ForeScout® Extended Module for CrowdStrike®

Configuration Guide

Version 1.1

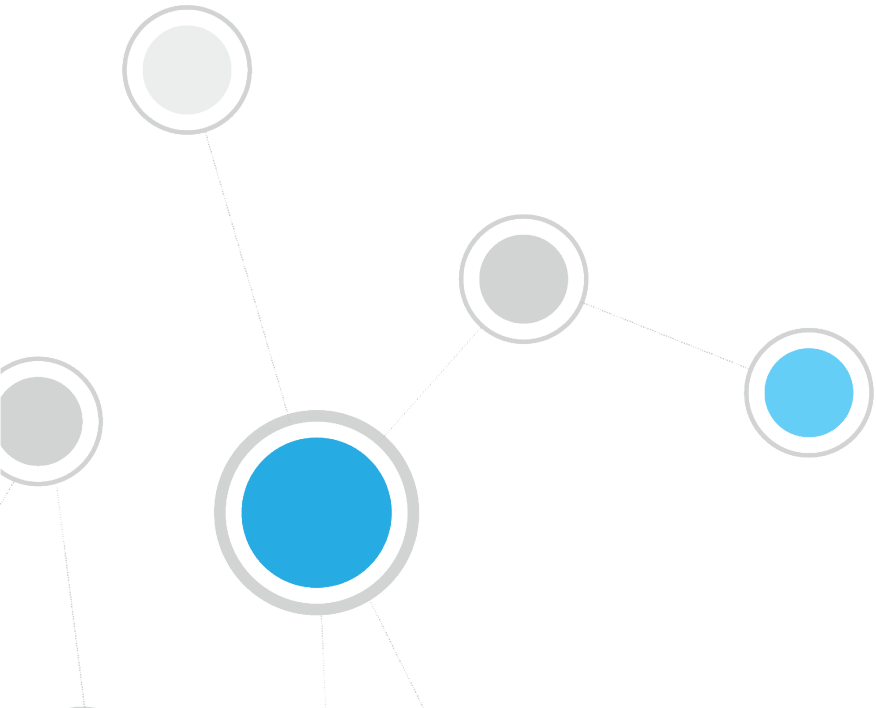


Table of Contents

About CrowdStrike Integration

ForeScout® CounterACT® is recognized as a leading network access control solution with continuous, agentless discovery of endpoint devices whether they are managed, unmanaged or otherwise unknown. CrowdStrike Falcon has revolutionized endpoint protection by unifying next-generation antivirus (NGAV) and endpoint detection and response (EDR). The ForeScout integration with CrowdStrike helps customers enforce compliance by assuring endpoints have the Falcon sensor and reduces the risk of having any unmanaged devices on their network. It also provides a means for distribution of endpoint management software which improves the user experience and increases operational efficiency.

The goal of this Module is to increase security protection across a wider device landscape that includes both traditional and non-traditional endpoints including BYOD and IoT. This is achieved through continuous device discovery/visibility, proactively hunting for threats across the device landscape and rapid remediation to prevent spread of threats and ensure endpoint compliance.

Fortify endpoint defenses, minimize security breaches and reduce your attack surface

- Gain visibility and control of devices across your network and beyond
- Verify the presence of functional CrowdStrike agent at the connection time and enroll devices with missing agents
- Monitor devices for Indicators of Attacks (IOAs) received from CrowdStrike and take actions to isolate, quarantine and remediate

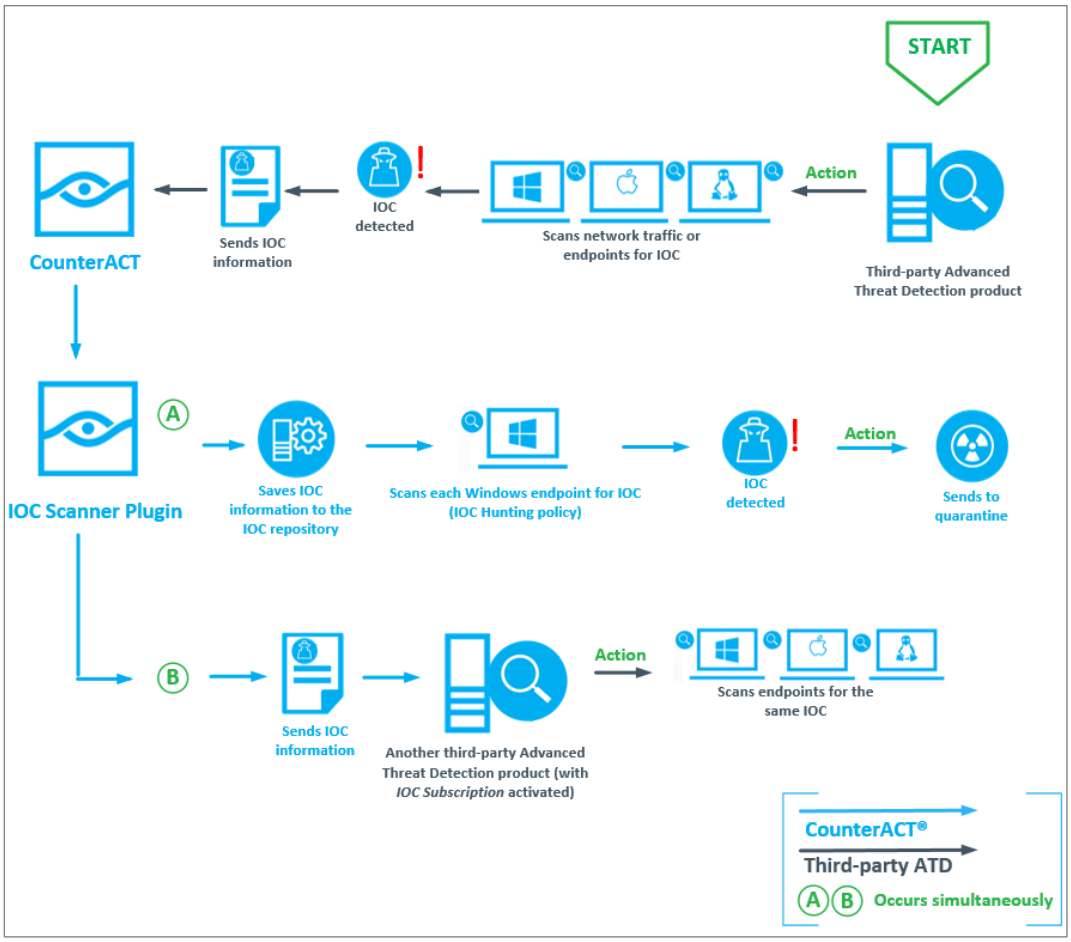
Provide combined automated response options to quarantine or remediate infected devices

Together, ForeScout and CrowdStrike protect customers by providing both broad and deep endpoint discovery, threat detection and remediation across a broader array of device types and networks. ForeScout will also help continually enforce device compliance upon network access. See Use Cases for more details.

Advanced Threat Detection with the IOC Scanner Module

This module works with the CounterACT IOC Scanner Plugin, an 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, 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 (CrowdStrike Module): Threat Hunting Policy Template:*** CrowdStrike 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 module, 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 Module uses these IOCs to mount further scan/analyze/remediate stages of CounterACT's ATD response, as follows:

- ***ATD Stage 2 (IOC Scanner Module): Real-time hunt for endpoints of interest based on threats and IOCs:*** The IOC Scanner Module detects endpoints with IOCs associated with recently reported threats.
- ***ATD Stage 3 (IOC Scanner Module): Evaluation and remediation:*** The IOC Scanner Module 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*.

About This Module

The CounterACT Extended Module for CrowdStrike supports CounterACT information sharing and interaction with components of the CrowdStrike cloud platform.

To use the module, you should have a solid understanding of CrowdStrike 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.

Use Cases

This section describes important use cases supported by this module.

CrowdStrike Falcon Agent Hygiene Policy

You can define a CounterACT policy that ensures the CrowdStrike Falcon agent is installed and functioning on all supported endpoints within the network. The module supports a set of host properties that detect CrowdStrike Falcon agent status on endpoints. Implement this use case with the CrowdStrike Agent Hygiene Policy Template.

Policy-Based Response to IoA from CrowdStrike

When CrowdStrike identifies malware or other malicious behavior known as Indicators of Attack (IoA), CounterACT is notified in near real-time and performs an action based on the risk level of the issue discovered. Implement this use case with the CrowdStrike Endpoint Threat Hunting Policy Template.

Restricting Compromised Endpoints Not Managed by CounterACT

CounterACT can restrict network access to non-corporate or other unmanaged endpoints based on IOCs reported to it by CrowdStrike. Implement this use case with the CrowdStrike Endpoint Threat Hunting Policy Template or other policies provided by the IOC Scanner Module.

How it Works

The following CrowdStrike components are required for this integrated solution:

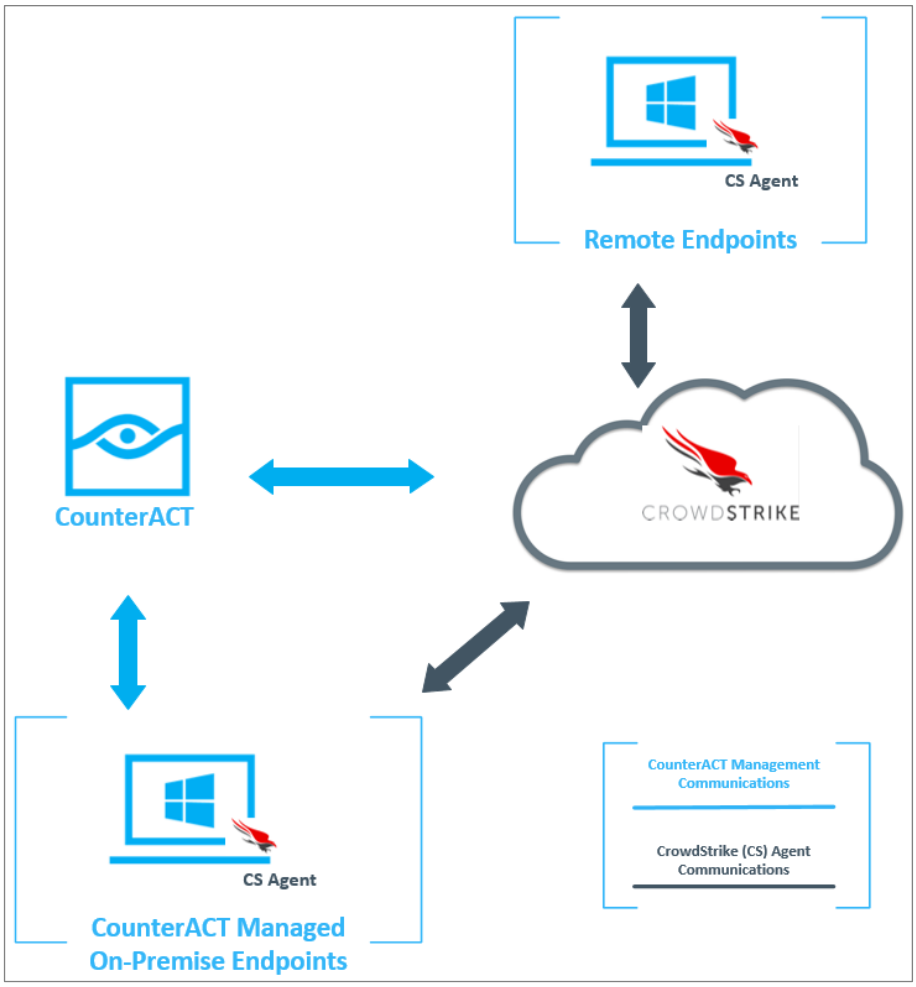
- ***CrowdStrike Cloud platform*** - CounterACT addresses the query API exposed by the platform to retrieve endpoint information.
- ***CrowdStrike Streaming API*** - CounterACT subscribes to CrowdStrike IOC and IoT streams.
- ***CrowdStrike Query API*** - Allows you to create custom indicators of compromise (IOCs), query and search for devices in your environment based on device properties, obtain information about indicators that ran in your environment, obtain details for processes that are running or that previously ran, and set the status of threat detections in Falcon Host.

The following CounterACT Components support the integration:

- ***ForeScout Extended Module for CrowdStrike*** - This module handles communication with CrowdStrike and provides the properties, actions, and policies described in this guide.
- ***CounterACT IOC Scanner Plugin*** - This plugin is the clearinghouse for IOC information and related functionality in CounterACT. When the Extended Module for CrowdStrike is installed, CrowdStrike cloud instances can be subscribed to IOC streams from the IOC Scanner Plugin. See Configure CrowdStrike as an IOC Subscriber.

In a typical deployment, several CrowdStrike cloud connections are defined in CounterACT. Connections to the cloud may be planned based on anticipated traffic or geographic location.

