin may suspend some functions if the volume of threat notifications from FireEye HX exceeds an internal threshold. In this case it is necessary to restart the plugin.

FireEye HX lets administrators customize threat criteria. This can potentially cause relatively common actions or events to be classified as threats - resulting in a large volume of threats reported to CounterACT. A throttling function limits the number of threats that FireEye HX can report to CounterACT: after CounterACT receives 100 threat notifications within 600 seconds (10 minutes), the plugin ceases to report notifications to the IOC Scanner plugin, and an event is written to the plugin log file.

### To restart the plugin after a traffic throttling event:

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, double-click **FireEye HX**. The Appliances Installed dialog opens.



4. Select the communicating appliance. Select **Stop** and select **Yes** to confirm the action. CounterACT stops the plugin on the device.
5. With the communicating device still selected, select **Start** and select **Yes** to confirm the action. CounterACT starts the plugin on the device.

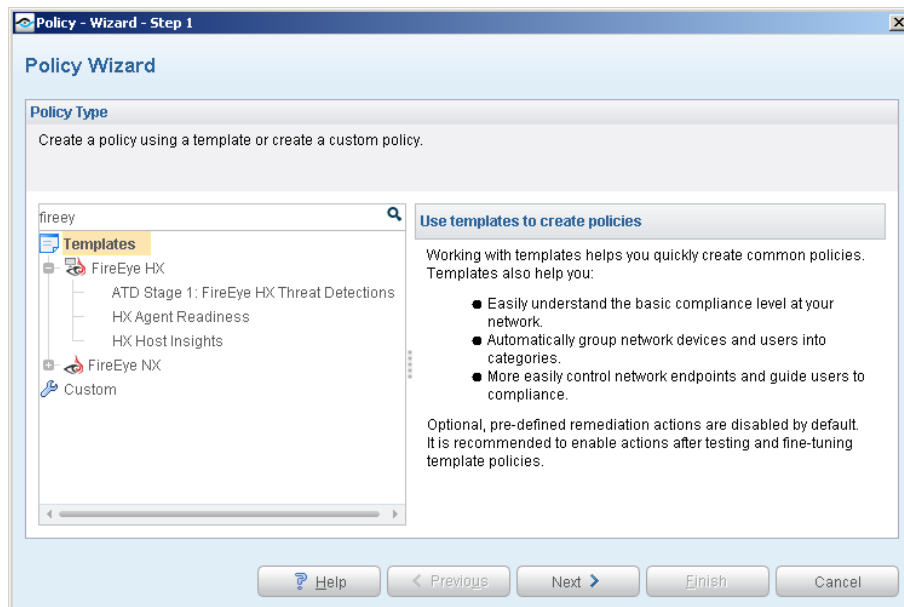
## Run FireEye HX Policy Templates

CounterACT templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

The following templates are available for detecting and managing endpoints:

- [ATD Stage 1: FireEye HX Threat Detections Policy Template](#)
- [HX Agent Readiness Policy Template](#)
- [HX Host Insights Policy Template](#)



### ATD Stage 1: FireEye HX Threat Detections Policy Template

Use this template to create a CounterACT policy that responds to threats detected by FireEye HX and reported to CounterACT. You can define different responses to threats based on their severity as reported by FireEye HX.

#### To use the HX Threat Detections policy 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 HX** folder and select **ATD Stage 1: FireEye HX Threat Detections**. The ATD Stage 1: FireEye HX Threat Detections pane opens.
4. Select **Next**. The Name pane opens.

