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

Legal Notice

© 2020 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 the Carbon Black Integration** ................................................................. 5  
Advanced Threat Detection with the IOC Scanner Plugin ........................................ 5  
Use Cases ........................................................................................................... 6  
Carbon Black Agent Compliance ........................................................................ 6  
Carbon Black Response Accelerate and Automate Policy-Driven Threat Response .................................................................................................................. 6  
Carbon Black and Forescout Threat Intelligence Sharing .................................... 6  
Additional Carbon Black Features ....................................................................... 7  
Trusted Software Publisher .................................................................................. 7  
Additional Carbon Black Documentation .............................................................. 7  

**About This Module** .......................................................................................... 7  

**Concepts, Components, and Considerations** ................................................. 8  
Concepts ............................................................................................................. 8  
Deployment Options ........................................................................................... 8  
Components ........................................................................................................ 10  
Considerations .................................................................................................... 11  

**What to Do** ..................................................................................................... 11  

**Requirements** ............................................................................................... 11  
Forescout Requirements ..................................................................................... 12  
Carbon Black Requirements ............................................................................. 12  
About Support for Dual Stack Environments ...................................................... 12  

**Forescout eyeExtend (Extended Module) Licensing Requirements** .......... 12  
Per-Appliance Licensing Mode .......................................................................... 13  
Flexx Licensing Mode ......................................................................................... 14  
More License Information .................................................................................. 15  

**Install the Module** ........................................................................................... 15  

**Configure the Module** ..................................................................................... 16  
Get an Authorization Token .................................................................................. 16  
Add a Carbon Black Response Connection ....................................................... 17  
Configure Syslog Messages from Carbon Black Response Server ................. 21  
Add a Carbon Black Protection Connection ..................................................... 21  
Test Your Carbon Black Configurations ............................................................ 25  

**Create Carbon Black Policies Using Templates** ............................................. 25  
Create a Carbon Black Agents Installed Policy .................................................. 25  
How Devices Are Detected and Handled ......................................................... 29  
Create a Carbon Black Endpoint Threat Hunting Policy ................................... 30  
How Devices Are Detected and Handled ......................................................... 33  

Carbon Black Network Threat Hunting Policy .......................................................... 34
How Devices are Detected and Handled ............................................................... 37

Create Custom Carbon Black Policies ................................................................. 37
Policy Properties .................................................................................................. 38
Carbon Black Protection Agent Properties ......................................................... 38
Carbon Black Protection Computer Properties ................................................. 39
Carbon Black Response Computer Vitals ......................................................... 40
Carbon Black Response Sensor Vitals ............................................................... 41
Policy Actions ..................................................................................................... 43

Working with Forescout eyeExtend for Carbon Black ........................................... 43
Access the Asset Inventory .................................................................................... 43
Access the Home Tab ......................................................................................... 44

Additional Forescout Documentation ................................................................. 45
Documentation Downloads ................................................................................... 45
Documentation Portal ............................................................................................ 46
Forescout Help Tools ............................................................................................. 46
About the Carbon Black Integration

Carbon Black offers threat detection capabilities from the network core to the endpoint, enhancing endpoint visibility and enabling a flexible and adaptive defense against known and unknown threats.

This integration of Carbon Black with the Forescout platform enhances Carbon Black’s abilities to:

- Verify Carbon Black Response and Protection agents are installed, operational and communicating properly with their respective Carbon Black instances.
- Provide comprehensive visibility across network-connected devices including BYOD, guest, IoT and managed devices.
- Share threat intelligence across solutions for joint threat hunting for Indicators of Compromise (IOCs) across endpoint and network tiers.

The Carbon Black agent installed on endpoints provides threat and endpoint information that complements information detected by the Forescout platform. Endpoints suspected of infection can be isolated, and remediation actions can be initiated automatically instead of requiring human intervention, allowing corporate security teams to deal with other threats in near real-time.

For more information, see Concepts, Components, and Considerations.