- A single CounterACT device connects to each cloud access point, handling communication for a cluster of CounterACT devices. CounterACT devices in the cluster only work with that CrowdStrike cloud instance.
- For each connection, the rate of messaging from CounterACT to the CrowdStrike cloud can be configured.
- CounterACT does not communicate directly with the CrowdStrike Falcon agent on endpoints.



This deployment method scales efficiently and allows tuning of traffic loads.

Known Limitation

Detection event volume/velocity varies widely depending on the size of the customer environment. It's typically pretty low volume though, as a ballpark, even a 100K endpoint environment isn't likely to have more than 200 detections per 24 hours. Large deviations from this norm are likely indicators of a misconfiguration or an attack (such as a DDOS).

In these rare instances, CrowdStrike implements throttling to prevent threats or attacks that would DDOS the CrowdStrike cloud or downstream enterprise security software such as a SIEM. A good indication CrowdStrike has started to throttle event detection would be if CounterACT receives an event hours or days *after* a detection. The following are examples of when CrowdStrike would throttle detection events (example but not limited to):

- If CrowdStrike identifies the same pattern/detection on the same host and process, it will only trigger a detection once (not over and over)
- The same pattern/detection and host (without the same process) will only trigger, at most, once every 5 minutes.
- Maximum of 1,000 detections per day on a single endpoint (clear indication that the host should be investigated)

What to Do

Perform the following to carry out the integration:

1. Verify that requirements are met. See Requirements for details.
2. Download and install the ForeScout Extended Module for CrowdStrike Module from the ForeScout website: www.forescout.com/support. See Install the Module.
3. Configure the Module
4. (Optional) Configure CrowdStrike as an IOC Subscriber.
5. Create policies that implement integration Use Cases. See Run CrowdStrike Policy Templates.
6. When the configurations have been tested and the policies created, you are ready to start Using the CrowdStrike Extended Module.

Additional CrowdStrike Documentation

Refer to CrowdStrike online documentation for more information about the CrowdStrike solution:

https://falcon.crowdstrike.com/support/documentation

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- CrowdStrike Requirements
- Network Requirements

CounterACT Software Requirements

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

- CounterACT version 8.0
- A module license for CrowdStrike Module.
- An active Maintenance Contract for the licensed CrowdStrike module is required.
- Core Extensions Module version 1.0 or above with the IOC Scanner Plugin running (see Core Extension Information).

ForeScout Extended Module License Requirements

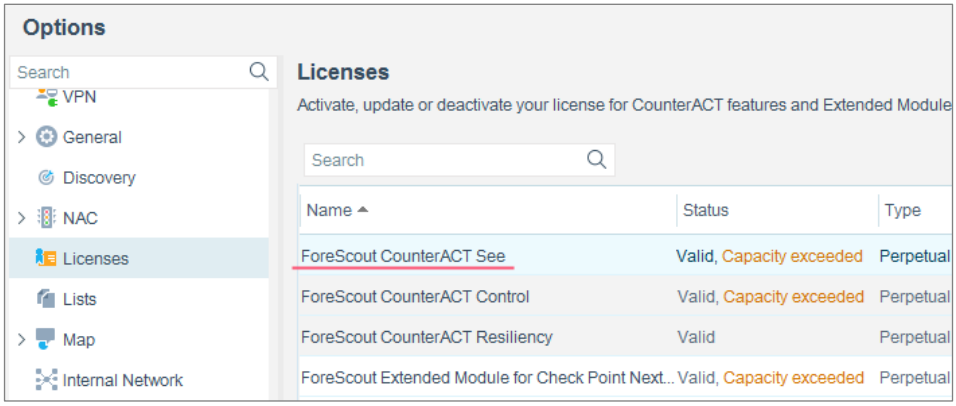
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- 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. T*he 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.

CrowdStrike Requirements

The module requires the following CrowdStrike Falcon components:

- A valid UUID, API Key, password and connectivity to CrowdStrike Streaming API Version 4.9 or later
- A valid username, password and connectivity to CrowdStrike Query API Version 3.3 or later

The Query API requires a special set of username and password credentials that can only be created by support@crowdstrike.com. This is not to be confused with the credentials that you use for the Falcon CrowdStrike user interface.

Network Requirements

When your environment routes Internet communications through a proxy server, you will need to configure the connection parameters for the proxy server that handles communication between this CrowdStrike Cloud Platform and its connecting CounterACT device.

To have a good performance, each connecting CounterACT device should handle no more than 40,000 devices on the network. Create multiple connecting appliance clusters if you have more devices on the network.

Install the Module

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

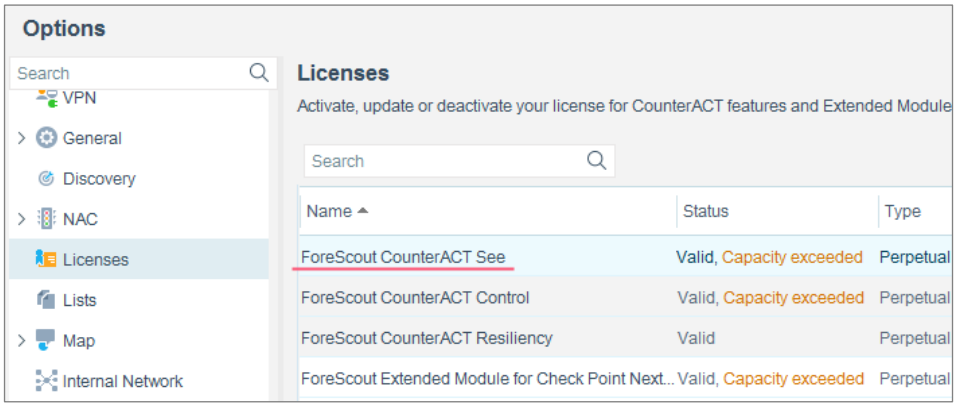
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    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.



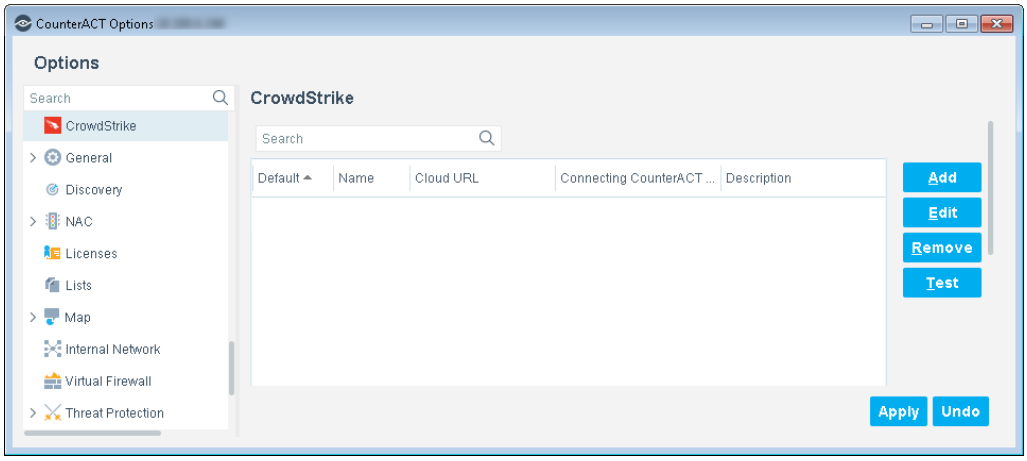
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

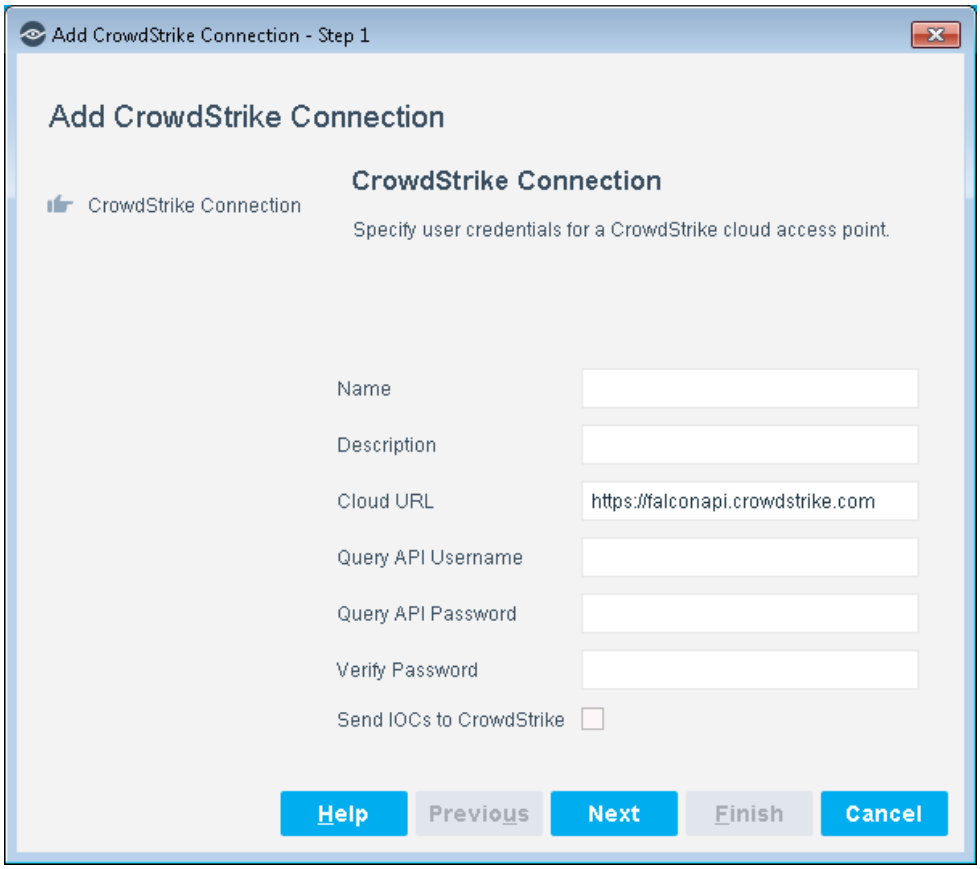
Configure the module to ensure that CounterACT can communicate with the CrowdStrike cloud. Perform this procedure after you Install the Module.

To add a connection to the CrowdStrike cloud:

1. In the CounterACT Console toolbar, select **Options** from the Tools menu.
2. Select **CrowdStrike** from the Options pane. The CrowdStrike configuration pane displays.



3. In the CrowdStrike pane, select **Add**. The Add CrowdStrike Connection wizard opens.

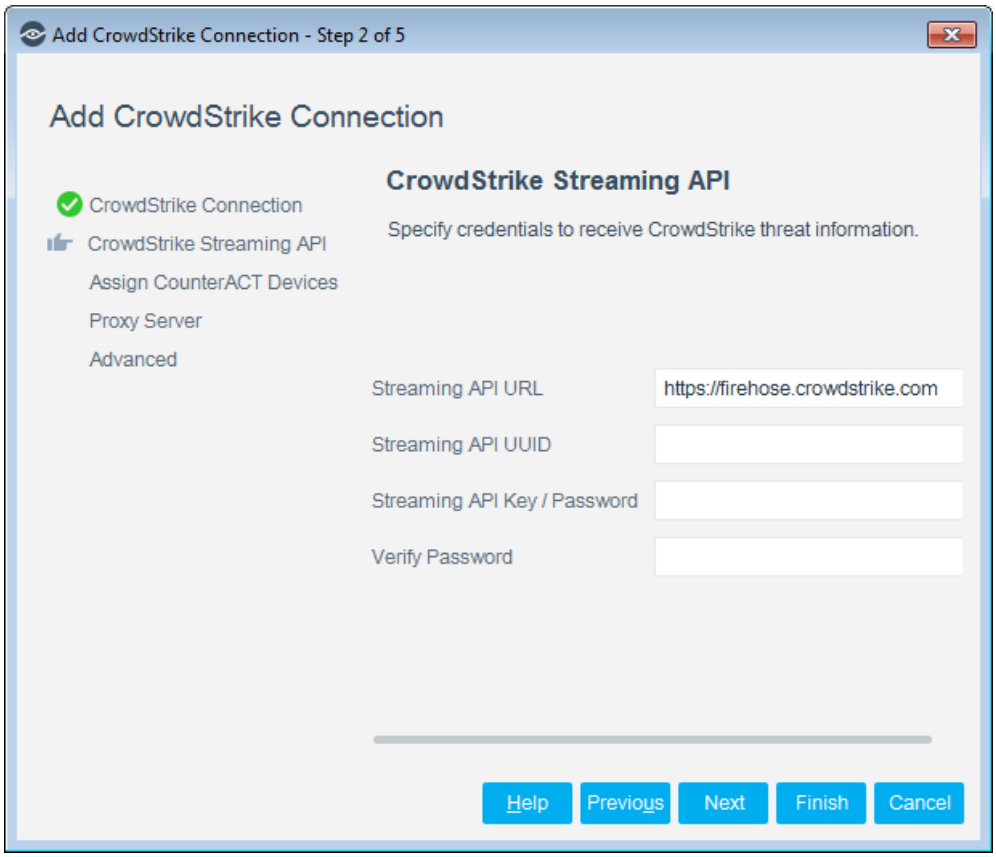


4. Specify the following fields to define a connection to the CrowdStrike cloud:

Name	Enter the name of the CrowdStrike connection.
Description	(Optional) Enter additional text to help users identify this CrowdStrike connection.

