Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2019 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.
Table of Contents

About CrowdStrike Integration ........................................................................................................ 5
  About Certification Compliance Mode .......................................................................................... 5
  Advanced Threat Detection with the IOC Scanner Plugin ............................................................. 5

About This Module .......................................................................................................................... 7
  Use Cases ..................................................................................................................................... 7
  CrowdStrike Falcon Agent Hygiene Policy ..................................................................................... 7
  Policy-Based Response to IoA from CrowdStrike ........................................................................ 7
  Restricting Compromised Endpoints Not Managed by the Forescout Platform ......................... 8
  How it Works ................................................................................................................................. 8
  Known Limitations ....................................................................................................................... 9
  What to Do ................................................................................................................................. 10
  Additional CrowdStrike Documentation ...................................................................................... 10

Requirements ................................................................................................................................ 10
  Forescout Requirements ............................................................................................................... 10
  Forescout eyeExtend (Extended Module) Licensing Requirements ............................................. 11
  Per-Appliance Licensing Mode .................................................................................................... 11
  Flexx Licensing Mode .................................................................................................................. 12
  More License Information ........................................................................................................... 13
  CrowdStrike Requirements ......................................................................................................... 13
  Network Requirements ................................................................................................................. 13

Install the Module ............................................................................................................................ 14

Configure the Module ...................................................................................................................... 14
  Configure CrowdStrike as an IOC Subscriber ............................................................................. 20

Test the Module Configuration ....................................................................................................... 21

Create CrowdStrike Policies Using Templates ................................................................................ 21
  Create a CrowdStrike Agent Hygiene Policy ................................................................................ 21
  Create a CrowdStrike Endpoint Threat Hunting Policy ................................................................. 25
  Create a CrowdStrike Network Threat Hunting Policy ................................................................. 29
  Create a CrowdStrike Visibility Beyond Campus Policy ............................................................. 34
  How Devices are Detected and Handled ....................................................................................... 38

Create Custom CrowdStrike Policies ........................................................................................... 39
  Policy Properties .......................................................................................................................... 39

Working with Forescout eyeExtend for CrowdStrike ................................................................... 41

Core Extension Information .......................................................................................................... 42

Additional Forescout Documentation ............................................................................................ 42
  Documentation Downloads .......................................................................................................... 42
Documentation Portal ................................................................. 43
Forescout Help Tools.................................................................... 43
About CrowdStrike Integration

Forescout 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 integration of the Forescout platform 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 the distribution of endpoint management software, which improves the user experience and increases operational efficiency.

The goal of Forescout eyeExtend for CrowdStrike 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.

The integration of the Forescout platform with CrowdStrike lets you:

- 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
- Employ combined automated response options to quarantine or remediate infected devices

Together, the Forescout platform 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. The Forescout platform also helps continually enforce device compliance upon network access. See Use Cases for more details.

About Certification Compliance Mode

Forescout eyeExtend for CrowdStrike supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

Advanced Threat Detection with the IOC Scanner Plugin

This module works with the Forescout 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 the Forescout platform 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 the Forescout platform, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

• **ATD Stage 1 (Forescout eyeExtend for CrowdStrike) – 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 Forescout 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 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 the Forescout platform's ATD response.

- **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, refer to the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide*.

**About This Module**

Forescout eyeExtend for CrowdStrike supports 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 Forescout platform 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 Forescout eyeExtend for CrowdStrike.

**CrowdStrike Falcon Agent Hygiene Policy**

You can define a Forescout platform 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. See *Create a CrowdStrike Agent Hygiene Policy*.

**Policy-Based Response to IoA from CrowdStrike**

When CrowdStrike identifies malware or other malicious behavior known as Indicators of Attack (IoA), the Forescout platform is notified in near real-time and performs an action based on the risk level of the issue discovered. See *Create a CrowdStrike Endpoint Threat Hunting Policy*. 
Restricting Compromised Endpoints Not Managed by the Forescout Platform

The Forescout platform can restrict network access to non-corporate or other unmanaged endpoints based on IOCs reported to it by CrowdStrike. See [Create a CrowdStrike Endpoint Threat Hunting Policy](#) or implement other policies provided by the IOC Scanner Plugin.

