ForeScout® Extended Module for FireEye® HX

Configuration Guide

Version 1.2

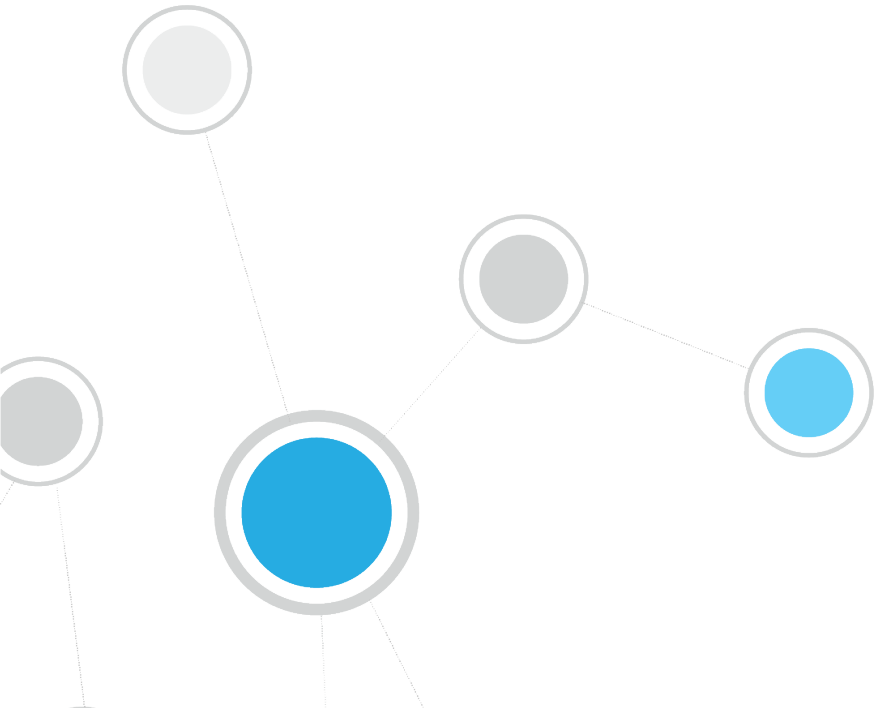


Table of Contents

About the FireEye HX Integration 3
Advanced Threat Detection with the IOC Scanner Plugin 3
Use Cases 4
Additional FireEye HX Documentation 5

About This Module 6
How It Works 7
What to Do 7

Requirements 7
CounterACT Software Requirements 8
FireEye HX Requirements 8
About Support for Dual Stack Environments 8

ForeScout Extended Module License Requirements 8
Per-Appliance Licensing Mode 9
Centralized Licensing Mode 10
More License Information 11

Configure FireEye HX 11

Install the Module 11

Configure the Module 13
Configure Additional FireEye HX Server Details 15
Restarting the Module - Traffic Throttling 15

Run FireEye HX Policy Templates 16
ATD Stage 1: FireEye HX Threat Detections Policy Template 17
HX Agent Readiness Policy Template 20
HX Host Insights Policy Template 23

Create Custom FireEye HX Policies 27
FireEye HX – Policy Properties 28

Display Inventory Data 30

Core Extensions Module Information 31

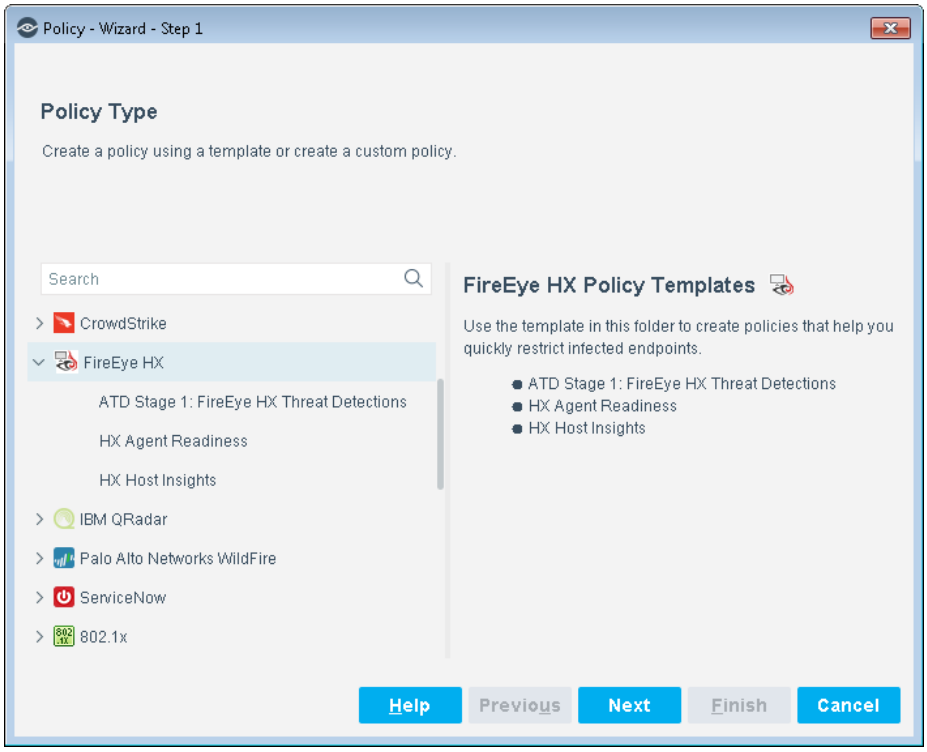
Additional CounterACT Documentation 33
Documentation Downloads 33
Documentation Portal 33
CounterACT Help Tools 34

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 ForeScout 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 module 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 module): Detect and report threats on endpoints:*** FireEye HX instances in your environment report threats to this module as they are detected on endpoints. Use the template provided with this module 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 module 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 *CounterACT IOC Scanner Plugin Configuration Guide*.