## Name the Policy

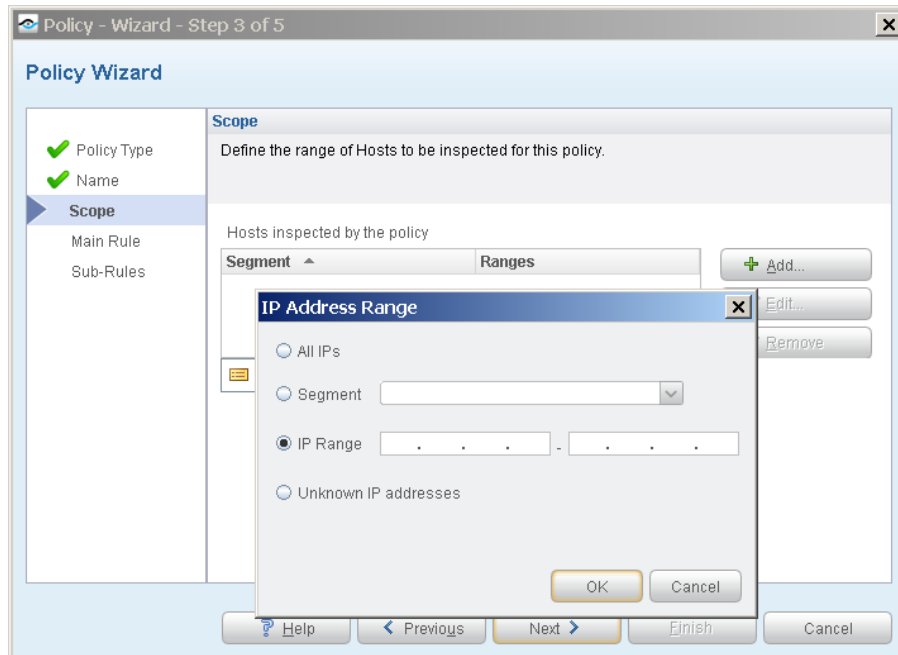
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.




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



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

### How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.



Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

### Main Rule

The main rule of this policy detects all threat detections reported to CounterACT in the last week.

**10.** Select **Next**. The Sub-Rules pane opens.

### Sub-Rules

The sub-rules of this policy detect threats based on their reported severity.

- For threats with *Critical* severity:



An optional **Send Message to Syslog** action to send a notification.



An optional **Switch Block** action is available.

By default, these actions are disabled.

- For threats with *High* severity:



An optional **Send Message to Syslog** action to send a notification.



An optional **Switch Block** action is available.

By default, these actions are disabled.

- For threats with *Medium* severity:



An optional **Send Message to Syslog** action to send a notification. By default, this action is disabled.

- For threats with *Low* severity:



An optional **Send Message to Syslog** action to send a notification. By default, this action is disabled.

**11.** Select **Finish** to create the policy.

**12.** On the CounterACT Console, select **Apply** to save the policy.

## HX Agent Readiness Policy Template

Use this template to create a CounterACT policy that detects Windows endpoints on which:

- The FireEye HX agent is not installed.
  - An optional action redirects users to a URL from which to install the agent. It is recommended that the URL be available from outside the corporate network to ensure that the user can access the FireEye HX agent installer. This action is disabled by default.

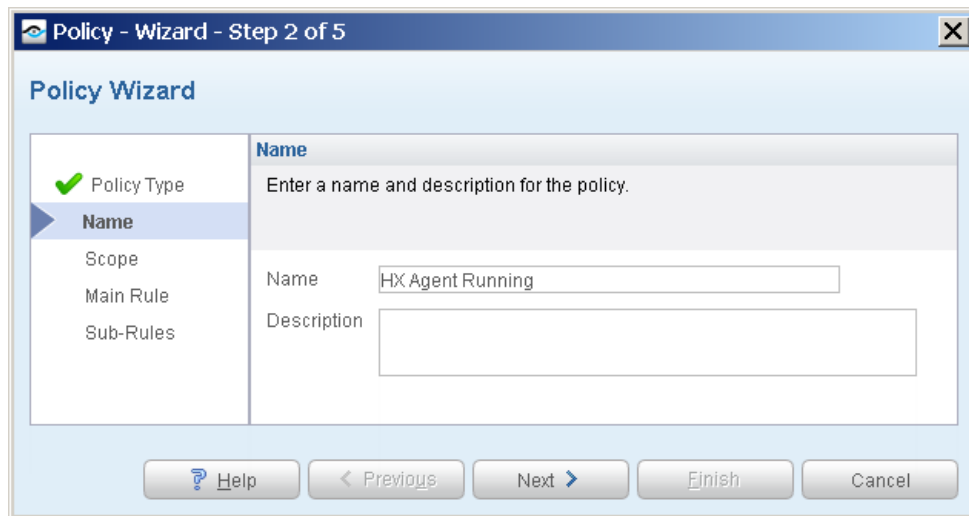
- The FireEye HX agent is installed but not running.
  - An optional remediation action runs a script to start the agent. This action is disabled by default.
- The FireEye HX agent is running but is not communicating with the defined FireEye HX server.
  - An optional action notifies the administrator by email that the FireEye HX agent is not communicating with the defined FireEye HX server. This action is disabled by default.