Advanced Threat Detection with the IOC Scanner Plugin

Forescout eyeExtend for Carbon Black works with the IOC Scanner Plugin, the Forescout platform’s action center for Advanced Threat Detection (ATD) and response. The IOC Scanner Plugin provides:

- A centralized repository of all threats and their IOCs reported to the Forescout platform by third-party endpoint detection and response (EDR), and other threat prevention systems, or added manually.
- Mechanisms that scan all Windows endpoints for threat and IOC information reported to 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 Carbon Black): Carbon Black Endpoint Threat Hunting Policy Template:** Carbon Black 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 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. The IOC Scanner parses the threat to 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**, Carbon Black Network Threat Hunting default policy: The IOC Scanner Plugin detects endpoints with IOCs associated with recently reported threats.

For more information about IOC-based threat detection and remediation, see the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide.

**Use Cases**

This section describes important use cases supported by Forescout eyeExtend for Carbon Black. To understand how this module helps you achieve these goals, see About This Module.

**Carbon Black Agent Compliance**

The Forescout platform improves security hygiene by verifying that Carbon Black agents are installed, running, and operating properly on supported corporate endpoints. The Forescout platform detects not-yet-enrolled devices and incorrectly functioning agents, and triggers workflows to enforce client-side and server-side compliance. See Carbon Black Agents Installed Policy.

**Carbon Black Response Accelerate and Automate Policy-Driven Threat Response**

When Carbon Black identifies malware or malicious behavior, it informs the Forescout platform in near real-time. Based on threat severity and your policy, the Forescout platform can automatically take appropriate actions, such as restricting, isolating or blocking compromised devices, and initiating remediation workflows. The combination of Carbon Black host actions and the Forescout platform’s network actions lets you reduce your mean time to respond (MTTR) and limit the impact of threats. See Carbon Black Endpoint Threat Hunting Policy Template.

**Carbon Black and Forescout Threat Intelligence Sharing**

Carbon Black identifies malware and IOCs through advanced techniques and notifies the Forescout platform upon detection. The Forescout platform leverages this threat intelligence to monitor the network for IOCs including unmanaged connected systems such as BYOD, guest and IoT devices as well as network infrastructure. Based on your policy, the Forescout platform can restrict, isolate, or block network access for compromised devices. See Carbon Black Network Threat Hunting Policy Template.
Additional Carbon Black Features

Trusted Software Publisher

During Forescout eyeExtend for Carbon Black configuration, you can approve trusted publishers, Forescout Technologies Inc. (with period) and Forescout Technologies Inc (without period). Alternately, you can remove these publishers' approval in the Carbon Black Protection server configuration. See Add a Carbon Black Protection Connection.

Additional Carbon Black Documentation

Refer to Carbon Black online documentation for more information about the Carbon Black solution:

https://developer.carbonblack.com
https://community.carbonblack.com/
https://www.carbonblack.com/resources/support/

About This Module

Forescout eyeExtend for Carbon Black lets you:

- Configure a dedicated Connecting Appliance for communication with Carbon Black Response and Carbon Black Protection, in order to aggregate and minimize traffic.
- Configure Forescout eyeExtend for Carbon Black to communicate with the Carbon Black Response and Carbon Black Protection servers.
- Configure the proxy server to be used for communicating with Carbon Black Response and Carbon Black Protection servers.
- Test the Connecting Appliance’s connection to Carbon Black Response and Carbon Black Protection servers, and view the information collected from the test, such as the number of sensors installed and visible.
- Configure the module to automatically add IOCs from Carbon Black to the IOC Scanner table upon detection.
- View IOCs related to threats reported by Forescout eyeExtend for Carbon Black and automatically added to the IOC repository. These IOCs are used by the IOC Scanner Plugin for Advanced Threat Detection (ATD). Refer to the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.
- Use the Inventory tab to display all threats and the corresponding endpoints on which they have been found.
- Enforce Carbon Black sensors installation and running on visible machines through a HTTP redirect action. Sensors (agents) can also be downloaded.
• Observe and make use of endpoint information collected through Carbon Black sensors through endpoint properties and use them for policy creation.

To use the module, you should have a solid understanding of Carbon Black concepts, functionality, and terminology, and an understanding of how policies and other basic features work. Additionally, you should have a solid understanding of how to leverage threat intelligence distributed by IOCs.

**Concepts, Components, and Considerations**

This section provides a basic overview of Carbon Black and the Forescout platform architecture:

- **Concepts** – basic integration concepts and deployment options.
- **Components** – devices in your network that participate in the integration.
- **Considerations** – setup details and common network structure issues to keep in mind when you implement this module.