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.

Evaluate Endpoint Readiness

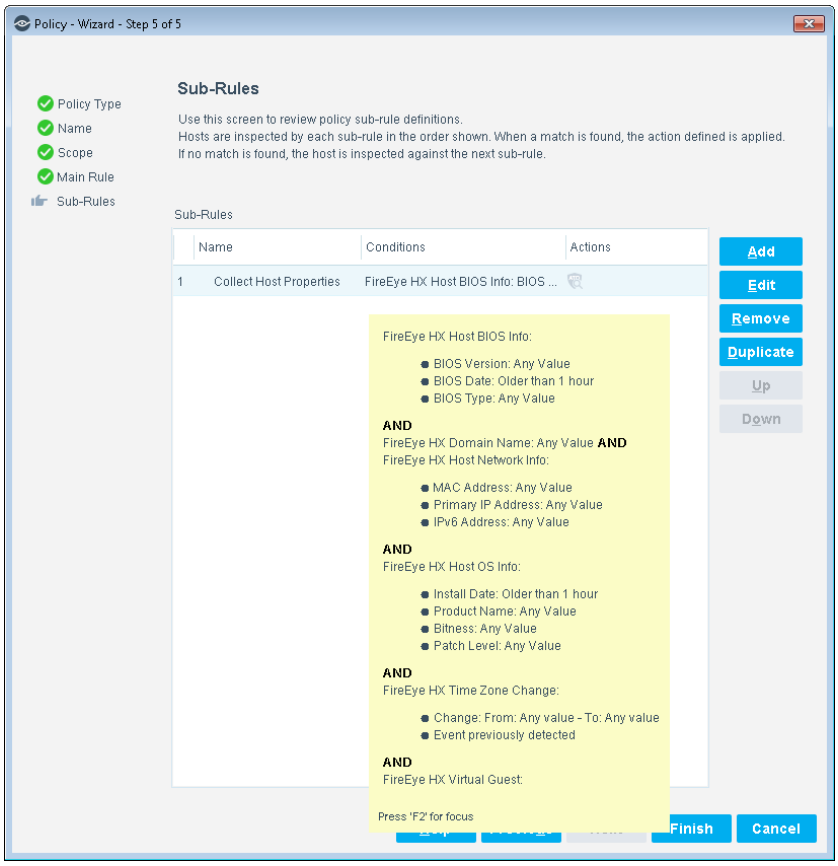
Use the HX Agent Readiness template to create a CounterACT policy that:

- 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. An 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 Module

This module allows 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 module, 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 module, 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 module 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 Module 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 module:

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

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- FireEye HX Requirements
- ForeScout Extended Module License Requirements
- Core Extensions Module Information

CounterACT Software Requirements

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

- CounterACT version 8.0
- Core Extensions Module 1.0 with the following components running:
  - Syslog Plugin
  - IOC Scanner Plugin

FireEye HX Requirements

The module requires the following FireEye HX components:

- FireEye Endpoint Security (HX Series) version 3.0.x, 3.1.x, or 4.0.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

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this component.*** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

ForeScout Extended Module License Requirements

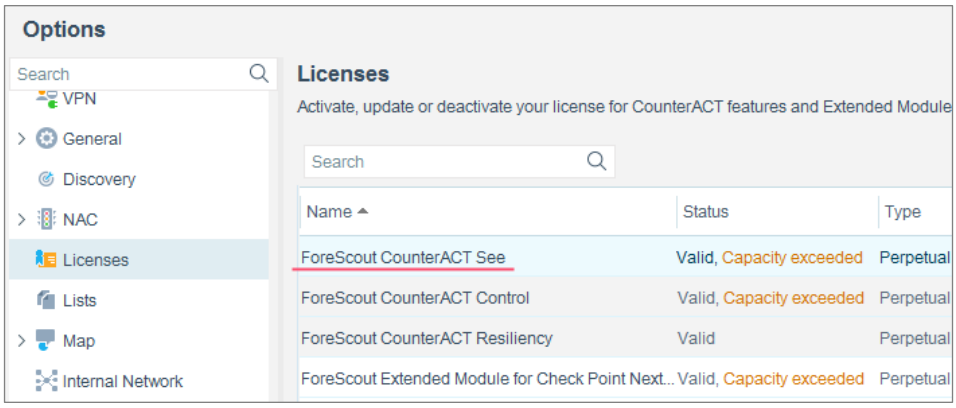
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

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.

> *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 Administration Guide for more information.*

Requesting a License

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

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

To view the number of currently detected devices:

1. Select the **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.

Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout representative.

No demo license is automatically installed during system installation.

License entitlements are managed in the ForeScout Customer Portal. After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

Integration Modules, which package together groups of related licensed modules, are not supported when operating in Centralized Licensing Mode. Only Extended Modules, packaging individual licensed modules are supported. The Open Integration Module is an Extended Module even though it packages more than one module.

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

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 Module

This section describes how to install the module. Before you install this module, first install the IOC Scanner Plugin. See CounterACT Software Requirements.