Cloud URL	A default URL to the CrowdStrike cloud access point displays, however, you can modify the URL for your needs.
Query API Username	Contact CrowdStrike Support to get a Query API username and password for accessing the CrowdStrike server.
Query API Password	
Verify Password	Re-enter the password.
Send IOCs to CrowdStrike	Select this box to send user-defined third-party generated IOCs to CrowdStrike for threat endpoint hunting.

5. Select **Next**. The CrowdStrike Streaming API pane opens.

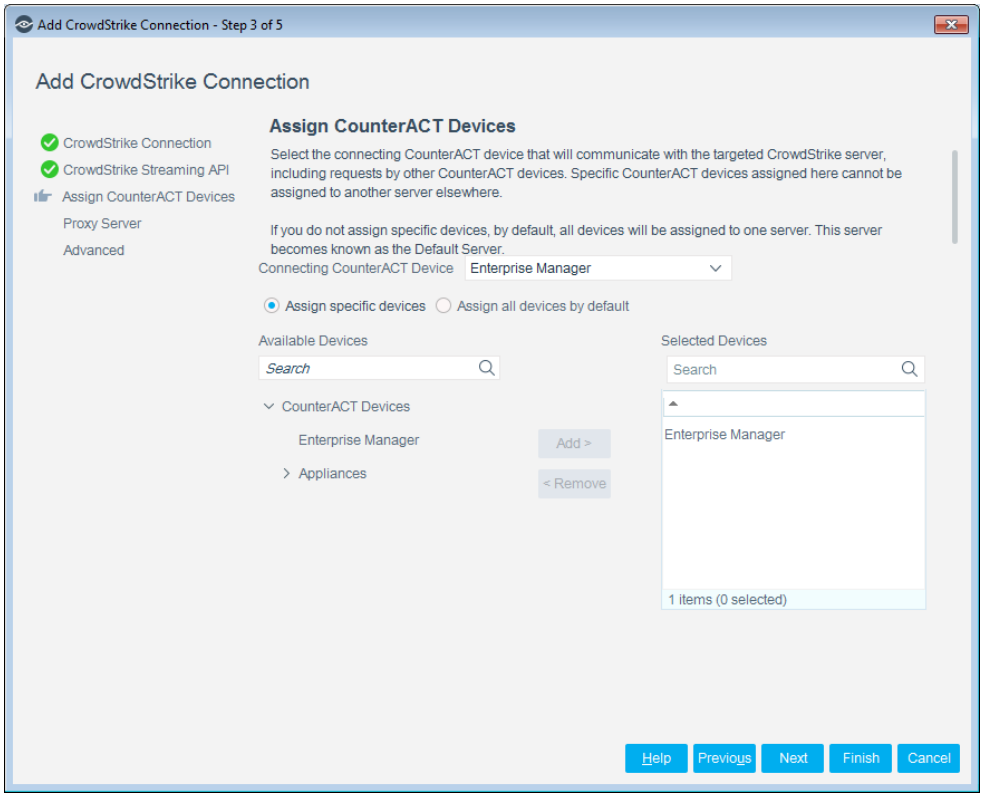


6. Enter the credentials you received from CrowdStrike to access the streaming API exposed by this cloud connection.

Streaming API URL	A default URL to the CrowdStrike Streaming API displays, however, you can modify the URL for your needs.
Streaming API UUID	Contact CrowdStrike Support to get a Streaming API Universally Unique Identifier (UUID) and password for accessing the CrowdStrike server.
Streaming API Password	
Verify Password	Re-enter the password.

At times, the CrowdStrike Cloud will receive threat information from its agents, but is slow to forward that threat information to CounterACT. However, whenever it does forward that information to CounterACT, it then acts on the threats as per its configured policies.

7. Select **Next**. The Assign CounterACT Devices pane displays.



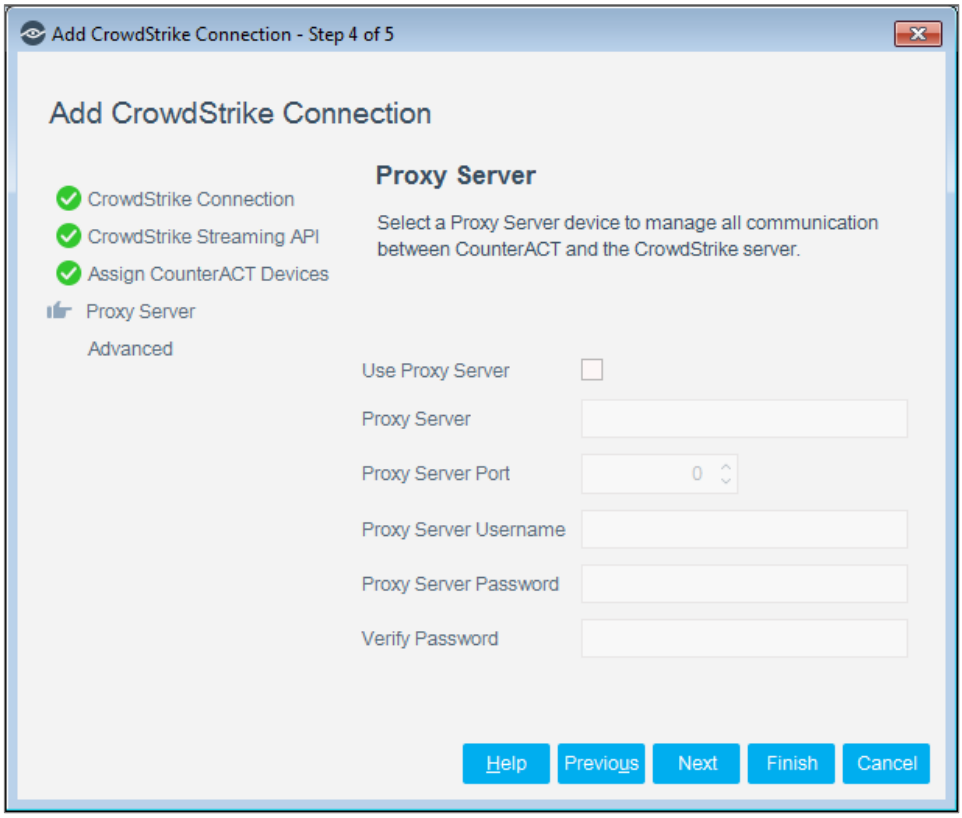
To have a good performance, each connecting CounterACT device should handle no more than 40,000 devices on the network. Create multiple connecting appliance clusters if you have more devices on the network.

8. In the **Connecting CounterACT Device** drop-down, select the device through which other CounterACT devices will communicate with this CrowdStrike cloud instance. The device specified in this field is the only CounterACT device that communicates directly with this cloud instance. If more than one CrowdStrike cloud instance is defined, this device cannot communicate with another CrowdStrike cloud instance.
9. Specify other CounterACT devices that interact with CrowdStrike through this cloud instance. These devices do not communicate with CrowdStrike directly. All communication between the CrowdStrike instance and CounterACT is handled by the device specified in the **Connecting CounterACT Device** field. If more than one CrowdStrike cloud instance is defined, each CounterACT device can only be assigned to one CrowdStrike instance.

Do one of the following:

- Select **Assign specific devices**. CounterACT devices that you move from the Available Devices column to the Selected Devices column will use this CloudStrike instance.
- Select **Assign all devices by default**. All CounterACT devices not assigned to another CrowdStrike instance will use this instance. In the CrowdStrike configuration pane, an icon indicates that this is the default connection to CrowdStrike. If only one CrowdStrike instance is defined, this options is selected by default.

10. Select **Next.** The Proxy Server pane displays.



When your environment routes Internet communications through a proxy server, you will need to configure the following connection parameters for the proxy server that handles communication between this CrowdStrike Cloud Platform and its connecting CounterACT device.

11. (Optional) If using a proxy server with Basic Authentication, enter proxy credentials into the following fields.

Use Proxy Server	Select this option to use a proxy server to communicate with the CrowdStrike Cloud Platform.
Proxy Server	Enter the IP address of the proxy server.
Proxy Server Port	Select the port used to communicate with the proxy server.

Proxy Server Username	(Optional) For proxies using Basic Authentication, enter the proxy server's login name for an authorized account defined on the proxy.
Proxy Server Password	(Optional) For proxies using Basic Authentication, enter the proxy server's login password.
Verify Password	Verify the proxy server's password.

12. Select **Next**. The Advanced pane displays.

13. Enter your configurations.

API Rate Limit	Select the number of API requests per second.

14. Select **Finish**. The connection is listed in the CrowdStrike configuration pane.
15. To test a CrowdStrike connection, select the connection in the CrowdStrike configuration pane and then select **Test**.

    If the test fails:

    – Check your configuration settings
    – Verify that authentication certificates were installed in CounterACT.
    – Verify that an account with the correct permissions is defined for CounterACT in the CrowdStrike cloud.

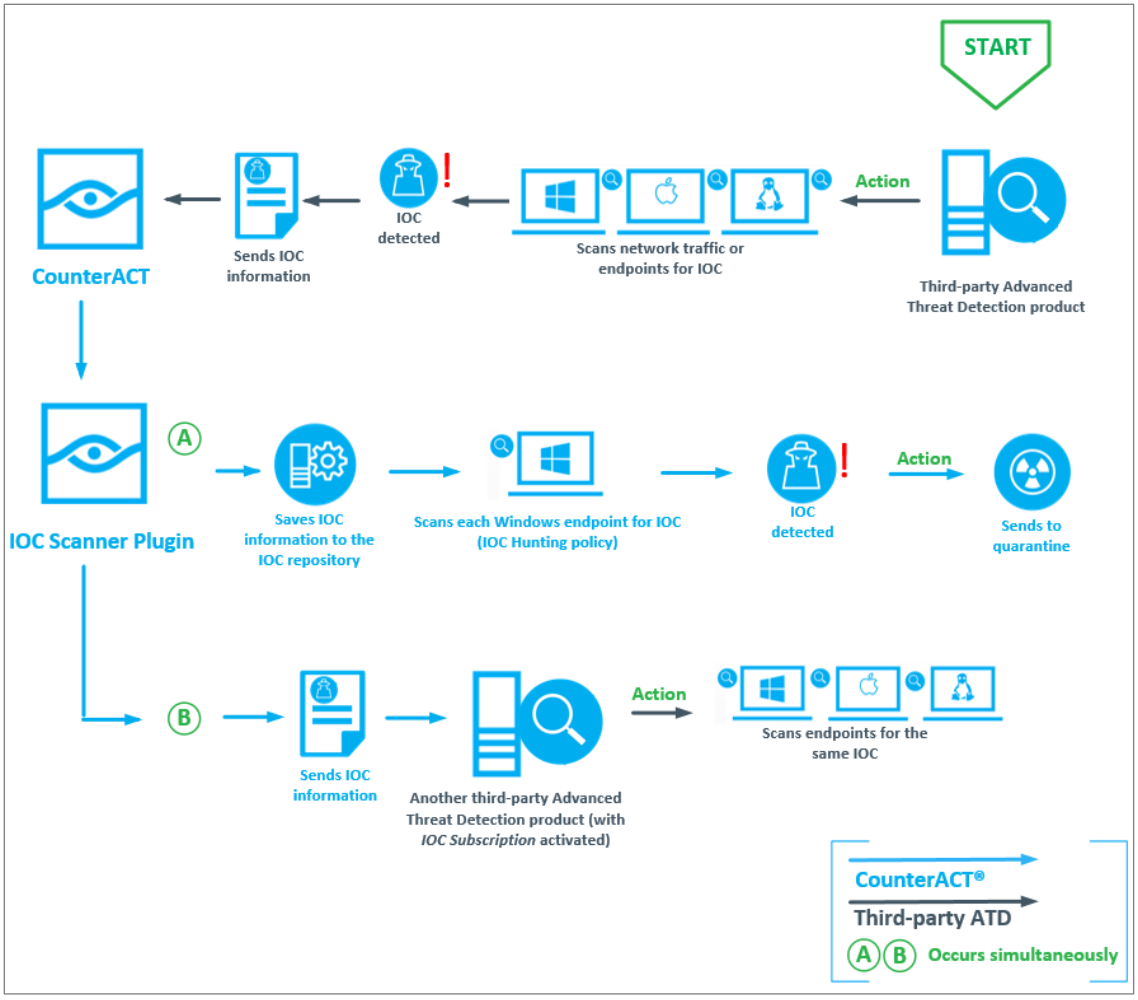
16. Repeat this procedure to define connections to other CrowdStrike cloud access points.