**Concepts**

This integration lets you connect one or more CounterACT® Appliances or an Enterprise Manager to a unique Carbon Black deployment. When multiple CounterACT Appliances are mapped to a single Carbon Black deployment, they are grouped into a connecting CounterACT Appliance cluster. This Appliance cluster handles communication between the Carbon Black deployment and the rest of CounterACT Appliances in your environment.

Typically, there is only one Carbon Black production deployment per customer, but this can vary. This module is designed to work with one or more instance of each: Carbon Black Response and Carbon Black Protection. CounterACT Appliances are connected to this Carbon Black deployment using a logical URL or IP address, and user credentials.

**Deployment Options**

There are two topologies that can be used to set up multiple CounterACT Appliances in a Carbon Black deployment. For both topologies, a single CounterACT Appliance can be assigned to only one Carbon Black deployment.

> The actual deployments can be designed to combine both topologies to meet particular network requirements.
**Peer-to-Peer:** Each CounterACT Appliance communicates directly with a Carbon Black instance. This is a one-to-one relationship, where each CounterACT Appliance or Enterprise Manager initiates queries whenever required. This is often the topology for remote sites.

A **CounterACT Connecting Appliance cluster** is a group of CounterACT Appliances connecting to Carbon Black products through that logical URL or IP address associated with the Carbon Black server. There may be more than one connecting Appliance clusters in a company, typically set up by geographical region, business unit or functional separation. These are the middle men for other CounterACT Appliances reaching out to the Carbon Black instance.
Components

Key components of the Carbon Black service delivery platform include the Carbon Black Agent, Carbon Black Protection, and Carbon Black Response.

- **The Carbon Black Agent** resides on Carbon Black managed devices and acts as a universal policy engine capable of delivering multiple management services. A single Carbon Black Agent (Response or Protection) can execute a diverse and extensible array of management services that range from real-time client status reporting, to patch and software distribution, to security policy enforcement. The Carbon Black Agent also automatically notifies the Carbon Black Server and the Console of changes in managed device configuration, providing a real-time view of device status.

- **Carbon Black Response** is a precise IR and threat hunting solution, allowing you to get the answers you need fast. Carbon Black Response continuously records and captures all threat activity so you can hunt threats in real time, visualize the complete attack kill chain, and then respond and remediate attacks, quickly.

- **Carbon Black Protection** provides a proven application-control solution for enterprise endpoints and critical systems. With Carbon Black Protection, IT, compliance, infrastructure, and security teams establish automated software execution controls and protection policies that safeguard corporate and customer data.

Carbon Black Protection works with existing software distribution systems and reputation services to automate approval of trusted software and eliminate whitelist management. This level of control reduces the attack surface of highly-sensitive and targeted systems, such as desktops, laptops, servers, and point-of-sale devices, to eliminate system downtime due to malware and ensure regulatory compliance.

- **The Carbon Black Server** is a software-based package that provides a control center and repository for managed-system configuration data, software updates and patches, and other management information.

- **The Carbon Black Console**, which runs from the Carbon Black Server, provides an operations control center for Carbon Black administrators and includes graphical displays of device, group, and enterprise-wide device status and dashboards for executing management actions through the Carbon Black infrastructure. The console also includes reporting functions and templates that enable graphical and tabular views on infrastructure status.

- **CounterACT Appliances** are Appliances that manage or monitor devices based on their assigned network segments. These Appliances communicate with Carbon Black through the CounterACT Connecting Appliance cluster(s).

- **Devices on the network** are the hardware assets whose information needs to be exchanged between the Forescout platform and Carbon Black. When these devices enters the network, the Forescout platform monitors them and provides information.

In this context, when Forescout eyeExtend for Carbon Black is installed on CounterACT connecting Appliance clusters (each CounterACT Appliance individually), the operator can configure connection parameters to the Carbon Black instance. These connection parameters include an IP address or logical URL (for example,
mycompany.CarbonBlack-instance.CarbonBlack.com), user credentials (this user would have the right privileges/permissions to perform the necessary operations), proxy settings, and advanced settings.

Considerations

This section addresses additional considerations for working with Forescout eyeExtend for Carbon Black.

When deploying the Forescout platform on the same network as Carbon Black Protection, users should ensure that the Carbon Black Protection administrator whitelists HPS and/or Secure Connector batch (*.bat) files or the run-time directory to ensure that the Forescout platform can successfully interrogate an endpoint.