To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **`.fpi`** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

   The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

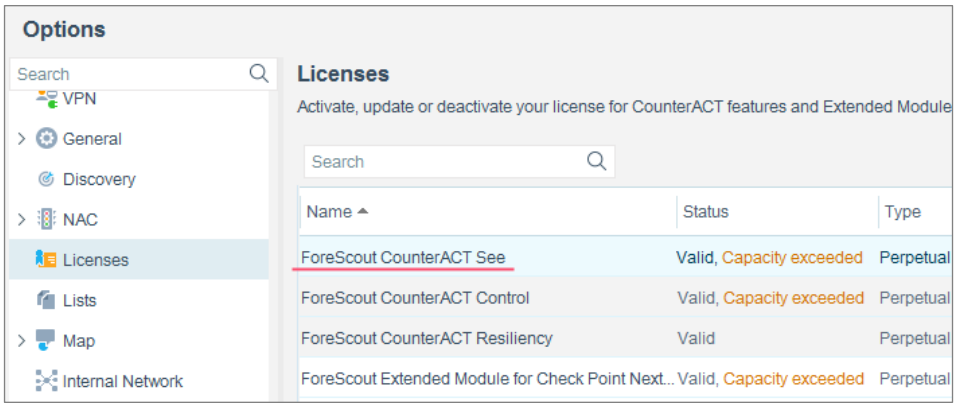
   In modules that contain more than one component, the installation proceeds automatically one component at a time.
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



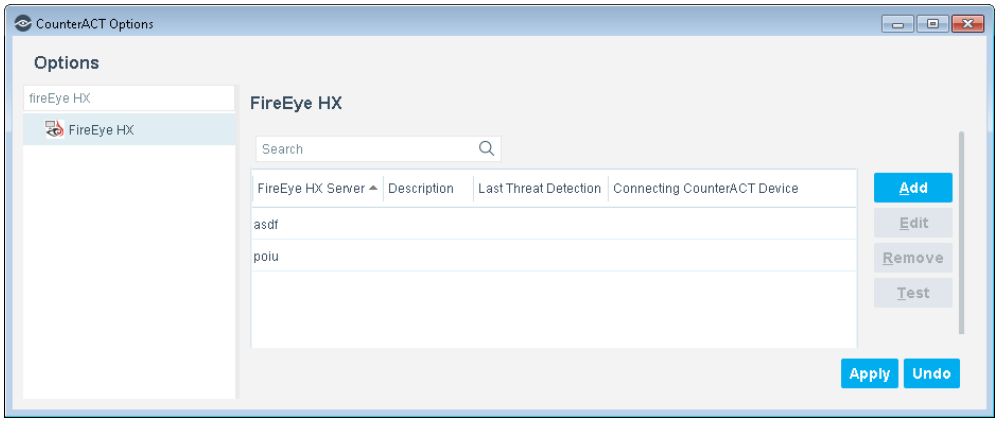
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

Configure the module to ensure that CounterACT can communicate with the FireEye HX 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 **Modules** folder.
3. In the **Modules** pane, select **FireEye HX**, and select **Configure**. The FireEye HX pane opens.



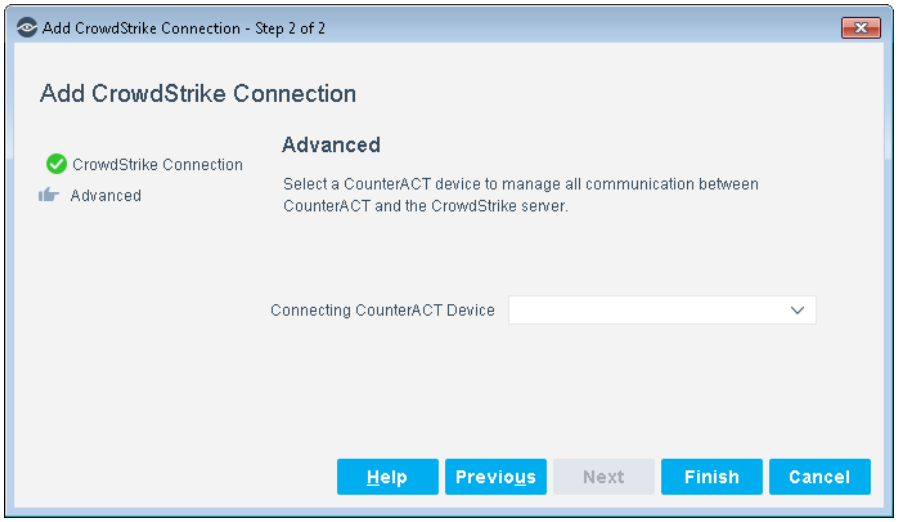
4. Select **Add** to define a FireEye HX server to communicate with CounterACT. The Add FireEye HX Server dialog box opens.

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 module. 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 module 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 module.

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 module 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.

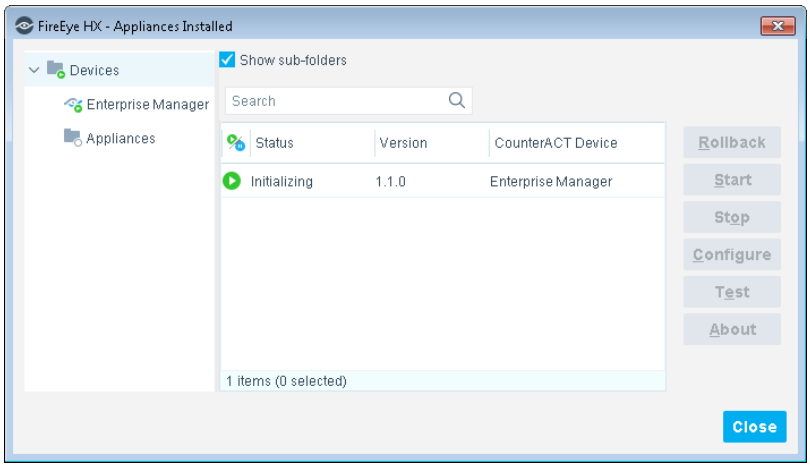
Restarting the Module - Traffic Throttling

Typically, the module is started and runs after installation. During operation, the module 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 module.