Configure CrowdStrike as an IOC Subscriber

The IOC Scanner Plugin lets CounterACT share IOC information with external platforms.

When the CrowdStrike Module is installed and running, it can be configured to automatically start IOC sharing with CrowdStrike by:

- Logging in to the CrowdStrike Streaming API to receive IOCs from CrowdStrike
- Subscribing CrowdStrike to CounterACT IOC streams. CrowdStrike displays in the *IOC Subscriptions* tab of the IOC Scanner Module configuration pane.



By default, IOCs are NOT forwarded to the CrowdStrike Cloud. Once configured, these subscriptions are configured to share all IOC information from CounterACT. In some environments it may be necessary to use settings that restrict the type or volume of IOCs that are shared by CounterACT.

For more information about IOC Scanner, refer to the *CounterACT IOC Scanner Module Configuration Guide*.

Test the Module Configuration

This section describes how to perform a configuration test. The test checks connectivity between the CloudStrike gateway IP address and the connecting CounterACT device.

To run a test:

1. In the CrowdStrike pane, select the server you want to test, and select **Test**.

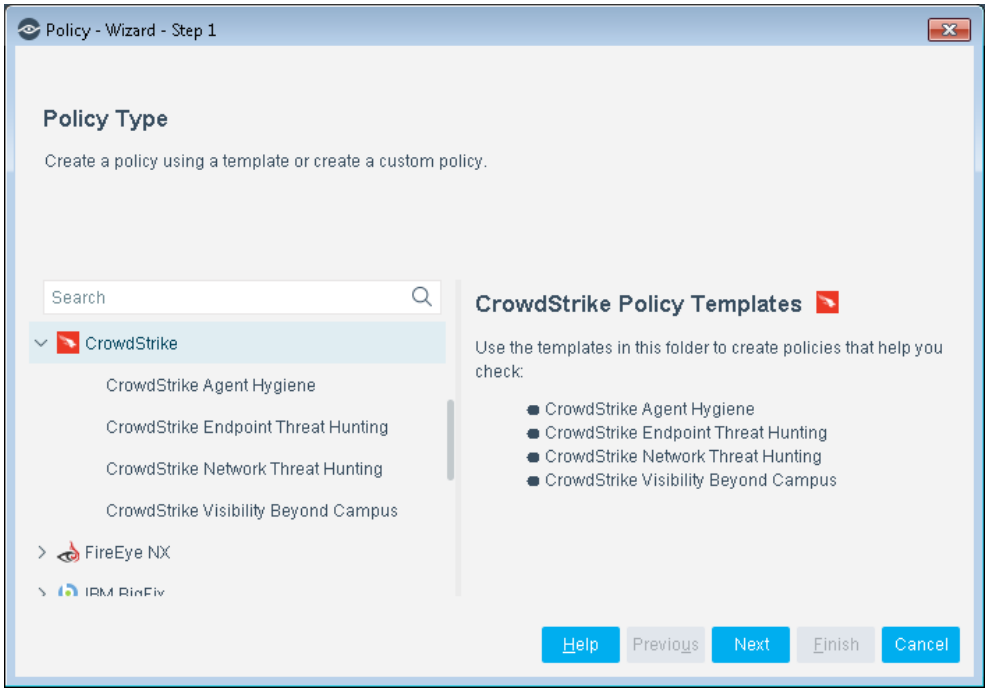
   The CrowdStrike Module Configuration Test dialog box displays the test results.

2. Select **Close**.

Run CrowdStrike Policy Templates

This module provides the following policy templates:

- CrowdStrike Agent Hygiene Policy Template: this template generates a policy that detects whether Windows endpoints are running the CrowdStrike Falcon agent.
- CrowdStrike Endpoint Threat Hunting Policy Template - this template provides a basic structure for most coordinated remediation scenarios involving CrowdStrike and CounterACT. It generates a policy that detects endpoints based on threats recently reported to CounterACT by CrowdStrike, and can apply CounterACT actions to remediate or restrict these endpoints.
- CrowdStrike Network Threat Hunting Policy Template - this template provides comprehensive network and endpoint detections, expands threat hunting to traditional, non-traditional and CrowdStrike-managed devices, and leverages bi-directional threat intelligence sharing to secure your network from threats.
- CrowdStrike Visibility Beyond Campus Policy Template - this template utilizes CrowdStrike endpoint protection sensors to detect activities across servers, desktops, and laptops.
- Sub-rules detect endpoints based on the severity of the reported threat. Optional actions provide examples of the ways CounterACT can remediate or restrict the endpoint in response to the threat.



You should have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates *and* Policy Management *chapters of the* CounterACT Administration Guide*.*

CrowdStrike Agent Hygiene Policy Template

The purpose of the Agent Hygiene template is assurance that the CrowdStrike Agent is correctly configured and active on all licensed and mandated endpoints. This template generates a policy that detects whether endpoints are running the CrowdStrike Falcon Agent.

The main rule of this policy detects endpoints that are managed by CounterACT using the CrowdStrike Query API. Optionally, add Remote Inspection for a secondary variation of the agent health.

Sub-rules of the policy run scripts or evaluate host properties to determine whether the CrowdStrike Falcon agent is installed and running on endpoints. Optional actions let you install the agent as needed.

Prerequisites

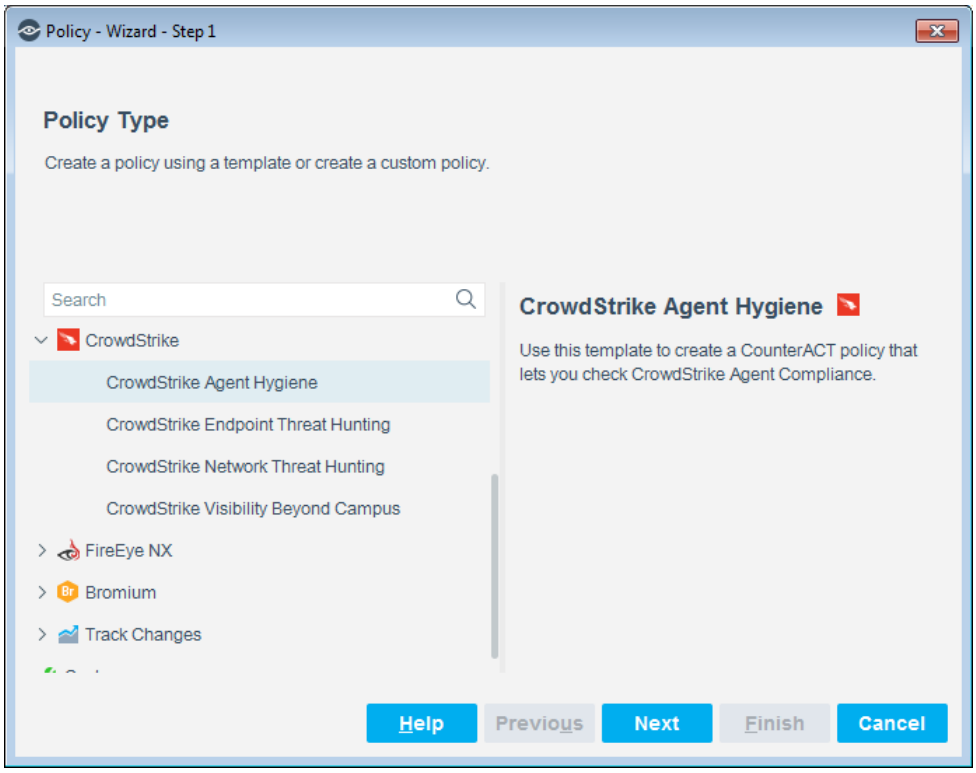
Policies you create with this template detect endpoints. Before you run a policy based on this template, verify that you have run policies based on the *Asset Classification* or *Primary Classification* policy templates.

Remote Inspection is used to run scripts and perform remediation actions on endpoints. Verify that Remote Inspection has been configured in your environment.

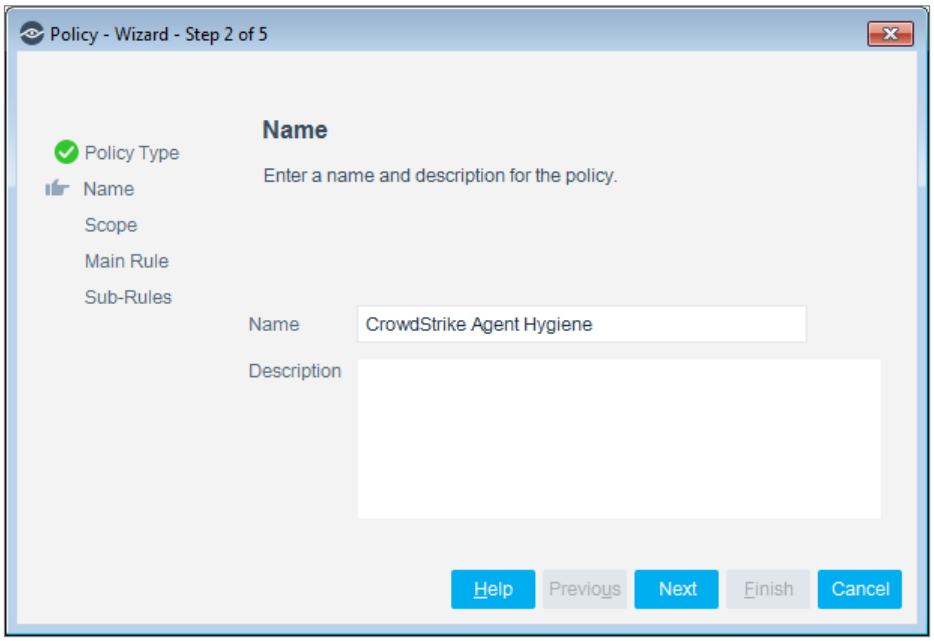
To use the CrowdStrike Agent Hygiene policy template:

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 CrowdStrike folder and select **CrowdStrike Agent Hygiene**.



4. Select **Next.** The policy wizard opens to the **Name** pane.



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.

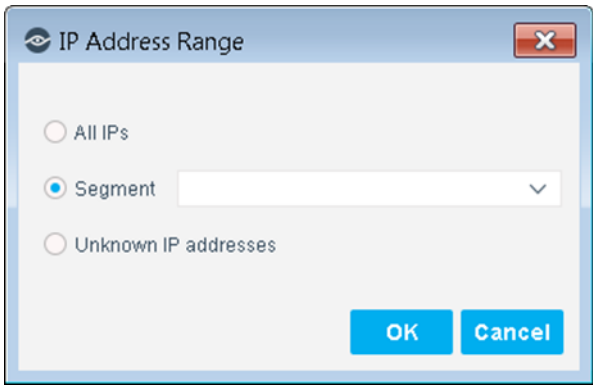
   Naming Tips

   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - The name should indicate what the policy verifies and what actions are taken.
   - The name should indicate 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 Hosts 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 page.
   - **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 displays in the Scope pane.
9. (Optional) To review and modify default policy logic before you create the policy, select **Next**. The Main Rule pane displays.