This module whitelists Forescout certificates (see Trusted Software Publisher), but this feature does not create whitelist exceptions for dynamically generated batch files (*.bat) because batch files are not signed by the Forescout platform.

For more information, refer to the Forescout Endpoint Module: HPS Inspection Engine Configuration Guide.

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See Requirements for details.
3. Define one of the following Carbon Black servers:
   - Define the target Carbon Black Response server and assign CounterACT Appliances to it. See Add a Carbon Black Response Connection for details.
   - Define the target Carbon Black Protection server and assign CounterACT Appliances to it. See Add a Carbon Black Protection Connection for details.
5. When the configurations have been tested and the policies created, you are ready to start Working with Forescout eyeExtend for Carbon Black.

Requirements

Verify that the following requirements are met:

- Forescout Requirements
Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Carbon Black. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- IOC Scanner Plugin version 2.4.

Carbon Black Requirements

Forescout eyeExtend for Carbon Black requires the following components:

- Carbon Black Response REST API version 1.0 with a running Appliance that has an established connection to the Internet.
- Carbon Black Protection Public API version 1.0 with a running Appliance that has an established connection to the Internet.

Forescout eyeExtend for Carbon Black works on the following platform:

- Carbon Black Event Forwarder version 3.2.0 – supports Syslog output type with TLS encryption & authentication support.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

About Support for Dual Stack Environments

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

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.

![About ForeScout Console: Enterprise Manager](image)

### 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.

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 cannot proceed unless you agree to the license agreement.

* The installation begins 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.
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 Carbon Black is installed on your targeted CounterACT Appliance, configure the module to ensure that the Forescout platform can communicate with the Carbon Black servers.

To complete the configuration of some of these connections, perform the following procedures:

- Get an Authorization Token
- Add a Carbon Black Response Connection
- Add a Carbon Black Protection Connection
- Test Your Carbon Black Configurations

Get an Authorization Token

This section describes how to get the authorization token for Carbon Black Response and Carbon Black Protection. The process varies according to the type of server (response or protection).

To get the token for a response server:

1. Log in to https://<IP address of Carbon Black Response server>/#/profile/token
2. Select CB ADMIN, and then select My Profile.
3. Select API Token.
4. When the API Token is displayed, copy it. You will need this API token when you Add a Carbon Black Response Connection.

To get the token for a protection server:

2. Select Administrator and then select login accounts.
3. Select Users and then select to View Details of a user.
4. Select the Show API token option.
5. When the API Token is displayed, copy it. You will need this API token when you Add a Carbon Black Protection Connection.
Add a Carbon Black Response Connection

This section describes how to connect your CounterACT Appliance to a Carbon Black Response server. This connection enables the communication of threat intelligence in the form of IOCs that identify malicious code.

**To add Carbon Black Response targets:**

1. In the Console, select **Options** from the Tools menu.
2. Select **Carbon Black** from the Options pane.
3. In the Carbon Black Response Connections tab, select **Add**.
4. Configure the connection as follows:

| Server Address | Enter a server address, the Fully Qualified Domain Name (FQDN) or the IPv4 address of the Carbon Black Response server that sends notifications to the CounterACT Appliance. The Carbon Black Response server must be able to handle the IP address ranges of its assigned CounterACT Appliances. |
| Server Port | Enter the port number used to access the Carbon Black Response server. By default, this is port 443. |
| API Token | Enter the access token to make web service API calls. You can generate the access key manually. |
| Validate Response 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.
6. Configure the CounterACT device assignment as follows:

<table>
<thead>
<tr>
<th>Connecting CounterACT Device</th>
<th>In an environment where more than one CounterACT device is assigned to a single Carbon Black server, the connecting CounterACT Appliance functions as a middle man between the Carbon Black server and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the Carbon Black server. Select the IP address of the connecting CounterACT device.</th>
</tr>
</thead>
</table>
| Assign specific devices     | This CounterACT Appliance is assigned to a Carbon Black server, but it does not communicate with it directly. All communication between the Carbon Black server and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the Carbon Black server.  
  - Select Available Devices and then select an item in the Available Devices list.  
  - Select Add. The selected device will send its requests to the Carbon Black server through the connecting Appliance. |
| Assign all devices by default | This is the connecting Appliance that CounterACT Appliances are assigned to if they are not explicitly assigned to another connection Appliance. Select this option to make this connecting Appliance the middle man for all CounterACT Appliances not assigned to another connecting Appliance. |

For more information, see Deployment Options.