#### To use the HX Agent Readiness policy 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 HX** folder and select **HX Agent Readiness**. The **HX Agent Readiness** 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.

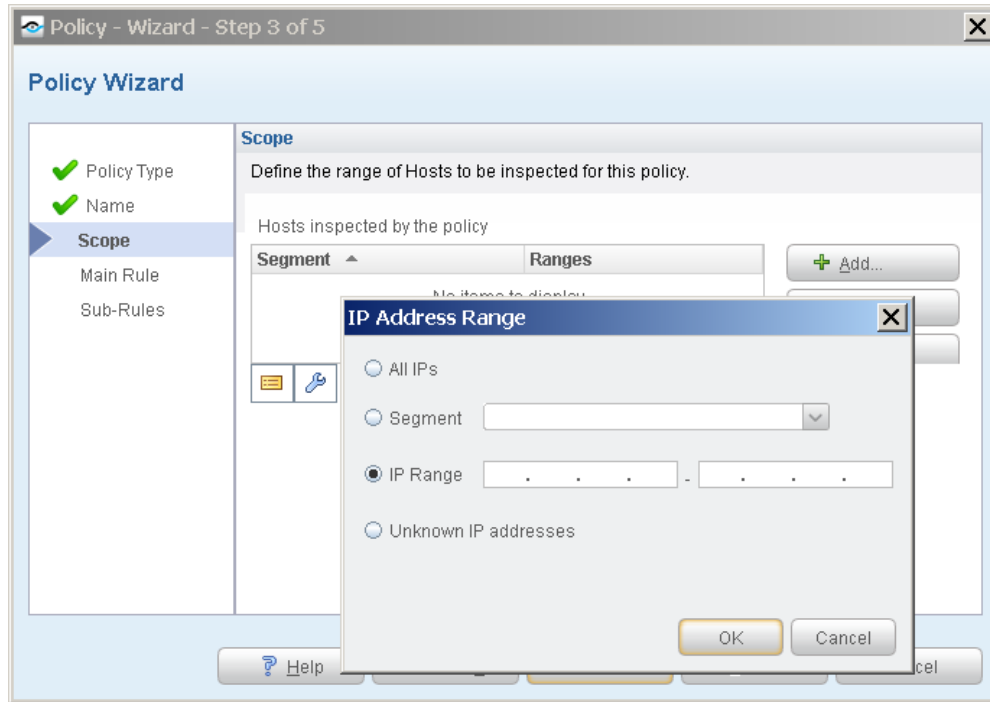


The screenshot shows a window titled "Policy - Wizard - Step 2 of 5". Inside, the "Policy Wizard" is displayed. On the left, a sidebar lists steps: "Policy Type" (with a green checkmark), "Name" (with a blue arrow), "Scope", "Main Rule", and "Sub-Rules". The main area is titled "Name" and contains the instruction "Enter a name and description for the policy." Below this, there is a text input field for "Name" containing the text "HX Agent Running" and a larger text area for "Description". At the bottom of the window, there are five buttons: "Help" (with a question mark icon), "Previous" (with a left arrow), "Next" (with a right arrow), "Finish", and "Cancel".


1. Define a unique name for the policy you are creating based on this template, and enter a description.
  - 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.
  - Use a name that indicates whether 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 Endpoints 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.