How Devices are Detected and Handled

Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

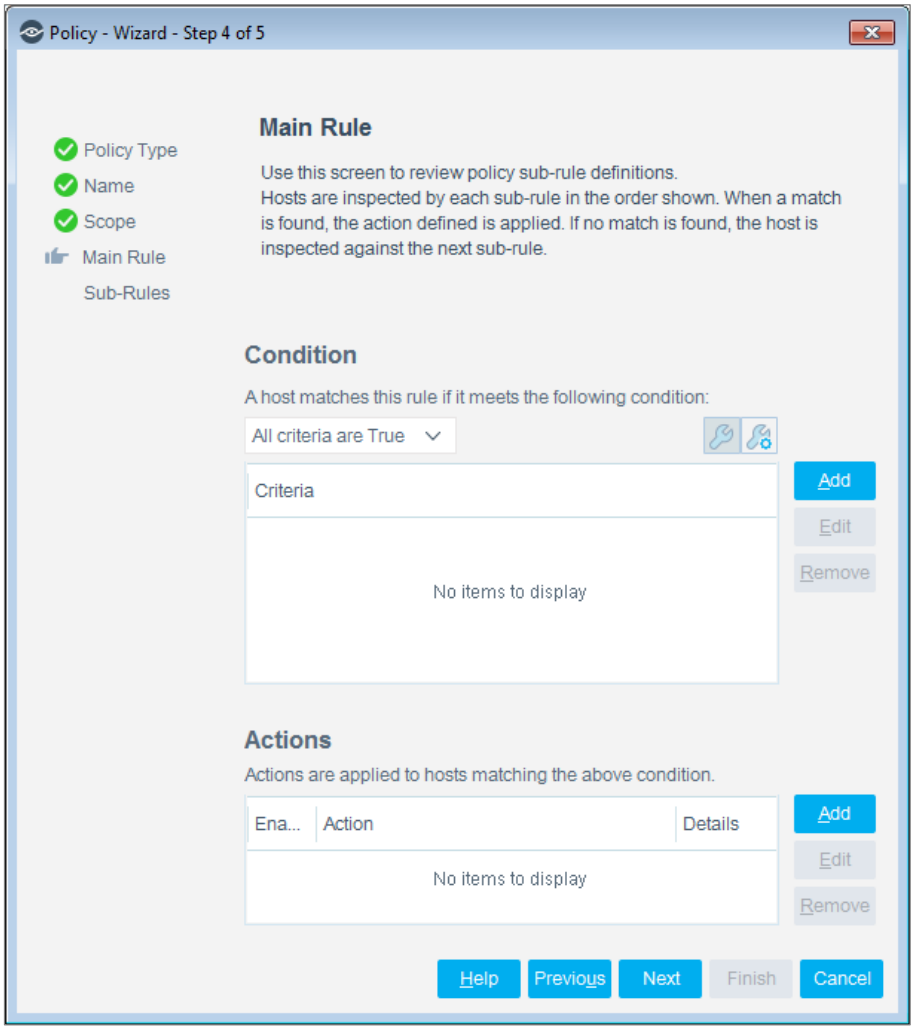
Endpoints that match the Main Rule pass to sub-rules of the policy for further evaluation. *Endpoints that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

When a match is found, the corresponding actions are applied to the endpoint. No further sub-rules are evaluated for this endpoint.

Main Rule

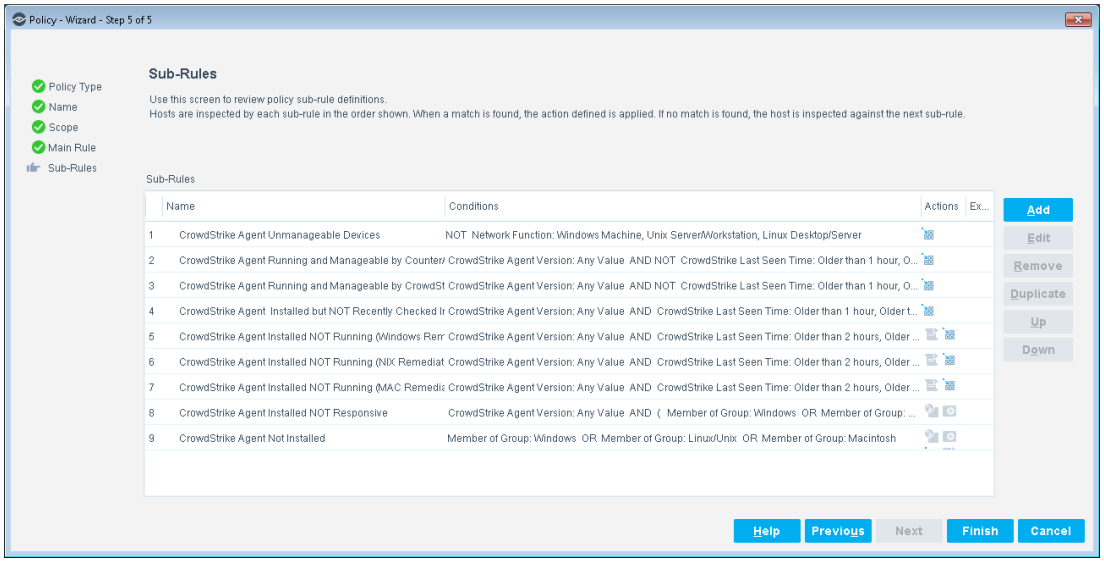
The main rule of this policy detects Windows endpoints that are managed using Remote Inspection.



10. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.
11. Select **Next**. The Sub-Rules pane displays.

Sub-Rules

The sub-rules of the CrowdStrike Agent Hygiene policy list the items CounterACT is to check when applying the Main Rule.



12. Double-click the CrowdStrike Agent Running and Manageable by CounterACT sub-rule to open it. The Policy: [Name] - Sub-Rule: CrowdStrike Agent Running and Manageable by CounterACT dialog box opens.
13. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section.
14. Select **OK**. In the Policy: [Name] Sub-Rule: CrowdStrike Agent Running and Manageable by CounterACT dialog box, select **OK**.
15. Repeat steps 12 - 14 to make changes in other sub-rules.
16. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
17. On the CounterACT Console, select **Apply** to save the policy.

CrowdStrike Endpoint Threat Hunting Policy Template

The purpose of this template is to set policy and enforcement with CounterACT based on parameters as reported by CrowdStrike. It generates a policy that detects endpoints based on threats recently reported to CounterACT by CrowdStrike. Based on the policy condition(s), CounterACT takes action. The compromised endpoint is contained and CrowdStrike generates threat intelligence and shares the IOCs with CounterACT via the CrowdStrike Network Threat Hunting Policy Template.

The main rule of the policy detects endpoints for which CounterACT received threat detections not older than one week.

Sub-rules detect endpoints based on the severity of the reported threat. Optional actions provide additional ways CounterACT can remediate or restrict the endpoints.

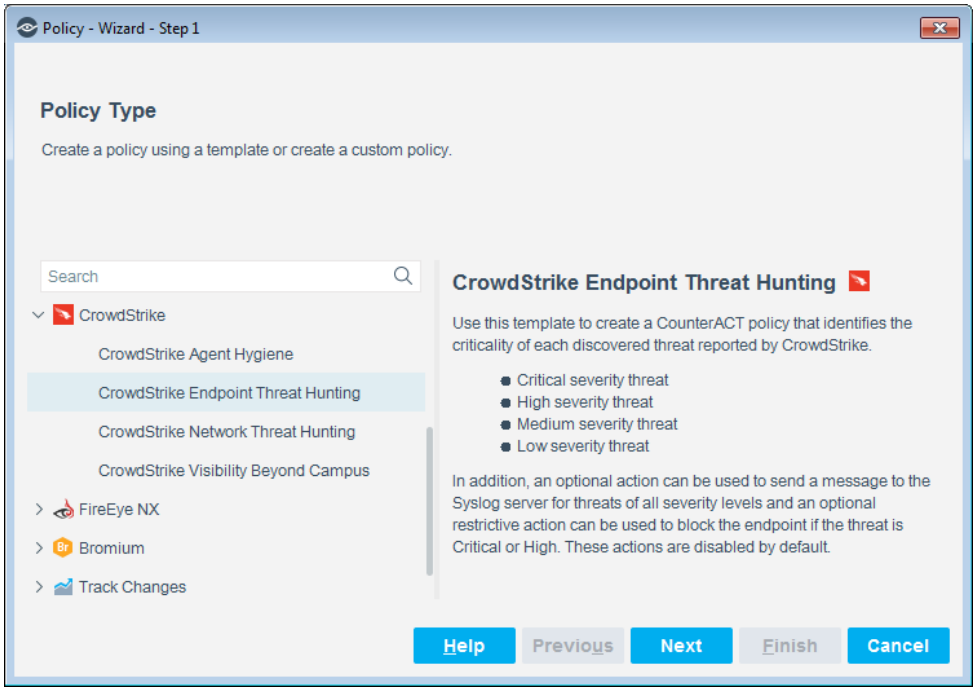
Prerequisites

Policies you create with this template detect endpoints. Before you run a policy based on this template, verify that you have run policies based on the *Asset Classification* or *Primary Classification* policy templates.

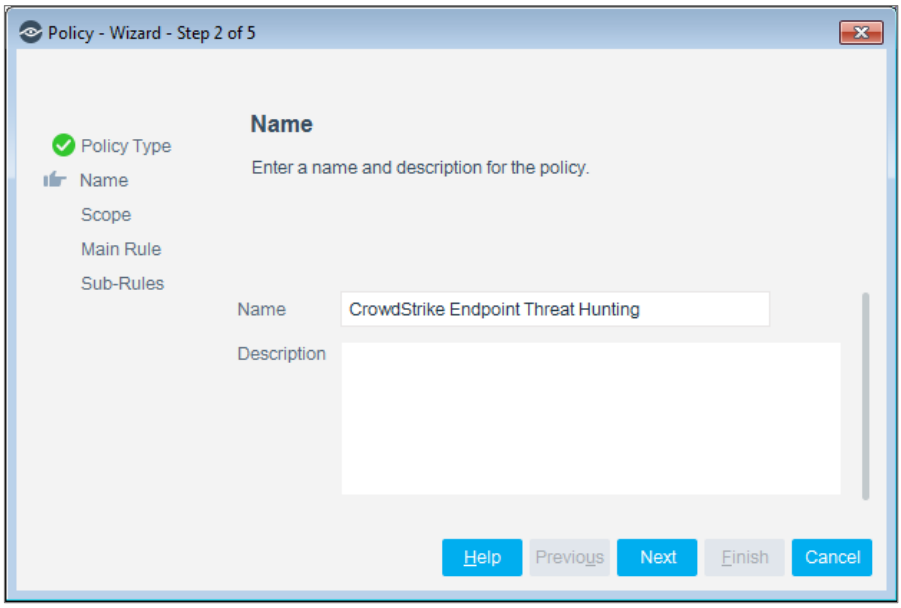
Remote Inspection is used to run scripts and perform remediation actions on endpoints. Verify that Remote Inspection has been configured in your environment.

To use the CrowdStrike Endpoint Threat Hunting 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 CrowdStrike folder and select **CrowdStrike Endpoint Threat Hunting**.



4. Select **Next.** The policy wizard opens to the **Name** pane.



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.

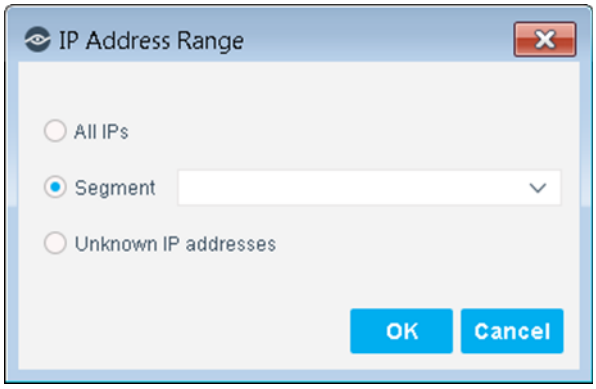
Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- The name should indicate what the policy verifies and what actions are taken.
- The name should indicate 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 displays.

Define Which Hosts 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 page.
- **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 d in the Scope pane.
9. (Optional) To review and modify default policy logic before you create the policy, select **Next**. The Main Rule pane displays.

How Devices are Detected and Handled

Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

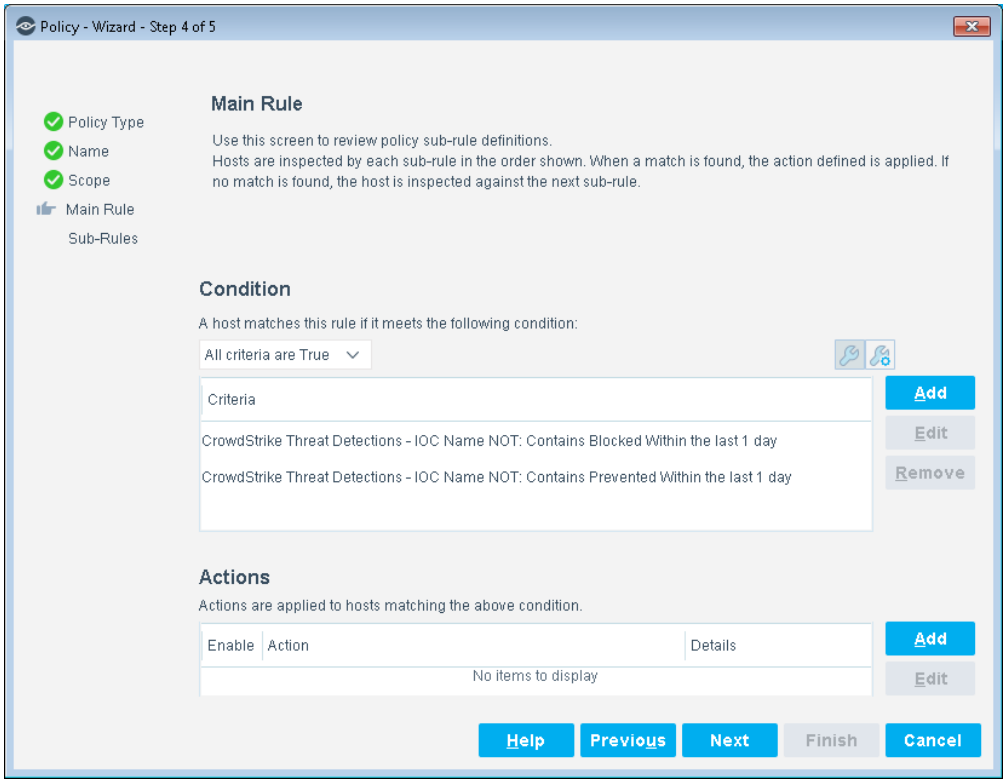
Endpoints that match the Main Rule pass to sub-rules of the policy for further evaluation. *Endpoints that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

When a match is found, the corresponding actions are applied to the endpoint. No further sub-rules are evaluated for this endpoint.