7. Select Next.
8. Configure the proxy server settings as follows:

<table>
<thead>
<tr>
<th><strong>Use Proxy Server</strong></th>
<th>If your environment routes internet communications through proxy servers, select this box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Server</strong></td>
<td>Enter the IP address of the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Port</strong></td>
<td>Select the port number of the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Username</strong></td>
<td>Enter the administrator username used to access the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Password</strong></td>
<td>Enter the administrator password used to access the proxy server.</td>
</tr>
<tr>
<td><strong>Verify Proxy Server Password</strong></td>
<td>Re-enter the administrator password.</td>
</tr>
</tbody>
</table>

9. Select **Finish**. The server is listed in the Carbon Black Response Server tab.

You can configure syslog messages now (see [Configure Syslog Messages from Carbon Black Response Server](#)) or continue to the [Add a Carbon Black Protection Connection](#).

The best practice is to perform a Test after setting up a connection. See [Test Your Carbon Black Configurations](#).
Configure Syslog Messages from Carbon Black Response Server

(Optional) You can configure syslog messages from Carbon Black Response server to the Forescout platform.

**To configure syslog messages:**

1. Access the CB Response Server.
2. Open `cb-coreservices.conf`; the full path name is `/etc/rsyslog.d/cb-coreservices.conf`
3. Locate this line:
   ```
   if $programname == 'cb-notifications' then /var/log/cb/
   notifications/cb-allnotifications.log;CbLogFormatWithPID
   ```
   and add/or append the following text:
   ```
   & @<IP address of the connecting CounterACT appliance>:<UDP port>;
   CbLogFormatWithPID & ~.
   ```
4. The Port number (default is 514) should be the UDP port for incoming syslog messages configured on the Syslog Plugin. Refer to the *Forescout Core Extensions Module: Syslog Plugin Configuration Guide*.
5. Save the file.
6. Restart the Carbon Black Response syslog service by selecting `service rsyslog restart`.

Add a Carbon Black Protection Connection

(Optional) This section describes how to connect your CounterACT Appliance to a Carbon Black Protection server.

Whitelisting for files signed by Forescout Technologies Inc. is configured automatically.

**To add Carbon Black Protection targets:**

1. In the Console, select **Options** from the Tools menu.
2. Select **Carbon Black** from the Options pane.
3. Select the Carbon Black Response Protection tab and then select **Add**.
4. Configure the connection as follows:

<table>
<thead>
<tr>
<th><strong>Server Address</strong></th>
<th>Enter a server address, the Fully Qualified Domain Name (FQDN) or the IPv4 address of the Carbon Black Protection server that sends notifications to the CounterACT Appliance. The Carbon Black Protection server must be able to handle the IP address ranges of its assigned CounterACT Appliances.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Port</strong></td>
<td>Enter the port number used to access the Carbon Black Protection server. By default, this is port 443.</td>
</tr>
<tr>
<td><strong>API Token</strong></td>
<td>Enter the access token to make web service API calls. You can generate the access key manually.</td>
</tr>
</tbody>
</table>
| **Validate Protection 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. |
Trust Forescout Technologies Inc. as a Publisher

When selected (default), Forescout Technologies Inc. (with period) and Forescout Technologies Inc (without period) are approved as trusted publishers.
If you clear this selection, these publishers from approval.

5. Select **Next**.

6. Configure the CounterACT device assignment as follows:

**Connecting CounterACT Device**

In an environment where more than one CounterACT device is assigned to a single Carbon Black server, the connecting CounterACT Appliance functions as a middle man between the Carbon Black server and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the Carbon Black server.

Select the IP address of the connecting CounterACT device.

**Assign specific devices**

This CounterACT Appliance is assigned to a Carbon Black server, but it does not communicate with it directly. All communication between the Carbon Black server and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the Carbon Black server.