## How Endpoints Are Detected and Handled

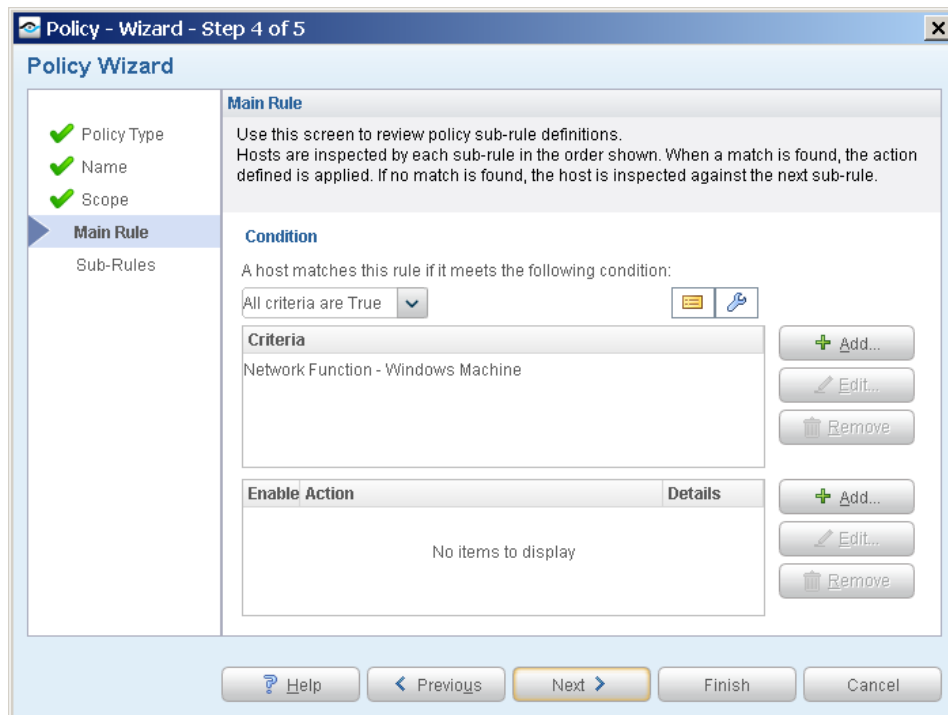
This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

## Main Rule

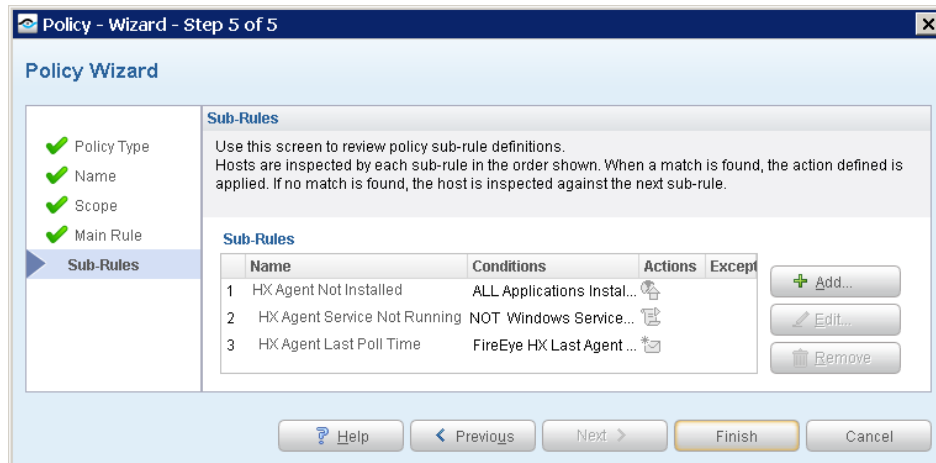
The main rule of this policy detects if the endpoint is a Windows machine. Non-Windows machines are not inspected by the sub-rules.