Main Rule

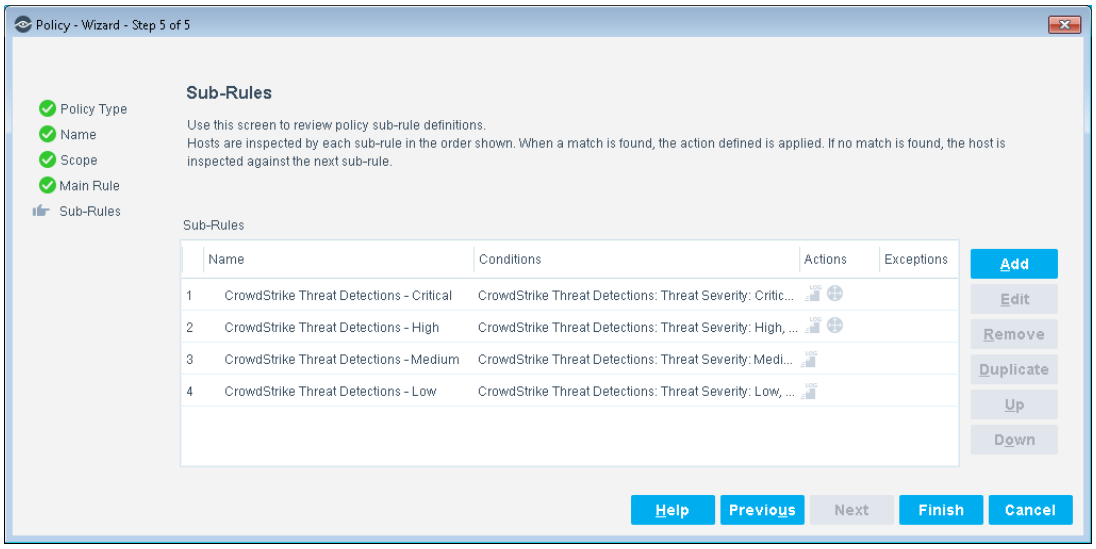
The main rule of this policy uses the CrowdStrike Threat Detection property to select all endpoints for which CounterACT received a CrowdStrike Threat Detection report within the last week.



10. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.
11. Select **Next**. The Sub-Rules pane displays.

Sub-Rules

The sub-rules of the CrowdStrike Endpoint Threat Hunting policy list the items CounterACT is to check when applying the Main Rule.



12. Double-click the CrowdStrike Threat Detections - Critical sub-rule to open it. The Policy: [Name] - Sub-Rule: CrowdStrike Threat Detections - Critical dialog box opens.
13. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section.
14. Select **OK**. In the Policy: [Name] Sub-Rule: CrowdStrike Threat Detections - Critical dialog box, select **OK**.
15. Repeat steps 12 - 14 to make changes in other sub-rules.
16. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
17. On the CounterACT Console, select **Apply** to save the policy.

CrowdStrike Network Threat Hunting Policy Template

The purpose of this template is to provide:

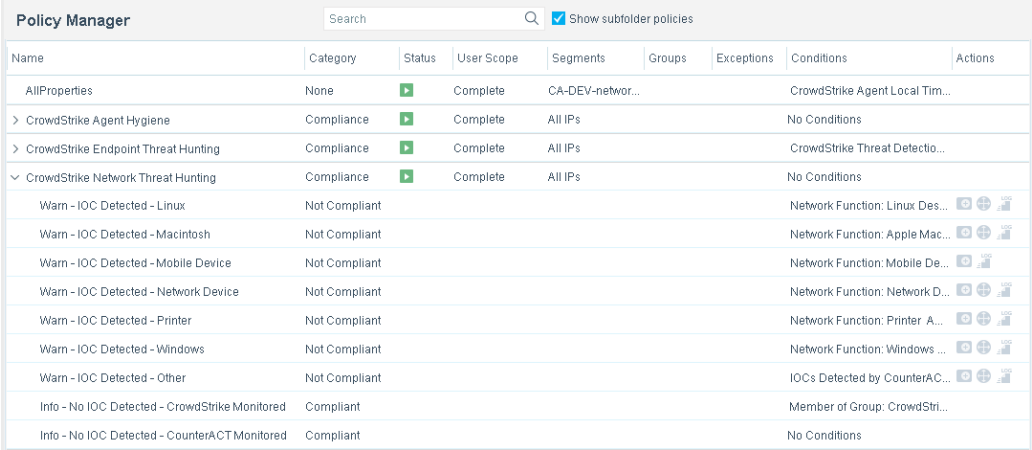
- Comprehensive network and endpoint detection tactics with discrete response
- Expand threat hunting to include non-traditional and non-CrowdStrike-managed devices, including IoT, Operational Technology (OT), BYOD and Guest devices.
- Leverage bi-directional threat intelligence sharing to secure your network from threats

CrowdStrike uses multiple methods to prevent and detect malware. These methods include machine learning, exploit blocking, blacklisting and indicators of attack. Indicators of attack are sent to CounterACT and blocked via network firewall or network quarantine.

When a new device enters the network and CounterACT identifies the device as a guest. Based on policy condition(s), CounterACT monitors network connections and DNS queries for IOAs or IOCs. CounterACT identifies a suspicious DNS query to a known CNC domain from the guest device. The compromised endpoint is then quarantined away from the production network.

The main rule of the policy detects IOCs on networks that CounterACT received threat detections in the past eight hours.

Sub-rules detect endpoints based on the network function type. Optional actions provide examples of the ways CounterACT can remediate or restrict the endpoints.



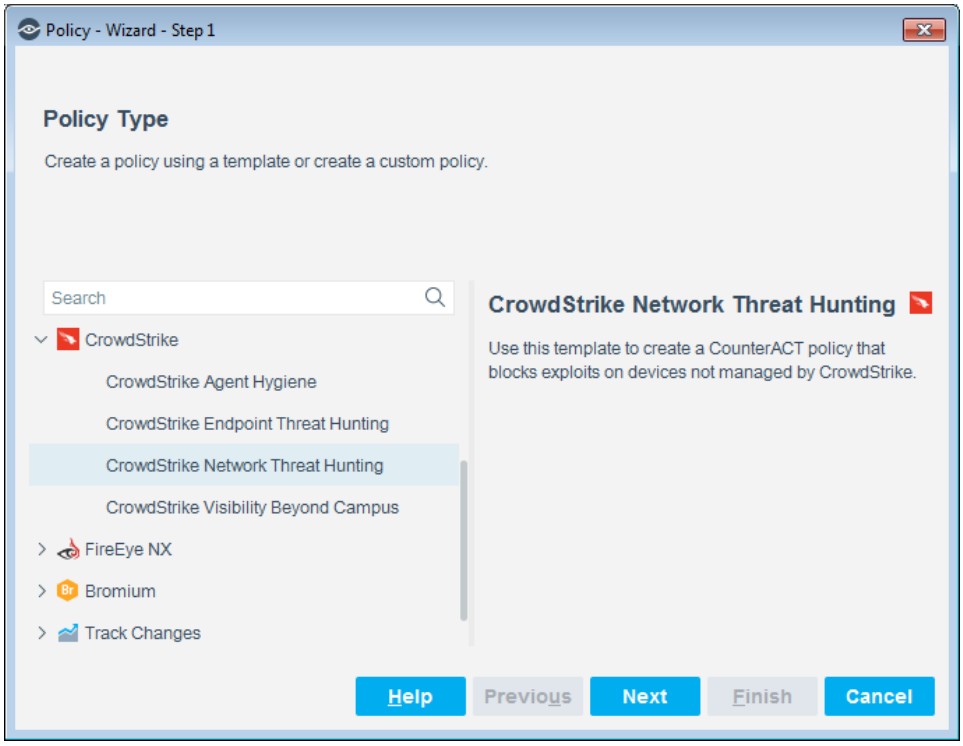
Prerequisites

Policies you create with this template detect endpoints. Before you run a policy based on this template, verify that you have run policies based on the *Asset Classification* or *Primary Classification* policy templates.

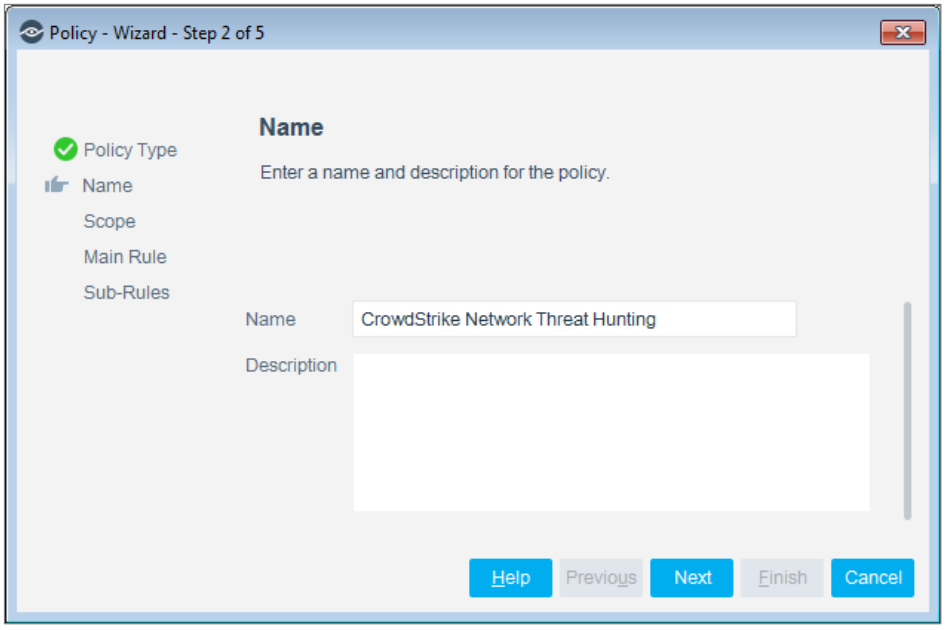
Remote Inspection is used to run scripts and perform remediation actions on endpoints. Verify that Remote Inspection has been configured in your environment.

To use the CrowdStrike Network Threat Hunting 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 CrowdStrike folder and select **CrowdStrike Network Threat Hunting**.



4. Select **Next.** The policy wizard opens to the **Name** pane.



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.

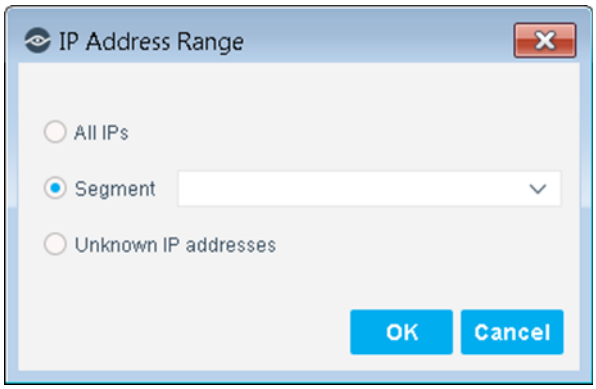
   Naming Tips

   – Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   – The name should indicate what the policy verifies and what actions are taken.
   – The name should indicate 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 pane displays.

Define Which Hosts 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 page.
   – **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 displays in the Scope pane.
9. (Optional) To review and modify default policy logic before you create the policy, select **Next**. The Main Rule pane displays.