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 module ceases to report notifications to the IOC Scanner Plugin, and an event is written to the module log file.

To restart the module 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 **Modules** folder.
3. In the **Modules** 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 module on the device.
5. With the communicating device still selected, select **Start** and select **Yes** to confirm the action. CounterACT starts the module on the device.

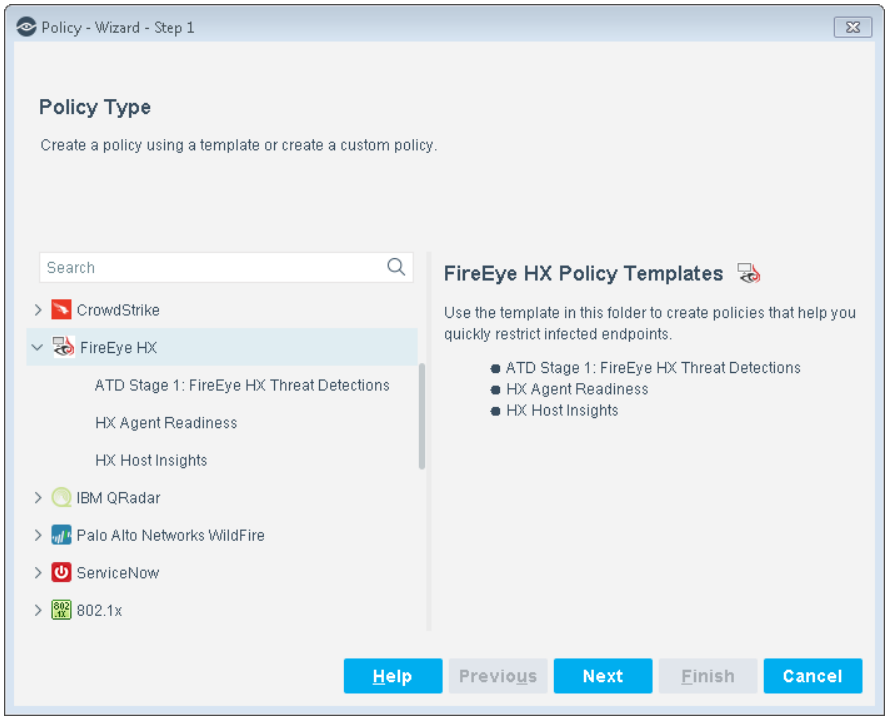
Run FireEye HX Policy Templates

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

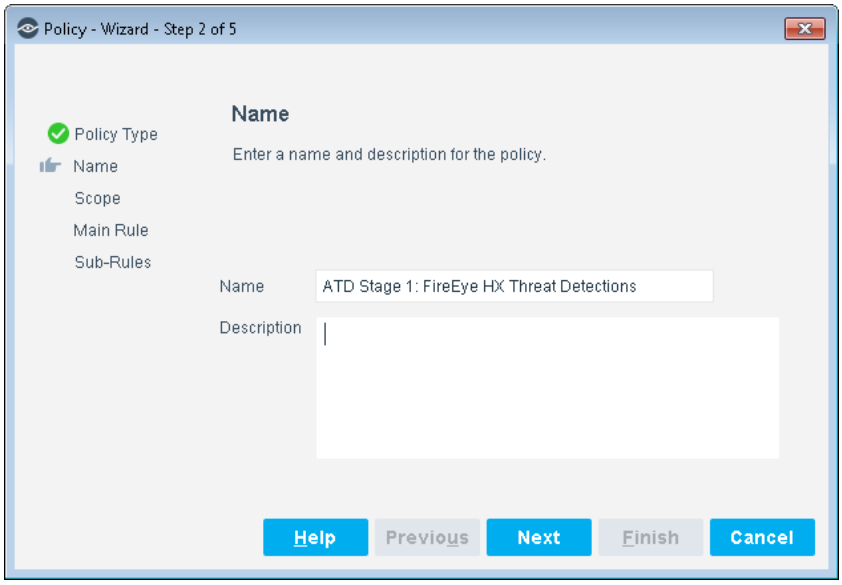
Use this template to create a CounterACT policy that responds to threats detected by FireEye HX and reported to CounterACT. You can define different responses to threats based on their severity as reported by FireEye HX.

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

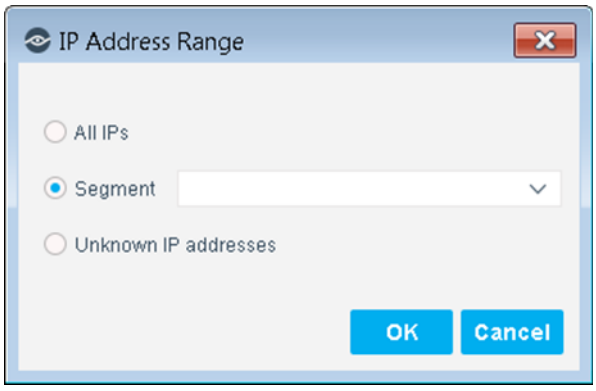
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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

7. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.

- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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:

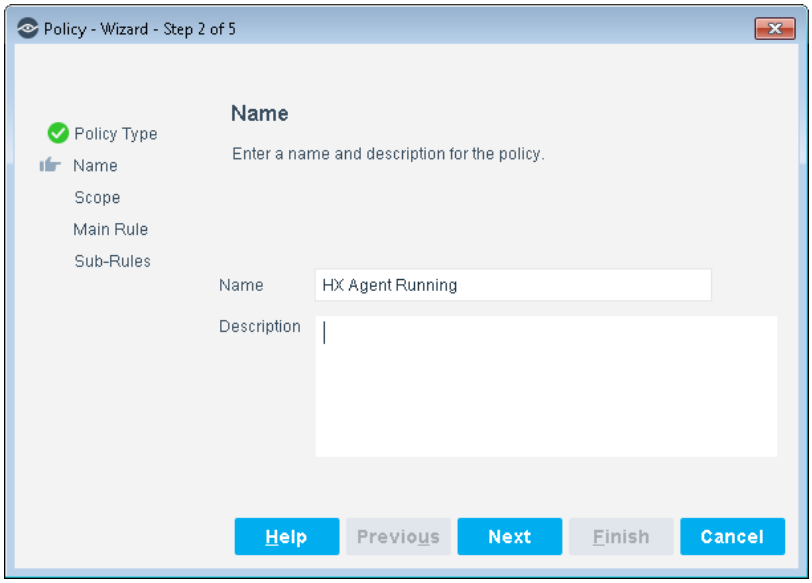
- The FireEye HX agent is not installed.
  - An optional action redirects users to a URL from which to install the agent. It is recommended that the URL be available from outside the corporate network to ensure that the user can access the FireEye HX agent installer. This action is disabled by default.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

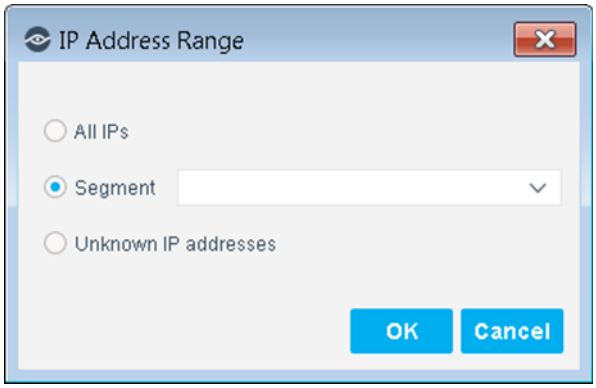
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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.
   - Use a name that indicates whether 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

7. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.

- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

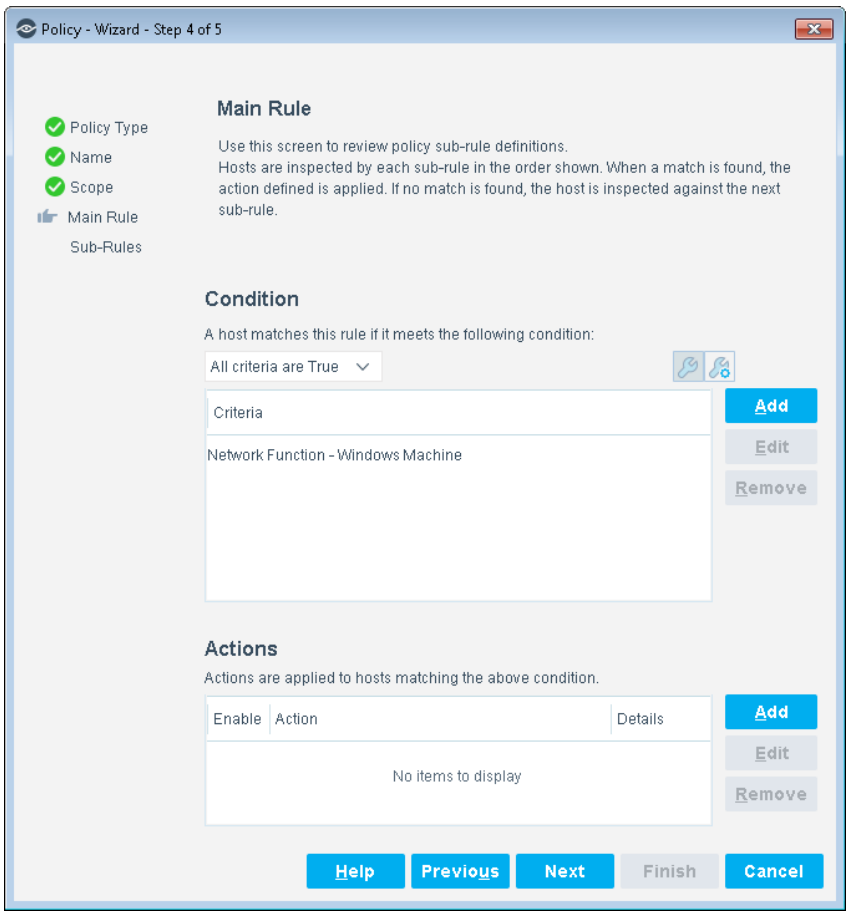
This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