6. Select **Next**. The Sub-Rules pane opens.

## Sub-Rules

The sub-rules of this policy detect if the FireEye HX agent is installed and running on the endpoint, and if the agent has polled the FireEye HX server recently.



- If the FireEye HX agent is not installed, an optional remediation action can be used to direct users to a URL from which to install the agent. If you enable this action, open it for editing, and then enter the URL in the **Redirect to Site** field. It is recommended that the URL be available from outside the network.
  - If the FireEye HX agent is installed but not running, an optional remediation action runs a script to start the agent.
  - If the FireEye HX agent has not polled the FireEye HX server recently, an optional remediation action can be used to send an email notification. If you enable this action, open it for editing, and then enter the administrator email address in the **To** field.
7. Select **Finish** to create the policy.
  8. On the CounterACT Console, select **Apply** to save the policy.

## HX Host Insights Policy Template

Use this template to create a CounterACT policy that collects endpoint information using the FireEye HX agent.

### To use the HX Host Insights policy 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 HX** folder and select **HX Host Insights**. The **HX Host Insights** pane opens.
4. Select **Next**. The Name pane opens.

### Name the Policy

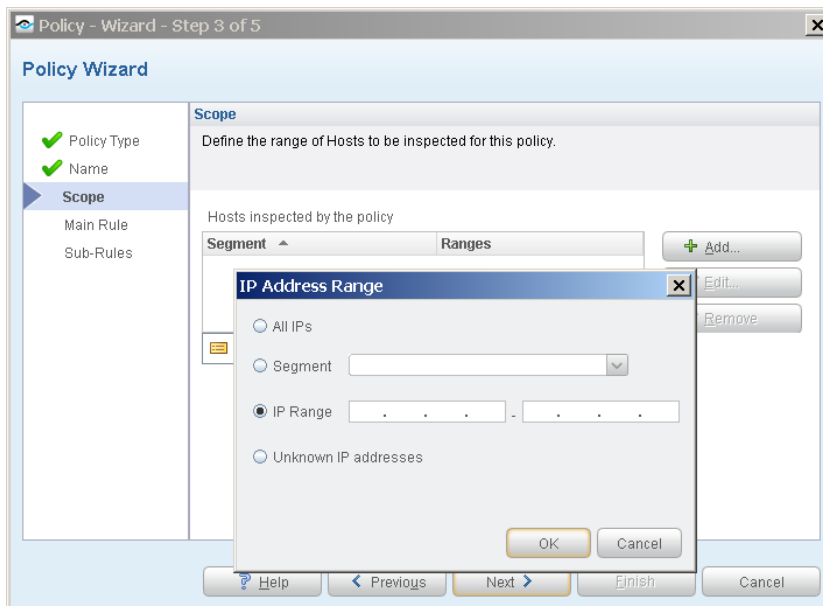
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.




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

### How Endpoints Are Detected and Handled

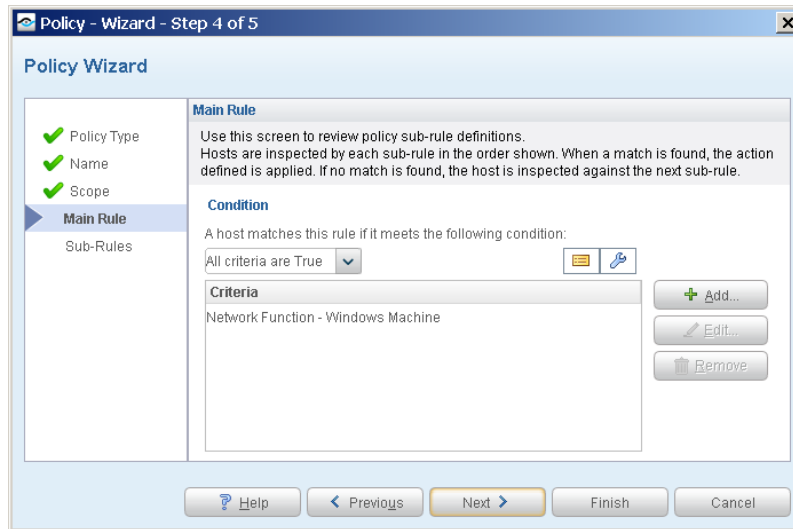
This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