How Devices are Detected and Handled

Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

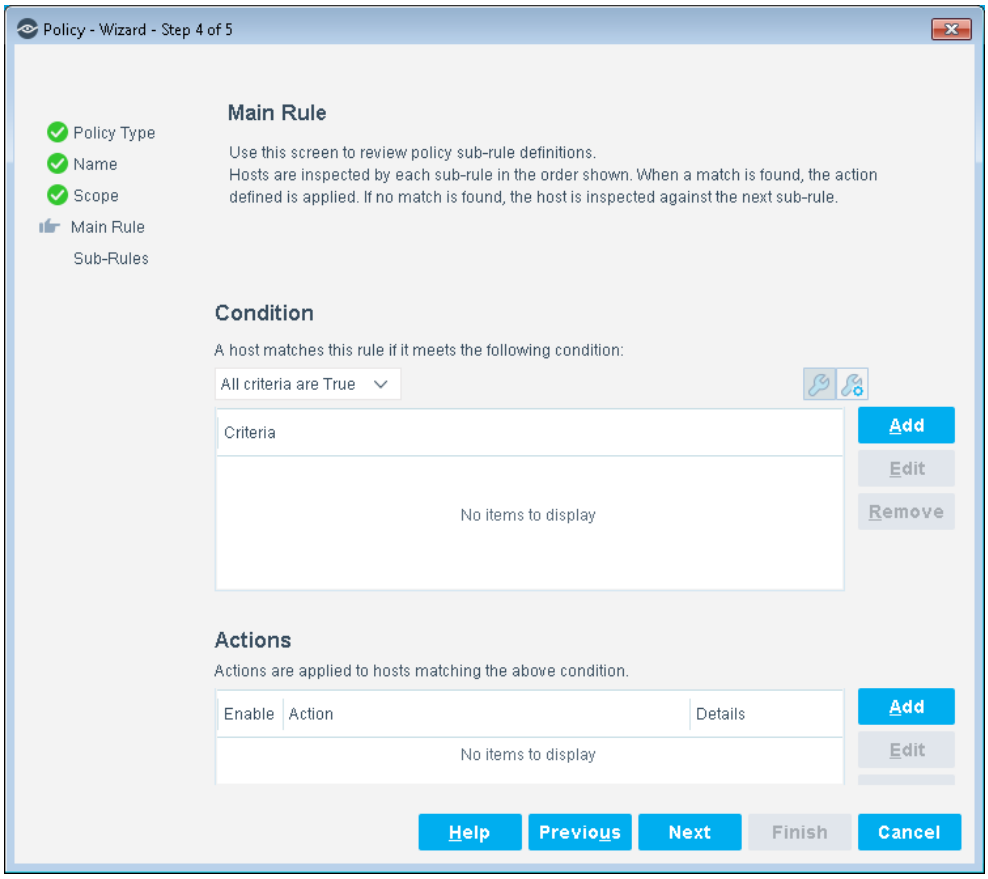
Endpoints that match the Main Rule pass to sub-rules of the policy for further evaluation. *Endpoints that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

When a match is found, the corresponding actions are applied to the endpoint. No further sub-rules are evaluated for this endpoint.

Main Rule

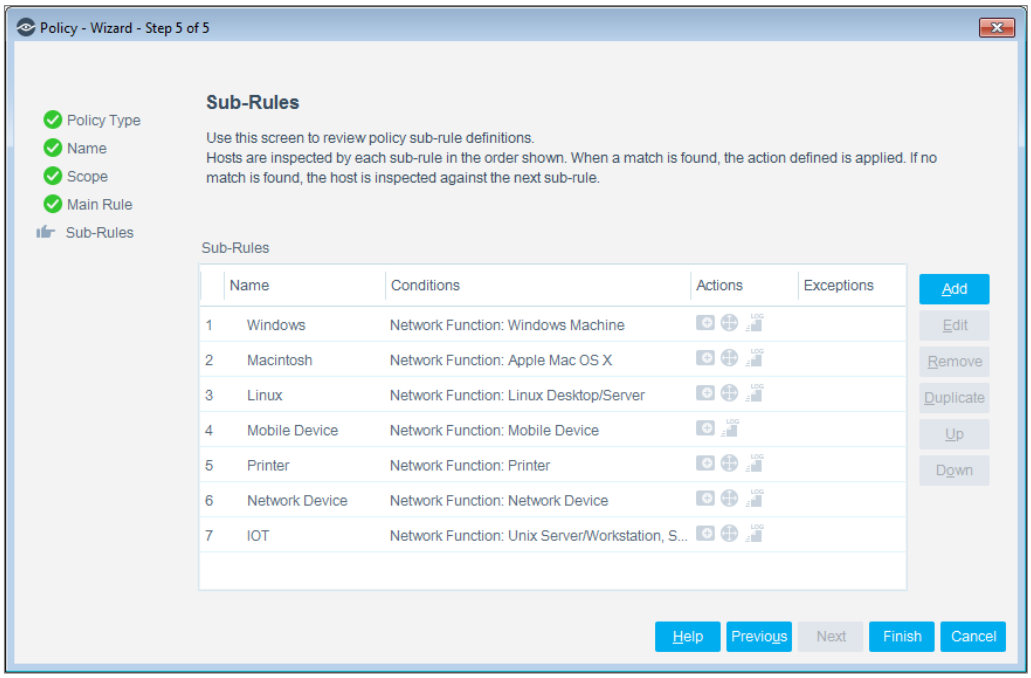
The main rule of this policy uses the **CrowdStrike Threat Detection** property to select all endpoints for which CounterACT received a CrowdStrike Threat Detection report within the last week.



10. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.
11. Select **Next**. The Sub-Rules pane displays.

Sub-Rules

The policy applies the following sub-rules to endpoints detected by the main rule:



12. Double-click the Windows sub-rule to open it. The Policy: [Name] - Sub-Rule: Windows dialog box opens.
13. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section.
14. Select **OK**. In the Policy: [Name] Sub-Rule: Windows dialog box, select **OK**.
15. Repeat steps 12 - 14 to make changes in other sub-rules.
16. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
17. On the CounterACT Console, select **Apply** to save the policy.

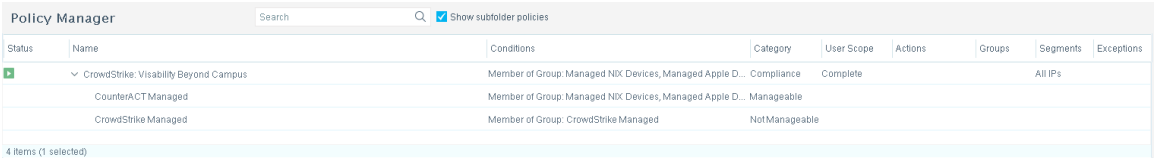
CrowdStrike Visibility Beyond Campus Policy Template

This template utilizes CrowdStrike endpoint protection sensors to detect activities across the servers, desktops, laptops, and across the remote employees who may be working from home.

A user begins to work from a remote location. Without the protection of the corporate firewall, the user's computer is compromised. CrowdStrike identifies the compromise and informs CounterACT. The compromised endpoint is contained and CrowdStrike generates threat intelligence and shares the IOCs or IOAs with CounterACT via the Network Threat Hunting template.

The main rule of this policy detects endpoints that are managed by CounterACT using the CrowdStrike Query API. Optionally, add Remote Inspection for a secondary variation of the agent health.

The sub-rules of this policy determine whether the host is a member a CounterACT-manageable or a CrowdStrike-manageable group.



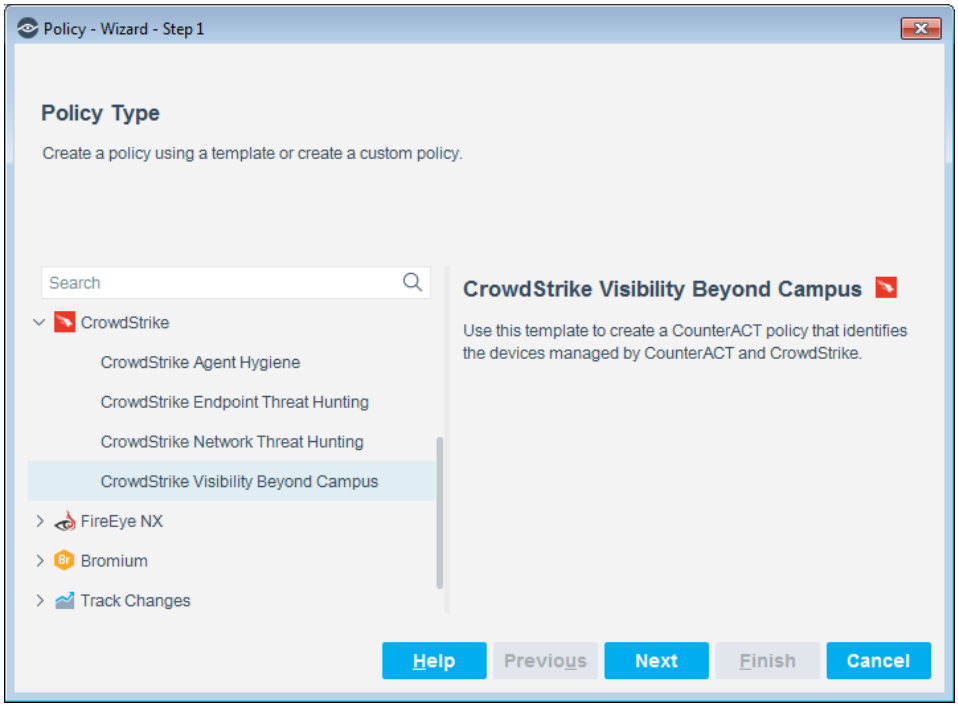
Prerequisites

Policies you create with this template detect endpoints. Before you run a policy based on this template, verify that you have run policies based on the *Asset Classification* or *Primary Classification* policy templates.

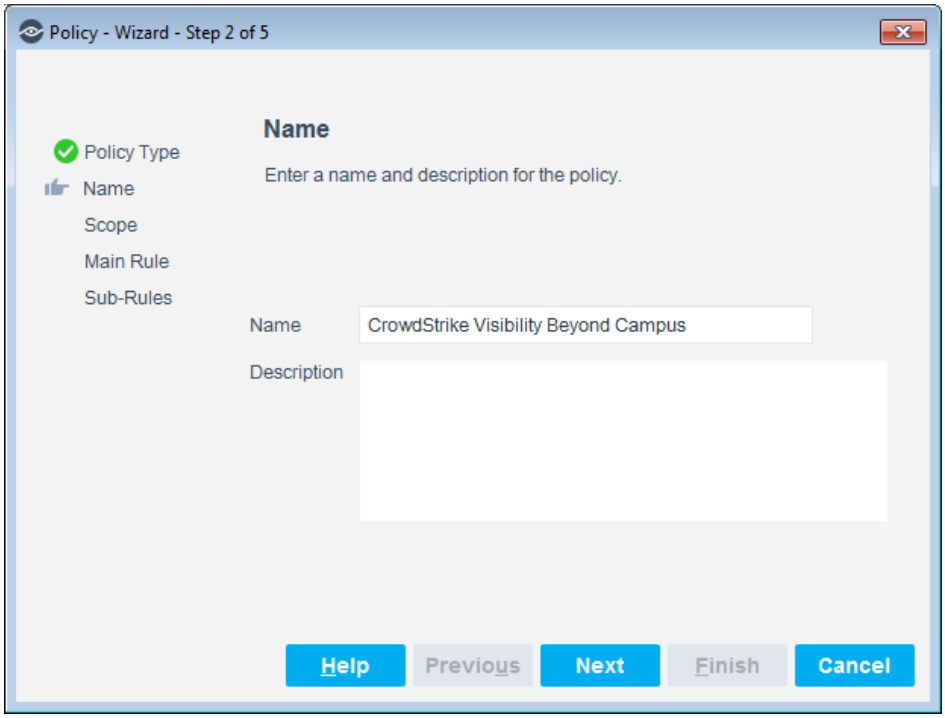
Remote Inspection is used to run scripts and perform remediation actions on endpoints. Verify that Remote Inspection has been configured in your environment.

To use the CrowdStrike Visibility Beyond Campus 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 CrowdStrike folder and select **CrowdStrike Visibility Beyond Campus**.



4. Select **Next.** The policy wizard opens to the **Name** pane.



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.

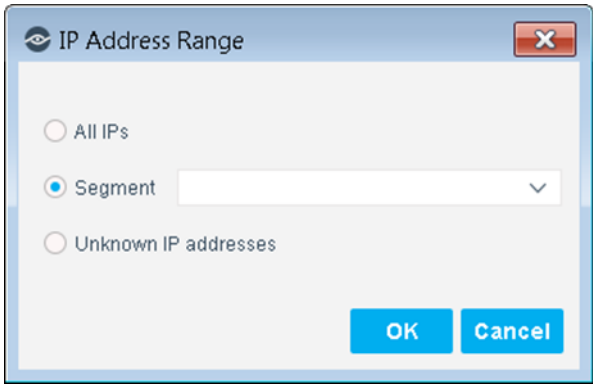
   Naming Tips

   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - The name should indicate what the policy verifies and what actions are taken.
   - The name should indicate 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 Hosts 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 page.
- **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 displays in the Scope pane.
9. (Optional) To review and modify default policy logic before you create the policy, select **Next**. The Main Rule pane displays.