- Select **Available Devices** and then select an item in the Available Devices list.
- Select **Add**. The selected device will send its requests to the Carbon Black server through the connecting Appliance.
Assign all devices by default

This is the connecting Appliance that CounterACT Appliances are assigned to if they are not explicitly assigned to another connection Appliance.
Select this option to make this connecting Appliance the middle man for all CounterACT Appliances not assigned to another connecting Appliance.

For more information, see Deployment Options.

7. Select Next.

8. Configure the proxy server as follows:

<table>
<thead>
<tr>
<th><strong>Use Proxy Server</strong></th>
<th>If your environment routes internet communications through proxy servers, select this box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Server</strong></td>
<td>Enter the IP address of the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Port</strong></td>
<td>Select the port number of the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Username</strong></td>
<td>Enter the administrator username used to access the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Password</strong></td>
<td>Enter the administrator password used to access the proxy server.</td>
</tr>
<tr>
<td><strong>Verify Proxy Server Password</strong></td>
<td>Re-enter the administrator password.</td>
</tr>
</tbody>
</table>

9. Select Finish. The server is listed in the Carbon Black Protections Server tab.
The best practice is to perform a **Test** after setting up a connection. See **Test Your Carbon Black Configurations**.

## Test Your Carbon Black Configurations

The best practice is to perform a Test after setting up a connection.

**To test the configuration:**

1. Select **Options** and then select **Carbon Black**. The Carbon Black pane opens to the Carbon Black Response Connections tab.
2. Select a connection and then select **Test**.

   *If you configured the Carbon Black server without the correct administrator permissions, the Test will fail. To correct this, add administrator rights to your Carbon Black account.*

3. Check your configurations and re-test. If the test passed, repeat step 2 for any additional connections.
4. Select the Carbon Black Protection Connections tab.
5. Repeat steps 2 and 3.

The configuration of the Carbon Black Protection server is now complete.

## Create Carbon Black Policies Using Templates

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

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

This section describes how to use Carbon Black templates to create policies to detect and manage endpoints. Refer to the following sections:

- [Carbon Black Agents Installed Policy](#)
- [Create a Carbon Black Endpoint Threat Hunting Policy](#)
- [Carbon Black Network Threat Hunting Policy](#)

### Create a Carbon Black Agents Installed Policy

This policy separates endpoints into groups based upon their Carbon Black agent status. A Carbon Black administrator can ensure that the Carbon Black Response Sensor is installed and functioning properly on endpoints within the network. A Carbon Black Sensor is a stand-alone Windows, Linux, or Mac application that is installed on both the Carbon Black Response Server, Carbon Black Protection server
and network hosts to allow Carbon Black to manage devices-based Carbon Black policies.

Some Carbon Black agents may be incompatible with your host architecture or OS.

Use the Carbon Black Agents Installed policy template to create a policy that:

- Detects endpoints that have both Carbon Black Response Sensor and Carbon Black Protection Agent installed
- Detects endpoints that have either Carbon Black Response Sensor or Carbon Black Protection Agent Installed
- Detects endpoints that have neither the Carbon Black Response Sensor nor the Carbon Black Protection Agent installed

In addition, optional actions can be used to:

- Direct users to a URL from which to install the agent if it is not installed. It is recommended that the URL be available from outside the network.

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 Carbon Black folder and select Carbon Black Agents Installed.

![Policy Wizard Step 1](image)

Policy - Wizard - Step 1

Policy Type
Create a policy using a template or create a custom policy.

Carbon Black Agents Installed

Use this template to create a CounterACT policy that classifies endpoints with installed Carbon Black agents.

- Endpoints that have both Carbon Black Protection Agent and Carbon Black Response Sensor installed are mapped to the "Carbon Black Protection and Response" group.
- Endpoints that only have Carbon Black Protection Agent installed are mapped to the "Carbon Black Protection" group. You may configure and enable HTTP redirection to download the missing Carbon Black Response Sensor.
- Endpoints that only have Carbon Black Response Sensor installed are mapped to the "Carbon Black Response" group. You may configure and enable HTTP redirection to download the missing Carbon Black Protection Agent.
- Endpoints that do not have Carbon Black Protection Agent or Carbon Black Response Sensor installed are mapped to the "No Carbon Black" group. You may configure and enable HTTP redirection to download the missing Carbon Black Response Sensor and the Carbon Black Protection Agent.
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.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

   *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 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 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 and Policy Actions.