### Main Rule

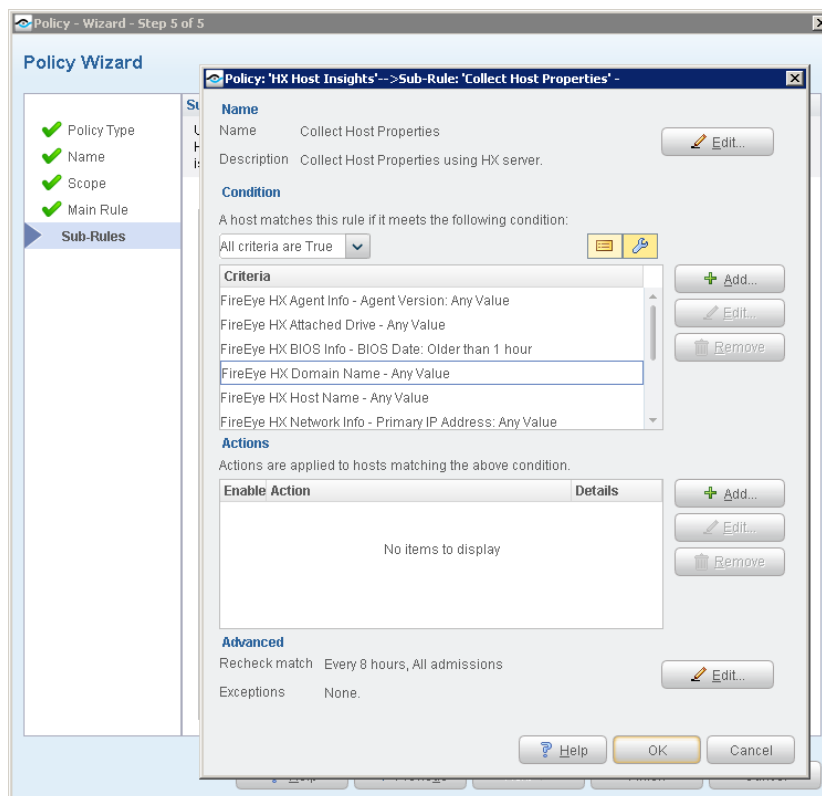
The main rule of this policy detects if the endpoint is a Windows machine. Non-Windows machines are not inspected by the sub-rules.



6. Select **Next**. The Sub-Rules pane opens.

### Sub-Rules

The sub-rules of this policy detect endpoints based on host properties provided by this plugin that report information retrieved from FireEye HX. See [FireEye HX – Policy Properties](#).



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



## Create Custom FireEye HX Policies

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

### Policies and Rules, Conditions and Actions

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

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

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

- Scan potentially compromised Windows endpoints for IOCs reported by the FireEye HX Plugin.
- Remediate infected endpoints.

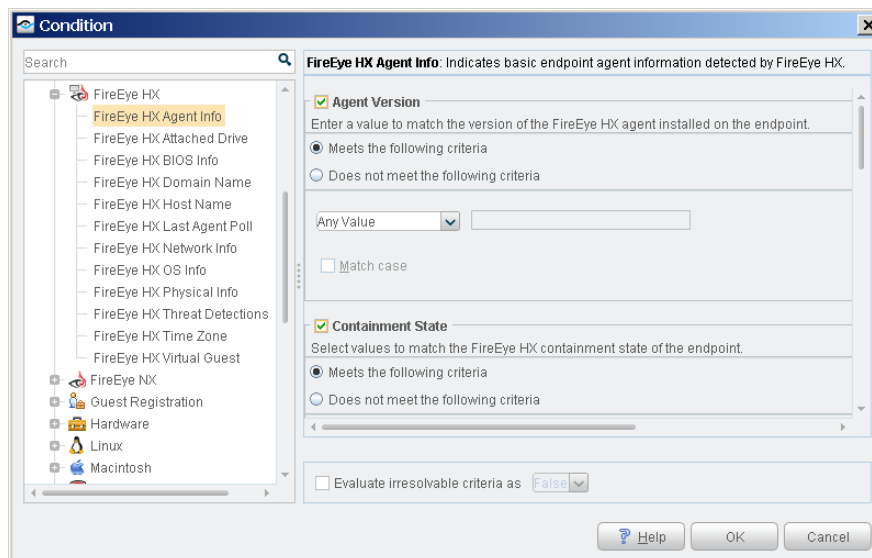
These items are available when you install the IOC Scanner Plugin.