How Devices are Detected and Handled

Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

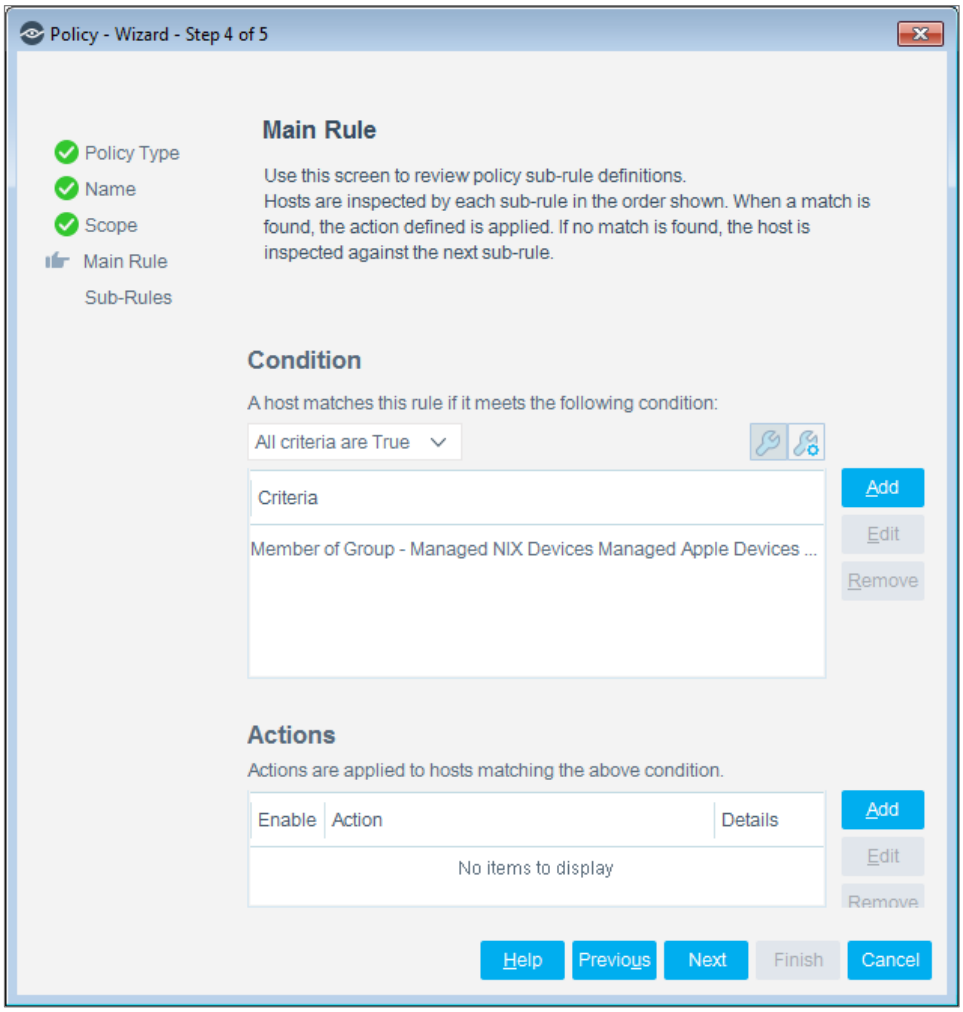
Endpoints that match the Main Rule pass to sub-rules of the policy for further evaluation. *Endpoints that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

When a match is found, the corresponding actions are applied to the endpoint. No further sub-rules are evaluated for this endpoint.

Main Rule

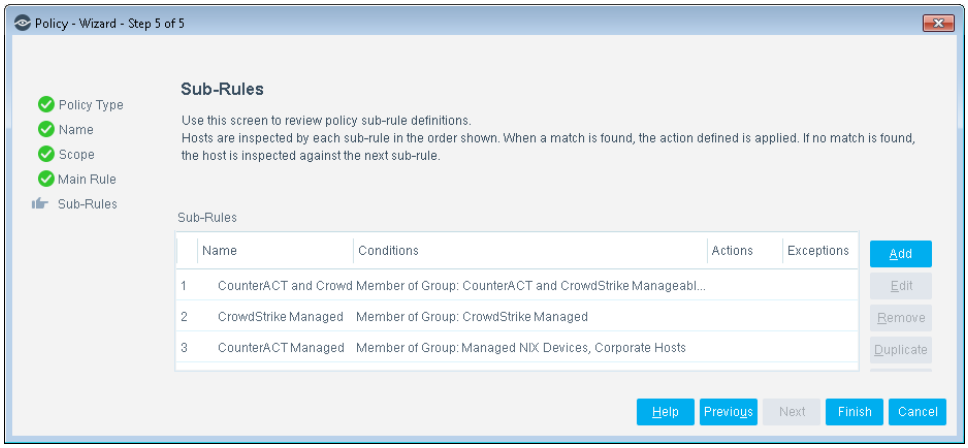
The main rule of this policy checks whether the network type of endpoints that are being managed are part of a group.



10. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.
11. Select **Next**. The Sub-Rules pane displays.

Sub-Rules

The policy applies the following sub-rules to endpoints detected by the main rule:



12. Double-click the Windows sub-rule to open it. The Policy: [Name] - Sub-Rule: CounterACT Managed dialog box opens.
13. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties section.
14. Select **OK**. In the Policy: [Name] Sub-Rule: CounterACT Managed dialog box, select **OK**.
15. Repeat steps 12 - 14 to make changes in other sub-rules.
16. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
17. On the CounterACT Console, select **Apply** to save the policy.

Create Custom CrowdStrike 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:

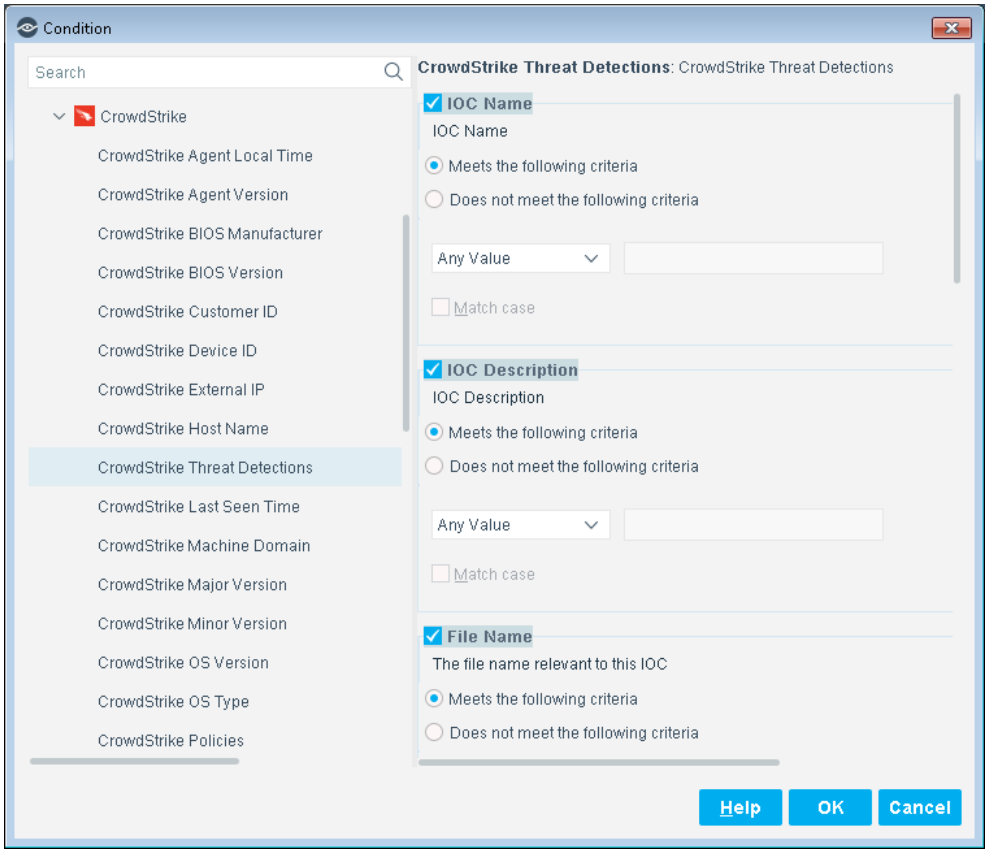
- Scan potentially compromised Windows endpoints for IOCs reported by the CrowdStrike Module.
- Remediate infected endpoints.

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.

Policy Properties

This section describes the properties that are available when you install the CrowdStrike Module.



To access CrowdStrike properties:

1. From the Policy Conditions dialog box, navigate to the Properties tree.
2. Expand the CrowdStrike folder in the Properties tree.
3. The following CrowdStrike properties are available. CounterACT populates and evaluates these properties based on information from the CrowdStrike cloud; endpoints are not directly queried. Refer to CrowdStrike Query API documentation for details and valid values for these data fields.

CrowdStrike Agent Local Time	CrowdStrike Agent Local Time on the endpoint.
CrowdStrike Agent Version	CrowdStrike Agent Version on the endpoint.
CrowdStrike BIOS Manufacturer	The BIOS manufacturer reported by CrowdStrike.

CrowdStrike BIOS Version	The BIOS version reported by CrowdStrike.
CrowdStrike Customer ID	The CrowdStrike Customer ID of the endpoint.
CrowdStrike Device ID	The CrowdStrike Device ID of the endpoint.
CrowdStrike Endpoint Status	The endpoint status in CrowdStrike.
CrowdStrike External IP	The external IP reported by CrowdStrike.
CrowdStrike Host Name	The host name reported by CrowdStrike.
CrowdStrike Last Seen Time	Time of CrowdStrike's last contact with the endpoint.
CrowdStrike Machine Domain	The machine domain reported by CrowdStrike.
CrowdStrike Major Version	The major version of the endpoint OS reported by CrowdStrike.
CrowdStrike Minor Version	The minor version of the endpoint OS reported by CrowdStrike.
CrowdStrike OS Type	The OS type reported by CrowdStrike.
CrowdStrike OS Version	Operating System Version detected by the CrowdStrike Agent.
CrowdStrike Policies	CrowdStrike policies that may be applied to the endpoint.
CrowdStrike Product Type Description	CrowdStrike Product Type Description.
CrowdStrike Site Name	CrowdStrike Site Name.
CrowdStrike System Manufacturer	CrowdStrike System Manufacturer.
CrowdStrike System Product Name	CrowdStrike System Product Name.
CrowdStrike Threat Detections	IOCs reported by CrowdStrike for the endpoint.

Using the CrowdStrike Extended Module

Once the CrowdStrike Module has been configured, you can view and manage the devices from Asset Inventory view in the CounterACT Console. This provides activity information, accurate at the time of the poll, on endpoints based on certain instances' properties. The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

To access the Asset Inventory tab:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. In the Views pane, expand the **CrowdStrike** folder.

If you did not configure to show the property in the Asset Inventory tab, your CrowdStrike properties will not display in the Views pane of the Asset Inventory tab.

3. In the left pane, select the **CrowdStrike** icon to expand it and then select any of the items in the list to view its properties.
4. Check that the properties match the configuration requirements.

To access the Home tab:

1. In the CounterACT Console, select the **Home** tab.
2. In the Views tree, expand **Policies** and then select **CrowdStrike**.
3. Select an item in the Detections pane. The Profile, Compliance and All policies tabs display the information related to the selected host.

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 Extension 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**.

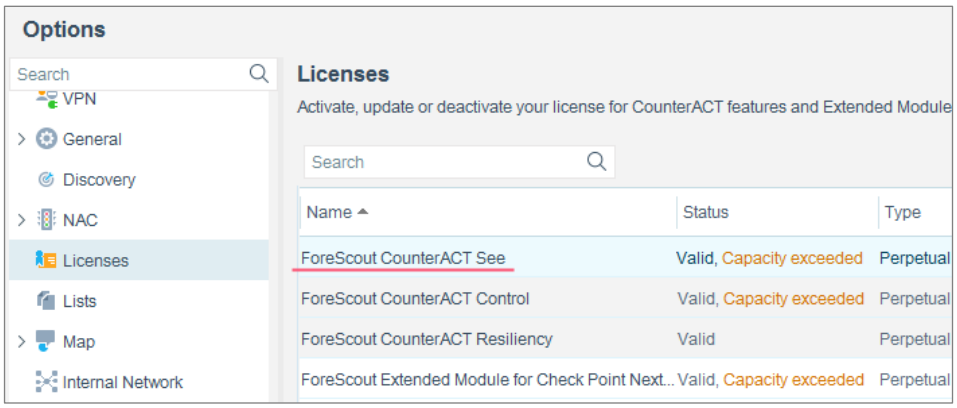
Documentation Portal

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

2018-04-10 09:21