How it Works

The following CrowdStrike components are required for this integrated solution:

- **CrowdStrike Cloud platform** – The Forescout platform addresses the query API exposed by the platform to retrieve endpoint information.
- **CrowdStrike Streaming API** – The Forescout platform subscribes to CrowdStrike IOC and IoT streams.
- **CrowdStrike Query API** – Lets you create custom 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 running or previously run processes, and set the status of threat detections in Falcon Host.

The following Forescout platform components support the integration:

- **Forescout eyeExtend for CrowdStrike** – This module handles communication with CrowdStrike and provides the properties, actions, and policies described in this guide.
- **IOC Scanner Plugin** – This plugin is the clearinghouse for IOC information and related functionality in the Forescout platform. When Forescout eyeExtend 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 the Forescout platform. 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 the Forescout platform to the CrowdStrike cloud can be configured.
- The Forescout platform does not communicate directly with the CrowdStrike Falcon agent on endpoints.
This deployment method scales efficiently and allows tuning of traffic loads.

**Known Limitations**

Detection event volume/velocity varies widely depending on the size of the customer environment. Typically, the volume is pretty low, and even a 100K endpoint environment is not 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 attack).

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 that CrowdStrike has started to throttle event detection would be if the Forescout platform receives an event hours or days after a detection. The following are examples of when CrowdStrike would throttle detection events:
If CrowdStrike identifies the same pattern/detection on the same host and process, it triggers a detection only once (not over and over).

The same pattern/detection and host (without the same process) triggers, at most, once every 5 minutes.

When the maximum of 1,000 detections per day on a single endpoint is exceeded (a clear indication that the host should be investigated).

What to Do

Perform the following steps to set up this integration:

1. Verify that requirements are met. See Requirements for details.
3. Configure the Module.
4. (Optional) Configure CrowdStrike as an IOC Subscriber.
5. Create policies that implement integration Use Cases. See Create CrowdStrike Policies Using Templates.
6. When the configurations have been tested and the policies created, you are ready to Working with Forescout eyeExtend for CrowdStrike.

Additional CrowdStrike Documentation

Refer to CrowdStrike online documentation for more information about the CrowdStrike solution:
https://falcon.crowdstrike.com/support/documentation

Requirements

Verify that the following requirements are met:

- Forescout Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements
- CrowdStrike Requirements
- Network Requirements

Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.1.
- A module license for Forescout eyeExtend for CrowdStrike. See Forescout eyeExtend (Extended Module) Licensing Requirements.
• Core Extensions Module version 1.1, with the IOC Scanner Plugin running (see Core Extension Information).

Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend product requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

• Per-Appliance Licensing Mode
• Flexx Licensing Mode

To identify your licensing mode:

• From the Console, select Help > About ForeScout.

Per-Appliance Licensing Mode

When installing the module you are provided with a 90-day demo 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.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

Demo license extension requests and permanent license requests are made from the 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 Forescout 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 the Forescout platform. 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 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.

Flexx Licensing Mode
When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend products. After the initial license file has been activated, you can
update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend products. For more information on obtaining eyeExtend licenses, contact your Forescout sales 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 eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module, but does not exceed the capacity of the Forescout eyeSight license.

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

**More License Information**

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the Forescout Administration Guide.
- **Flexx Licensing.** Refer to the Flexx Licensing How-to Guide.

You can also contact your Forescout sales representative for more information.

**CrowdStrike Requirements**

This 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 ensure good performance, each connecting CounterACT device should handle no more than 40,000 devices on the network. Create multiple connecting CounterACT device 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 Plugin. See Forescout 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 - Flexx Licensing Mode
   To identify your licensing mode, select Help > About ForeScout from the Console.
2. Download the module .fpi file.
3. Save the file to the machine where the Console is installed.
4. Log into the 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.

Configure the Module

After Forescout eyeExtend for CrowdStrike is installed, configure the module to ensure that the Forescout platform can communicate with the CrowdStrike cloud.

To add a connection:
1. In the Console, select Options from the Tools menu.
2. Select CrowdStrike from the Options pane.
3. In the CrowdStrike pane, select **Add**.