#### To create a custom policy:

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

## FireEye HX – Policy Properties

This section describes the FireEye HX properties that are available when you install the FireEye HX Plugin.



**To access FireEye HX properties:**

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the FireEye HX folder in the Properties tree.

The following properties are available.

<b>FireEye HX Agent Info</b>	<p>Indicates basic endpoint agent information detected by FireEye HX. The endpoint agent information detected is:</p> <ul style="list-style-type: none"> <li>▪ Agent Version</li> <li>▪ Containment State</li> <li>▪ Agent ID</li> <li>▪ Agent Status</li> </ul>
<b>FireEye HX Attached Drive</b>	<p>Indicates the drive letter of an attached drive that the FireEye HX agent detected on the endpoint.</p> <p>A Track Changes property indicates changes in the value(s) of this field.</p>
<b>FireEye HX BIOS Info</b>	<p>Indicates host information that the FireEye HX agent detected on the endpoint. The information detected is:</p> <ul style="list-style-type: none"> <li>▪ BIOS Date</li> <li>▪ BIOS Version</li> <li>▪ BIOS Type. Possible values are: <ul style="list-style-type: none"> <li>▪ BIOS: The FireEye HX Agent reports that Windows is running with a BIOS-type firmware interface.</li> <li>▪ UEFI: The FireEye HX Agent reports that Windows is running with a UEFI-type firmware interface. If a UEFI firmware is configured to run in BIOS-compatibility mode, the BIOS Type is reported as BIOS and not UEFI.</li> <li>▪ Unknown: The FireEye HX Agent cannot determine the BIOS type firmware interface.</li> </ul> </li> </ul> <p>A Track Changes property indicates changes in the value(s) of this field.</p>
<b>FireEye HX Domain Name</b>	<p>Indicates the domain name that the FireEye HX agent detected on the endpoint.</p> <p>A Track Changes property indicates changes in the value(s) of this field.</p>
<b>FireEye HX Host Name</b>	<p>Indicates the host name that the FireEye HX agent detected. A Track Changes property is defined for this property.</p>
<b>FireEye HX Last Agent Poll</b>	<p>Indicates the last time the FireEye HX agent on the endpoint connected to the HX server.</p>
<b>FireEye HX Network Info</b>	<p>Indicates network information that the FireEye HX agent detected on the endpoint. The endpoint information detected is:</p> <ul style="list-style-type: none"> <li>▪ Primary IP Address</li> <li>▪ MAC Address</li> <li>▪ IPv6 Address</li> <li>▪ DHCP Server</li> <li>▪ IP Gateway</li> </ul> <p>A Track Changes property indicates changes in the value(s) of this field.</p>