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 and Policy Actions.

- 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.

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 are passed 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.

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

The sub-rules of the Carbon Black Agents Installed policy list the items that the Forescout platform is to check when applying the sub-rule.
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 a Carbon Black Endpoint Threat Hunting Policy**

The purpose of this template is to set policy and enforcement with the Forescout platform based on parameters as reported by Carbon Black. This policy checks whether there have been threats recently reported to the Forescout platform by Carbon Black. Carbon Black generates threat intelligence and shares the IOCs with the Forescout platform about the compromised endpoint. Based on the policy condition(s), the Forescout platform can remediate or restrict the endpoints. You can also specify the actions to take on the endpoint, for example, *Send Syslog Message* or *Block Switch*.

Sub-rules detect endpoints based on the severity of the reported threat.

**To create a policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager.
3. Expand the Carbon Black folder and select **Carbon Black 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.


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.

  Filter the range by including only certain groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range is displayed in the Scope pane.

9. Select **Next**.

The main rule of this policy uses the Carbon Black Endpoint Threat Hunting property to select all endpoints for which the Forescout platform received a Carbon Black Threat Detection report within the last day. 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](#) and [Policy Actions](#).
11. Select **Next**.

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

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** and **Policy Actions**.

   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.

**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 are passed 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.

The main rule of this policy uses the Carbon Black Endpoint Threat Hunting property to select all endpoints for which the Forescout platform received a Carbon Black Threat Detection report within the last day.
Carbon Black Network Threat Hunting Policy

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-Carbon Black-managed devices, including IoT, Operational Technology (OT), BYOD, and Guest devices.
- Leverage threat intelligence received from Carbon Black to secure your network from threats

Carbon Black 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, the Forescout platform identifies the device as a guest. Based on policy conditions, 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.

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.

Before you create a Network Threat Hunting Policy, review the Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide.

To create a policy:

1. Log in to the Console and select Policy.
2. Select Add from the Policy Manager.
3. Expand the Carbon Black folder and select Carbon Black Network 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.


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.

10. The Sub-Rules pane lists the items the Forescout platform is to check. For details on the default policy logic, see How Devices are Detected and Handled.
11. Double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.

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

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


15. 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.

Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence. 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.

The sub-rules pane of the Carbon Black Network Threat Hinting policy lists the items the Forescout platform is to check when applying the main rule.

**Create Custom Carbon Black 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 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 Carbon Black.

- Remediate infected endpoints.

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

**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 Carbon Black properties that are available when you install Forescout eyeExtend for Carbon Black.

To access Carbon Black properties:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the Carbon Black folder in the Properties tree.

The following Carbon Black property categories are available.

- **Carbon Black Protection Agent Properties**
- **Carbon Black Protection Computer Properties**
- **Carbon Black Response Computer Vitals**
- **Carbon Black Response Sensor Vitals**

**Carbon Black Protection Agent Properties**

Carbon Black Protection Agent Properties provide information (version, installed, etc.) on the Carbon Black Protection Agent installed on a host.

To configure protection agent properties:

1. In the Condition dialog box, expand **Cb Protection Agent Properties**.
2. Select a Carbon Black Response property. The following parameters are available for configuration:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version</td>
<td>The version of Carbon Black Protection Platform Agent.</td>
</tr>
<tr>
<td>Policy Status</td>
<td>The detailed status of policy on the Carbon Black Protection Agent.</td>
</tr>
<tr>
<td>Agent Installed</td>
<td>Whether the Carbon Black Protection sensor is installed on the endpoint.</td>
</tr>
</tbody>
</table>

3. Select **OK** or select another Carbon Black property category in the Condition dialog box.

**Carbon Black Protection Computer Properties**

Carbon Black Computer Properties provides information on the host (for example, operating system or MAC address) where a Carbon Black Protection Agent is installed.