4. Configure the connection to the CrowdStrike cloud as follows:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter the name of the CrowdStrike connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter additional text to help users identify this CrowdStrike connection.</td>
</tr>
<tr>
<td><strong>Cloud URL</strong></td>
<td>A default URL to the CrowdStrike cloud access point is displayed, however, you can modify the URL for your needs.</td>
</tr>
</tbody>
</table>
### Contact CrowdStrike Support

Contact CrowdStrike Support to get a Query API username and password for accessing the CrowdStrike server.

### Verify Password

Re-enter the password to verify it.

### Send IOCs to CrowdStrike

Select this option to send user-defined third-party generated IOCs to CrowdStrike for threat endpoint hunting.

### Validate CrowdStrike Server Certificate

Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:

- **Self-signed server certificate** – the server certificate must be installed on the CounterACT Appliance
- **Certificate Authority (CA) signed server certificate** – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance

Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*.

### 5. Select **Next**.

![Add CrowdStrike Connection - Step 2 of 5](image)
6. Enter the credentials you received from CrowdStrike to access the streaming API exposed by this cloud connection.

<table>
<thead>
<tr>
<th><strong>Streaming API URL</strong></th>
<th>A default URL to the CrowdStrike Streaming API is displayed, however, you can modify the URL for your needs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Streaming API UUID</strong></td>
<td>Contact CrowdStrike Support to get a Streaming API Universally Unique Identifier (UUID) and password for accessing the CrowdStrike server.</td>
</tr>
<tr>
<td><strong>Streaming API Password</strong></td>
<td>Re-enter the password.</td>
</tr>
</tbody>
</table>

Sometimes, the CrowdStrike Cloud receives threat information from its agents, but is slow to forward that threat information to the Forescout platform. Once that information is forwarded to the Forescout platform, it acts on the threats as per its configured policies.

7. Select **Next**.

To ensure good performance, each connecting CounterACT device should handle no more than 40,000 devices. Create multiple connecting CounterACT device clusters if you have more devices on the network.
8. From the **Connecting CounterACT Device** drop-down list, select the device through which other CounterACT devices will communicate with this CrowdStrike cloud instance. The specified device is the only CounterACT device that communicates directly with this cloud instance and 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 the ForeScout platform 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 be assigned to only 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 explicitly assigned to another CrowdStrike instance are assigned to 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 option is selected by default.

10. Select **Next**.
When your environment routes Internet communications through a proxy server, you 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) When using a proxy server with Basic Authentication, configure the proxy server settings as follows:

<table>
<thead>
<tr>
<th>Use Proxy Server</th>
<th>Select this option to use a proxy server to communicate with the CrowdStrike Cloud Platform.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>Enter the IP address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Select the port used to communicate with the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Username</td>
<td>(Optional) For proxies using Basic Authentication, enter the proxy server’s login name for an authorized account defined on the proxy.</td>
</tr>
<tr>
<td>Proxy Server Password</td>
<td>(Optional) For proxies using Basic Authentication, enter the proxy server’s login password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Verify the proxy server’s password.</td>
</tr>
</tbody>
</table>

12. Select Next.

13. In the API Rate Limit field, set 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 the Forescout platform.
Verify that an account with the correct permissions is defined for the Forescout platform in the CrowdStrike cloud.

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

The best practice is to perform a test after setting up a connection. See Test the Module Configuration.

**Configure CrowdStrike as an IOC Subscriber**

The IOC Scanner Plugin lets the Forescout platform share IOC information with external platforms.

When Forescout eyeExtend for CrowdStrike 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 Forescout IOC streams. CrowdStrike is displayed in the IOC Subscriptions tab of the IOC Scanner Plugin configuration pane.
By default, IOCs are NOT forwarded to the CrowdStrike Cloud. Once configured, these subscriptions are configured to share all IOC information from the Forescout platform. In some environments it may be necessary to use settings that restrict the type or volume of IOCs that are shared by the Forescout platform.

For more information about IOC Scanner, refer to the Forescout Core Extensions Module: IOC Scanner Plugin 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 test results are displayed in the CrowdStrike Module Configuration Test dialog box.