<b>FireEye HX OS Info</b>	Indicates operating system information that the FireEye HX agent detected on the endpoint. The operating system information detected is: <ul style="list-style-type: none"> <li>Product Name</li> <li>Patch Level</li> <li>Bitness</li> <li>OS Date</li> </ul>
<b>FireEye HX Physical Info</b>	Indicates basic endpoint physical information detected by FireEye HX. The physical information detected is: <ul style="list-style-type: none"> <li>Processor</li> <li>Physical Memory</li> <li>Available Memory</li> </ul>
<b>FireEye HX Threat Detections</b>	Indicates threats that FireEye HX detected on the endpoint. You can use this property in CounterACT policies to immediately remediate a threat detected by FireEye HX. For example, create a policy that detects if FireEye HX has detected a Critical severity threat, and trigger remediation when an endpoint meets this condition. The threat information detected is: <ul style="list-style-type: none"> <li>Threat Severity</li> <li>Threat Name</li> <li>Threat File Name</li> <li>Threat File Hash</li> <li>Threat Hash Type</li> </ul>
<b>FireEye HX Time Zone</b>	Indicates the time zone that the FireEye HX agent detected on the endpoint. A Track Changes property indicates changes in the value(s) of this field.
<b>FireEye HX Virtual Guest</b>	Indicates if the FireEye HX agent detected a virtual guest operating system running on the endpoint. A Track Changes property indicates changes in the value(s) of this field.

### Related IOC Scanner Plugin Properties

In addition to the properties provided by this plugin, the IOC Scanner Plugin provides the **IOCs Detected by CounterACT** property, which contains data from threats detected by this plugin. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for property details.

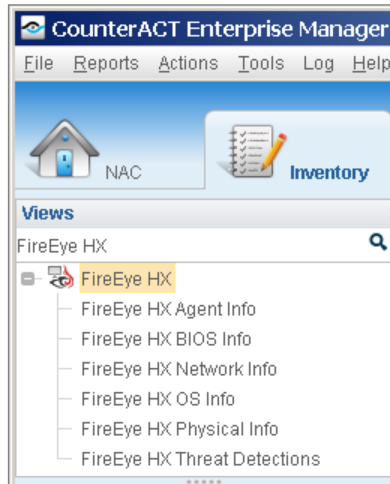
## Display Inventory Data

Use the CounterACT Inventory to view a real-time display of vulnerabilities detected by FireEye HX. The inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoint information reported by the FireEye HX agent.
- View endpoints that have been detected with specific threats.
- Easily track FireEye HX threat detection activity.
- Incorporate inventory detections into policies.

**To access the inventory:**

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to **FireEye HX** folder.



The following information, based on the FireEye HX properties, is available:

- FireEye HX Agent Info
- FireEye HX BIOS Info
- FireEye HX Network Info

*For the FireEye HX Network Info Inventory view, the FireEye HX agent reports on both IPv4 and IPv6 network interfaces. When the agent reports on IPv6 interfaces, no value is reported for the Primary IP Address field. You can use the Last Host field to identify IPv4 and IPv6 network interfaces associated with a single endpoint.*

- FireEye HX OS Info
- FireEye HX Physical Info
- FireEye HX Threat Detections

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.

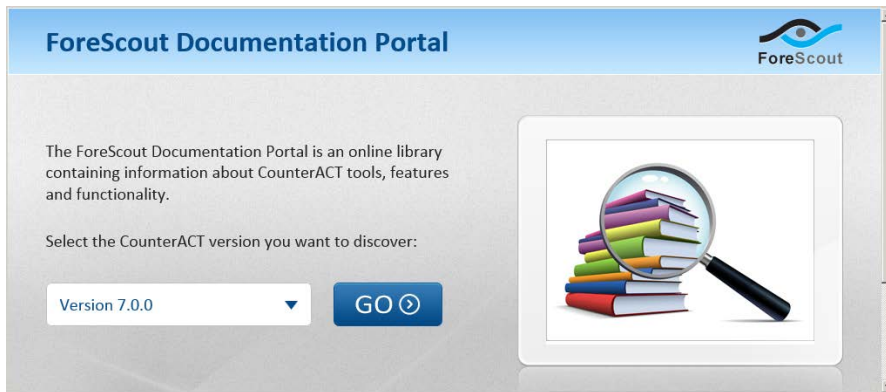
## Additional CounterACT Documentation

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](http://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

Copyright © ForeScout Technologies, Inc. 2000-2016. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by 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 an Early Availability Product, the terms applicable to your use of such product are set forth at: <http://www.forescout.com/early-availability-agreement/>.
  - 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](mailto:documentation@forescout.com)

2016-08-18 16:57