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

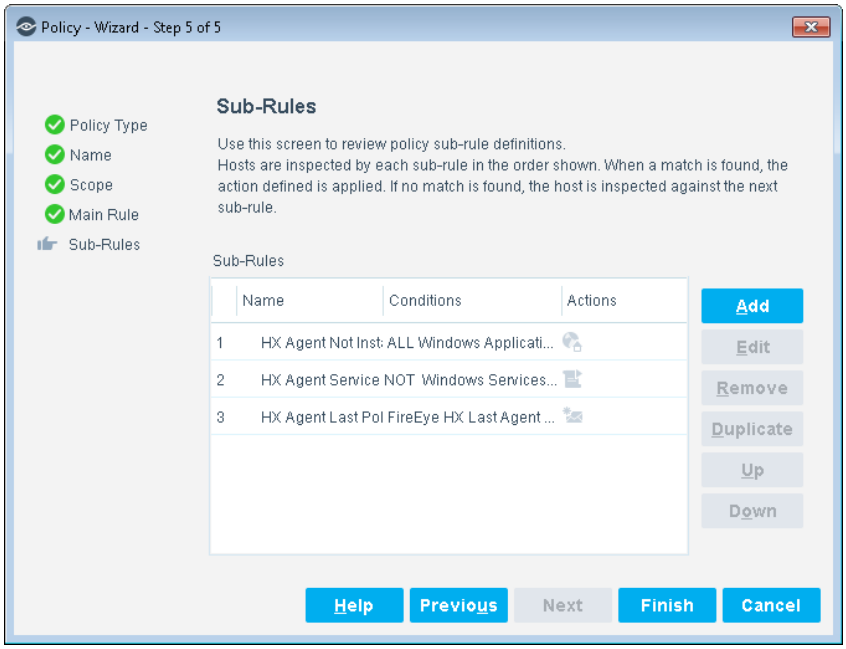
The main rule of this policy detects if the endpoint is a Windows machine. Non-Windows machines are not inspected by the sub-rules.



10. 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.

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

12. 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.

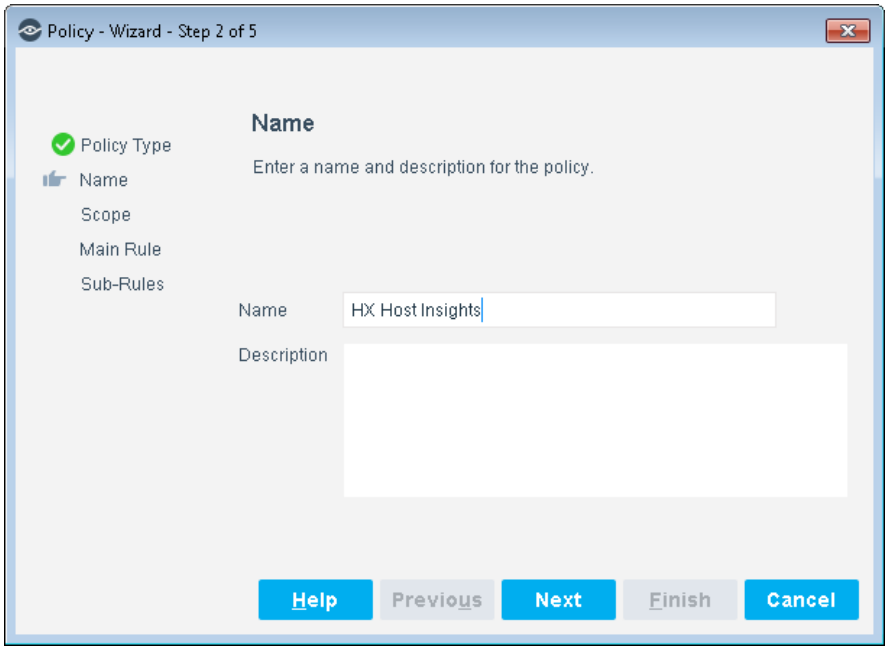
To use the HX Host Insights policy template:

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

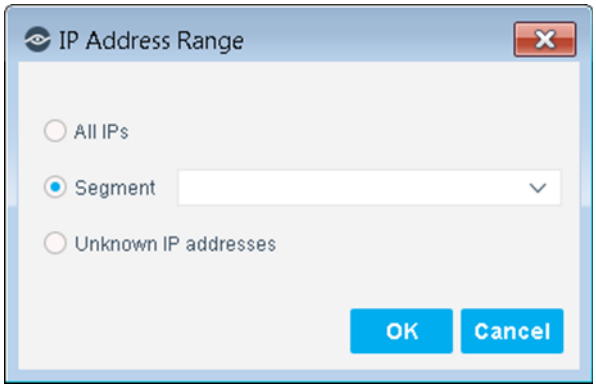
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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

7. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

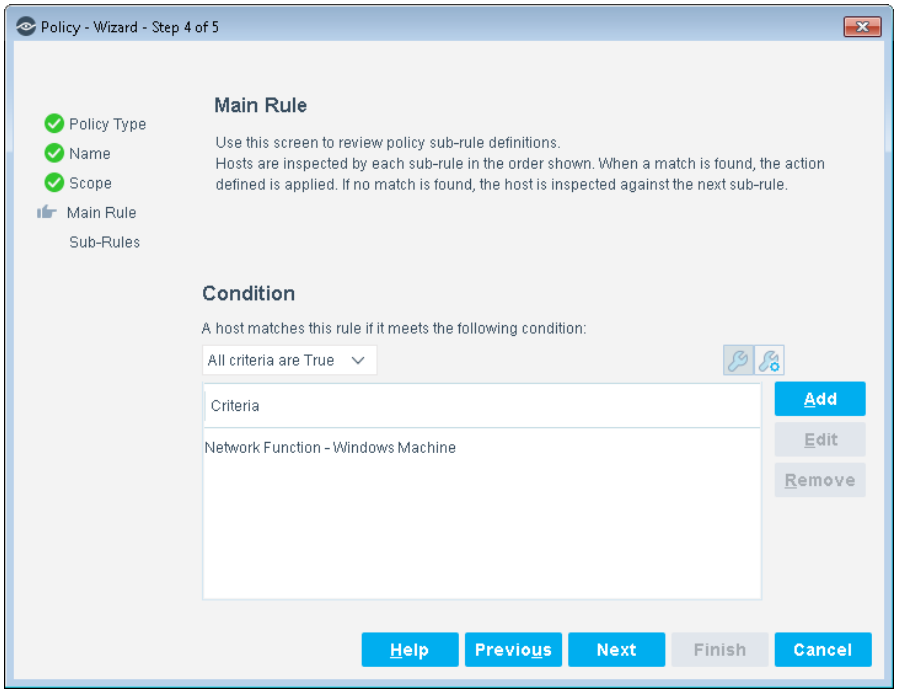
This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

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

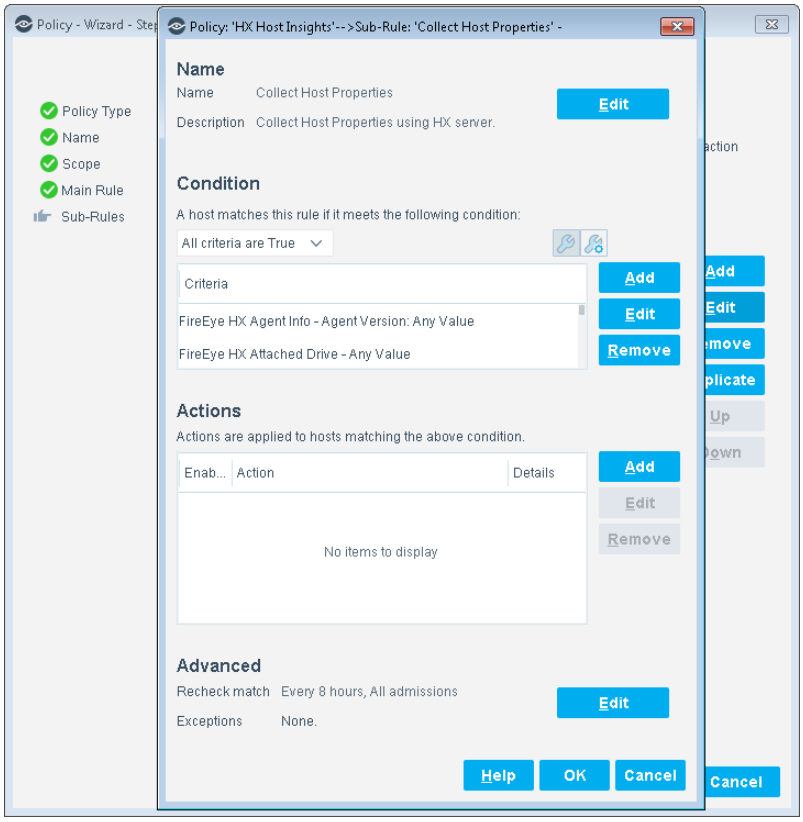
The main rule of this policy detects if the endpoint is a Windows machine. Non-Windows machines are not inspected by the sub-rules.



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

Sub-Rules

The sub-rules of this policy detect endpoints based on host properties provided by this module that report information retrieved from FireEye HX. See FireEye HX – Policy Properties.



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

12. 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 Module.
- Remediate infected endpoints.

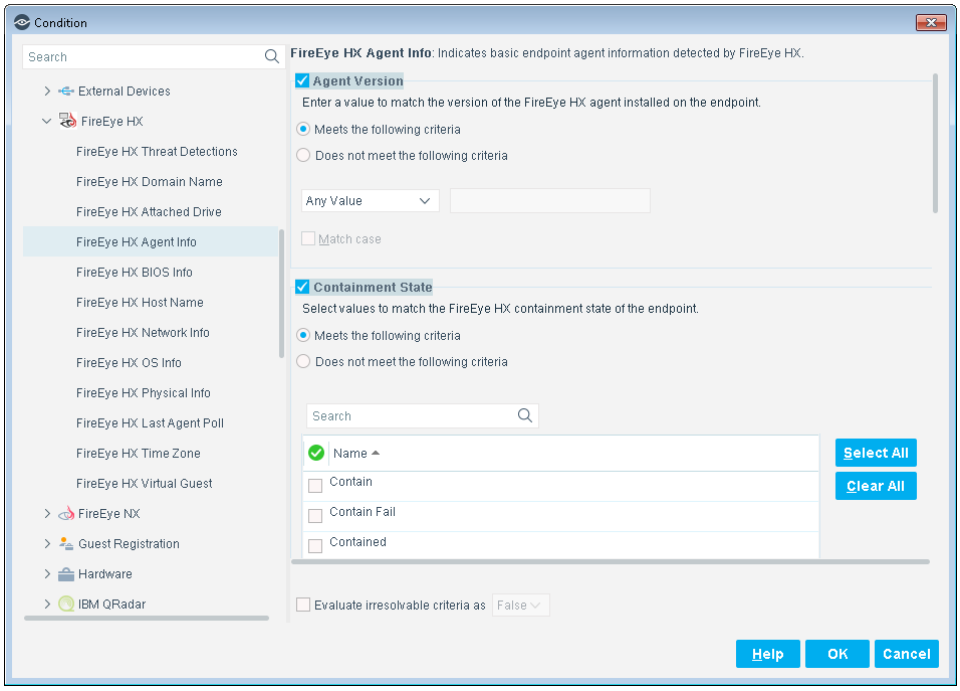
These items are available when you install the IOC Scanner Plugin.