2. Select Close.

Create CrowdStrike Policies Using Templates

This section describes how to use the CrowdStrike policy templates provided with this module to create policies to detect and manage endpoints. Refer to the following sections:

- Create a CrowdStrike Agent Hygiene Policy
- Create a CrowdStrike Endpoint Threat Hunting Policy
- Create a CrowdStrike Network Threat Hunting Policy
- Create a CrowdStrike Visibility Beyond Campus Policy

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

Create a CrowdStrike Agent Hygiene Policy

The CrowdStrike Agent Hygiene Policy template generates a policy that detects whether Windows endpoints are running the CrowdStrike Falcon agent. The purpose of the Agent Hygiene policy is to ensure 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.
Endpoints are classified in this policy based on the CrowdStrike host ID. The IP address, MAC address, and hostname are used to retrieve the CrowdStrike host ID from the Falcon cloud and classify the endpoints in this policy.

The main rule of this policy detects endpoints that are managed by the Forescout platform 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 *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 create a policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the CrowdStrike folder and select **CrowdStrike Agent Hygiene**.
4. Select **Next**.
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.
   - 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.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

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 is displayed in the Scope pane.
9. Select **Next**.

![Policy Wizard - Step 4 of 5](image)

The main rule of this policy detects Windows endpoints that are managed using Remote Inspection. For details on the default policy logic, see **How Devices are Detected and Handled**.

10. (Optional) Add conditions and actions to the main rule as required. For details, see **Policy Properties**.
11. Select **Next**.
12. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.

13. Add conditions and actions as required. For details, see Policy Properties.

   You can also edit the conditions and actions in the Main Rule and Sub-Rules panes when you edit an existing policy.

14. Select OK. Repeat for additional sub-rules as required.

15. In the Sub-Rules pane, select Finish.

16. In the Console, select Apply to save the policy.

Create a CrowdStrike Endpoint Threat Hunting Policy

The CrowdStrike Endpoint Threat Hunting Policy template provides a basic structure for most coordinated remediation scenarios involving CrowdStrike and the Forescout platform. It generates a policy that detects endpoints based on threats recently reported to the Forescout platform by CrowdStrike. Based on the policy conditions, the Forescout platform can take actions to remediate or restrict these endpoints. The compromised endpoint is contained and CrowdStrike generates threat intelligence and shares the IOCs with the Forescout platform via the Create a CrowdStrike Network Threat Hunting Policy.

The main rule of this policy uses the CrowdStrike Threat Detection property to select all endpoints for which the Forescout platform received a CrowdStrike Threat Detection report within the last week. The sub-rules detect endpoints based on the severity of the reported threat. Optional actions provide additional ways the Forescout platform 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 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 create a policy:

1. Log in to the Console and select Policy.
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.
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.
   - 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.

   Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.
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 is displayed in the Scope pane.

9. Select Next.

The main rule of this policy uses the CrowdStrike Threat Detection property to select all endpoints for which the Forescout platform received a CrowdStrike Threat Detection report within the last week. For details on the default policy logic, see How Devices are Detected and Handled.

10. (Optional) Add conditions and actions to the main rule as required. For details, see Policy Properties.

11. Select Next.
The sub-rules of the CrowdStrike Endpoint Threat Hunting policy list the items the Forescout platform is to check when applying the main rule.

12. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.

13. Add conditions and actions as required. For details, see Policy Properties.

   You can also edit the conditions and actions in the Main Rule and Sub-Rules panes when you edit an existing policy.

14. Select OK. Repeat for additional sub-rules as required.

15. In the Sub-Rules pane, select Finish.

16. In the Console, select Apply to save the policy.

Create a CrowdStrike Network Threat Hunting Policy

The purpose of the CrowdStrike Network Threat Hunting Policy 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

The Network Threat Hunting Policy 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 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 the Forescout platform and blocked via network firewall or network quarantine.

When a new device enters the network and the Forescout platform identifies the device as a guest. Based on policy condition(s), the Forescout platform monitors network connections and DNS queries for IOAs or IOCs. The Forescout platform 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 this policy uses the CrowdStrike Threat Detection property to detect IOCs on networks that the Forescout platform 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 the Forescout platform 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 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 create a policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the CrowdStrike folder and select **CrowdStrike Network Threat Hunting**.

<table>
<thead>
<tr>
<th>Policy Manager</th>
<th>Search</th>
<th>Show subfolder policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Category</td>
<td>Status</td>
</tr>
<tr>
<td>AllProperties</td>
<td>Note</td>
<td>Complete</td>
</tr>
<tr>
<td>CrowdStrike Agent Hygiene</td>
<td>Compliance</td>
<td>Complete</td>
</tr>
<tr>
<td>CrowdStrike Endpoint Threat Hunting</td>
<td>Compliance</td>
<td>Complete</td>
</tr>
<tr>
<td>CrowdStrike Network Threat Hunting</td>
<td>Compliance</td>
<td>Complete</td>
</tr>
<tr>
<td>Win-IOC Detected - Linux</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Macintosh</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Mobile Device</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Network Device</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Printer</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Windows</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - Other</td>
<td>Not Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - CounterACT Monitor</td>
<td>Compliant</td>
<td></td>
</tr>
<tr>
<td>Win-IOC Detected - CrowdStrike Monitor</td>
<td>Compliant</td>
<td></td>
</tr>
</tbody>
</table>

Version 1.2
4. Select **Next**.

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`.
   - 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.

Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

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 is displayed in the Scope pane.

9. Select **Next**.
The main rule of this policy uses the CrowdStrike Threat Detection property to select all endpoints for which the Forescout platform received a CrowdStrike Threat Detection report within the last week. For details on the default policy logic, see [How Devices are Detected and Handled](#).

10. (Optional) Add conditions and actions to the main rule as required. For details, see [Policy Properties](#).

11. Select **Next**.
12. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.

13. Add conditions and actions as required. For details, see Policy Properties.

   - You can also edit the conditions and actions in the Main Rule and Sub-Rules panes when you edit an existing policy.

14. Select OK. Repeat for additional sub-rules as required.

15. In the Sub-Rules pane, select Finish.

16. In the Console, select Apply to save the policy.

Create a CrowdStrike Visibility Beyond Campus Policy

The CrowdStrike Visibility Beyond Campus Policy 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 the Forescout platform. The compromised endpoint is contained and CrowdStrike generates threat intelligence and shares the IOCs or IOAs with the Forescout platform via the Network Threat Hunting template.

The main rule of this policy detects endpoints that are managed by the Forescout platform 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 *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 create a policy:**

1. Log in to the Console and select **Policy**.
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**.
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.
   - 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.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

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 is displayed in the Scope pane.

9. Select **Next**.

![Policy Wizard Step 4](image)

The main rule of this policy checks whether the network type of endpoints that are being managed are part of a group. For details on the default policy logic, see **How Devices are Detected and Handled**.

10. (Optional) Add conditions and actions to the main rule as required. For details, see **Policy Properties**.

11. Select **Next**.
In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.

Add conditions and actions as required. For details, see Policy Properties.

You can also edit the conditions and actions in the Main Rule and Sub-Rules panes when you edit an existing policy.

Select OK. Repeat for additional sub-rules as required.

In the Sub-Rules pane, select Finish.

In the Console, select Apply to save the policy.

How Devices are Detected and Handled

Policy rules instruct the Forescout platform 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.

You can edit the main rule and sub-rules in the main rule and sub-rules panes when you create or edit a policy.
Create Custom CrowdStrike Policies

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

**Policies and Rules, Conditions and Actions**

Forescout platform policies contain a series of rules. Each rule includes:

- Conditions based on host property values. The Forescout platform 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 Forescout 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 Forescout eyeExtend for CrowdStrike.
- Remediate infected endpoints.

**To create a custom policy:**

1. In the Console, select **Policy**. 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 Forescout eyeExtend for CrowdStrike.

The Forescout platform 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.