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 Module.



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.

FireEye HX Agent Info	Indicates basic endpoint agent information detected by FireEye HX. The endpoint agent information detected is: ▪ Agent Version ▪ Containment State ▪ Agent ID ▪ Agent Status
FireEye HX Attached Drive	Indicates the drive letter of an attached drive that the FireEye HX agent detected on the endpoint. A Track Changes property indicates changes in the value(s) of this field.

FireEye HX BIOS Info	Indicates host information that the FireEye HX agent detected on the endpoint. The information detected is: ▪ BIOS Date ▪ BIOS Version ▪ BIOS Type. Possible values are: ▪ BIOS: The FireEye HX Agent reports that Windows is running with a BIOS-type firmware interface. ▪ 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. ▪ Unknown: The FireEye HX Agent cannot determine the BIOS type firmware interface. A Track Changes property indicates changes in the value(s) of this field.
FireEye HX Domain Name	Indicates the domain name that the FireEye HX agent detected on the endpoint. A Track Changes property indicates changes in the value(s) of this field.
FireEye HX Host Name	Indicates the host name that the FireEye HX agent detected.A Track Changes property is defined for this property.
FireEye HX Last Agent Poll	Indicates the last time the FireEye HX agent on the endpoint connected to the HX server.
FireEye HX Network Info	Indicates network information that the FireEye HX agent detected on the endpoint. The endpoint information detected is: ▪ Primary IP Address ▪ MAC Address ▪ IPv6 Address ▪ DHCP Server ▪ IP Gateway A Track Changes property indicates changes in the value(s) of this field.
FireEye HX OS Info	Indicates operating system information that the FireEye HX agent detected on the endpoint. The operating system information detected is: ▪ Product Name ▪ Patch Level ▪ Bitness ▪ OS Date
FireEye HX Physical Info	Indicates basic endpoint physical information detected by FireEye HX. The physical information detected is: ▪ Processor ▪ Physical Memory ▪ Available Memory

FireEye HX Threat Detections	Indicates threats that FireEye HX detected on the endpoint. You can use this property in CounterACT policies to immediate 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: ▪ Threat Severity ▪ Threat Name ▪ Threat File Name ▪ Threat File Hash ▪ Threat Hash Type
FireEye HX Time Zone	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.
FireEye HX Virtual Guest	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 module, the IOC Scanner Plugin provides the **IOCs Detected by CounterACT** property, which contains data from threats detected by this module. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for property details.

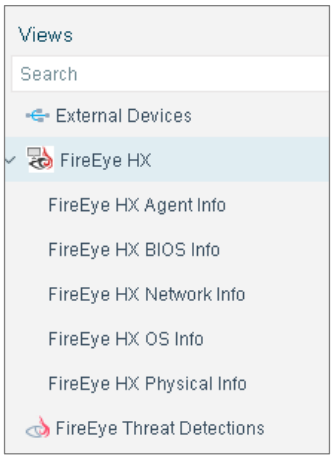
Display Inventory Data

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

1. Select the **Access 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 on the Console>Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT Asset Inventory.

Core Extensions Module Information

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

Advanced Tools Plugin	DNS Query Extension Plugin	NetFlow Plugin
CEF Plugin	External Classifier Plugin	Reports Plugin
Device Classification Engine	Flow Analyzer Plugin	Syslog Plugin
DHCP Classifier Plugin	IOC Scanner Plugin	Technical Support Plugin
DNS Client Plugin	IoT Posture Assessment Engine	Web GUI Plugin
DNS Enforce Plugin	NBT Scanner Plugin	

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are installed and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

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

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

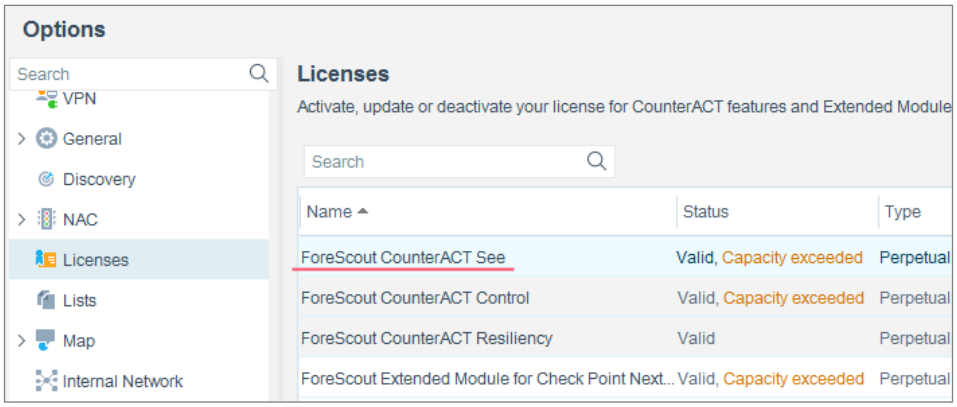
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-10 09:21