**To access CrowdStrike properties:**

1. From the Policy Conditions dialog box, go to the Properties tree.
2. Expand the CrowdStrike folder in the Properties tree.
The following CrowdStrike properties are available:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Agent Local Time</td>
<td>CrowdStrike Agent Local Time on the endpoint.</td>
</tr>
<tr>
<td>CrowdStrike Agent Version</td>
<td>CrowdStrike Agent Version on the endpoint.</td>
</tr>
<tr>
<td>CrowdStrike BIOS Manufacturer</td>
<td>The BIOS manufacturer reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike BIOS Version</td>
<td>The BIOS version reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike Customer ID</td>
<td>The CrowdStrike Customer ID of the endpoint.</td>
</tr>
<tr>
<td>CrowdStrike Device ID</td>
<td>The CrowdStrike Device ID of the endpoint.</td>
</tr>
<tr>
<td>CrowdStrike Endpoint Status</td>
<td>The endpoint status in CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike External IP</td>
<td>The external IP reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike Host Name</td>
<td>The host name reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike Last Seen Time</td>
<td>Time of CrowdStrike's last contact with the endpoint.</td>
</tr>
<tr>
<td>CrowdStrike Machine Domain</td>
<td>The machine domain reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike Major Version</td>
<td>The major version of the endpoint OS reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike Minor Version</td>
<td>The minor version of the endpoint OS reported by CrowdStrike.</td>
</tr>
<tr>
<td>CrowdStrike OS Type</td>
<td>The OS type reported by CrowdStrike.</td>
</tr>
</tbody>
</table>
Working with Forescout eyeExtend for CrowdStrike

Once Forescout eyeExtend for CrowdStrike has been configured, you can view and manage the devices from Asset Inventory view in the Console. This provides activity information, accurate at the time of the poll, on endpoints based on specific 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:**

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **CrowdStrike** folder.
   
   - *If you did not configure the module to show the property in the Asset Inventory, your CrowdStrike properties are not displayed in the Views pane.*
3. In the Views pane, select the **CrowdStrike** icon to expand it and then select any item in the list to view its properties.
4. Check that the properties match the configuration requirements.

**To access the Home tab:**

1. In the Console, select **Home**.
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.

<table>
<thead>
<tr>
<th><strong>CrowdStrike OS Version</strong></th>
<th>Operating System Version detected by the CrowdStrike Agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CrowdStrike Policies</strong></td>
<td>CrowdStrike policies that may be applied to the endpoint.</td>
</tr>
<tr>
<td><strong>CrowdStrike Product Type Description</strong></td>
<td>CrowdStrike Product Type Description.</td>
</tr>
<tr>
<td><strong>CrowdStrike Site Name</strong></td>
<td>CrowdStrike Site Name.</td>
</tr>
<tr>
<td><strong>CrowdStrike System Manufacturer</strong></td>
<td>CrowdStrike System Manufacturer.</td>
</tr>
<tr>
<td><strong>CrowdStrike System Product Name</strong></td>
<td>CrowdStrike System Product Name.</td>
</tr>
<tr>
<td><strong>CrowdStrike Threat Detections</strong></td>
<td>IOCs reported by CrowdStrike for the endpoint.</td>
</tr>
</tbody>
</table>
Refer to *Working on the Console > Working with Inventory Detections* in the *Forescout Administration Guide* or the Console Online Help for information about working with the Asset Inventory.

**Core Extension Information**

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

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- DHCP Classifier Plugin
- External Classifier Plugin
- Flow Analyzer Plugin
- Flow Collector
- IOC Scanner Plugin
- NBT Scanner Plugin
- Packet Engine
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web Client Plugin
- IoT Posture Assessment Engine

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

**Additional Forescout Documentation**

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

**Documentation Downloads**

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Portal](#)

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.
**Forescout Resources Page**

The Forescout Resources Page provides links to the full range of technical documentation.

**To access the Forescout Resources Page:**

**Product Updates Portal**

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

**To access the Product Updates Portal:**

**Customer Portal**

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

**To access documentation on the Forescout Customer Portal:**
- Go to [https://Forescout.force.com/support/](https://Forescout.force.com/support/) and select **Downloads**.

**Documentation Portal**

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

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

**To access the Documentation Portal:**
- Go to [https://updates.forescout.com/support/files/counteract/docs_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/) and use your customer support credentials to log in.

**Forescout Help Tools**

Access information directly from the Console.

*Console Help Buttons*

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

*Forescout Administration Guide*

- Select **Forescout Help** from the **Help** menu.
**Plugin Help Files**
- After the plugin is installed, select **Tools > Options > Modules**, select the plugin and then select **Help**.

**Online Documentation**
- Select **Online Documentation** from the **Help** menu to access either the [Forescout Resources Page](#) (Flexx licensing) or the [Documentation Portal](#) (Per-Appliance licensing).