**To configure protection computer properties:**

1. In the Condition dialog box, expand **Cb Protection Computer Properties**.
2. Select a Carbon Black Response property. The following parameters are available for configuration:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Connected</td>
<td>Indicates if this computer is connected.</td>
</tr>
<tr>
<td>Days Offline</td>
<td>Indicates the number of days this computer was offline.</td>
</tr>
<tr>
<td>Computer IDs</td>
<td>Indicates the unique computer ID, name, description, and customized tag.</td>
</tr>
<tr>
<td>Computer Inactive</td>
<td>Indicates if this computer was uninstalled or disabled.</td>
</tr>
<tr>
<td>Local Approval</td>
<td>Indicates if this computer is in local approval mode.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Indicates the operating system name.</td>
</tr>
<tr>
<td>Platform</td>
<td>Indicates the platform ID and virtualization status.</td>
</tr>
<tr>
<td>Computer Policies</td>
<td>Indicates the details of the policy this computer belongs to: ID, name, and whether the computer's policy is assigned automatically through Active Directory.</td>
</tr>
<tr>
<td>Logged Users</td>
<td>Displays the list of last logged-in users.</td>
</tr>
</tbody>
</table>

3. Select OK or select another Carbon Black property category in the Condition dialog box.

**Carbon Black Response Computer Vitals**

Carbon Black Computer Vitals provides information (threat detections, computer name, etc.) on the host that a Carbon Black Response Sensor is installed on.

**To configure computer vitals properties:**

1. In the Condition dialog box, expand **Cb Response Computer Vitals**.
2. Select a Carbon Black Response property. The following parameters are available for configuration:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Indicates the NetBIOS and DNS names of this computer.</td>
</tr>
<tr>
<td>Computer SID</td>
<td>Indicates the security identifier machine of this host.</td>
</tr>
<tr>
<td>Threat Detections</td>
<td>Indicates the information of the IOC detected on the Carbon Black Response server. This includes IOC name, date, filename, hash, hash type and threat severity.</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>Displays a pipe-delimited list of IP and MAC address pairs for each network interface.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Displays the human-readable string of the installed operating system.</td>
</tr>
</tbody>
</table>

3. Select OK or select another Carbon Black property category in the Condition dialog box.

**Carbon Black Response Sensor Vitals**

Carbon Black Response Sensor Vitals provides information (for example, ID, status and version) on the Carbon Black Response Sensor installed on a host.

1. In the Condition dialog box, expand **Cb Response Sensor Vitals**.
2. Select a Carbon Black Response property. The following parameters are available for configuration:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Indicates the Group ID this Response Sensor is assigned to.</td>
</tr>
<tr>
<td>Last Check-in</td>
<td>Indicates the last communication with this computer in server-local time and zone.</td>
</tr>
<tr>
<td>Network Isolation</td>
<td>Indicates the Carbon Black Response network isolation status.</td>
</tr>
<tr>
<td>Next Expected Check-in</td>
<td>Indicates the next expected communication from this computer in server-local time and zone.</td>
</tr>
<tr>
<td>Sensor Health Status</td>
<td>Indicates the Carbon Black Response Sensor's self-reported health status.</td>
</tr>
<tr>
<td>Sensor Health Score</td>
<td>Indicates the Carbon Black Response Sensor's self-reported health score, from 0 to 100. The higher the score, the better the Response Sensor's health.</td>
</tr>
<tr>
<td>Sensor ID</td>
<td>Indicates the Response Sensor's identification number.</td>
</tr>
<tr>
<td>Sensor Installed</td>
<td>Indicates whether the Carbon Black Response Sensor is installed on the endpoint.</td>
</tr>
<tr>
<td>Sensor Version</td>
<td>Indicates the Carbon Black Response Sensor version and build ID from the API / Builds / Endpoint.</td>
</tr>
</tbody>
</table>

3. Select OK or select another Carbon Black property category in the Condition dialog box.

**Related IOC Scanner Plugin Properties**

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

### Policy Actions

There are no actions in Forescout eyeExtend for Carbon Black, however Forescout platform actions are available for detecting and handling endpoints. You can also create custom policies using other plugins or Forescout eyeExtend products.

### Working with Forescout eyeExtend for Carbon Black

Once Forescout eyeExtend for Carbon Black has been configured, you can view and manage the devices from Inventory view in the Console. This provides activity information, accurate at the time of the poll, on endpoints based on certain instances’ properties. The 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

### Access the Asset Inventory

**To access the inventory:**

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **Carbon Black** folder.
If you did not configure the module to show the property in the Asset Inventory, your Carbon Black properties are not displayed in the Views pane.

3. In the Views pane, expand **Carbon Black** and then select any item in the list to view its properties.

4. Check that the properties match the configuration requirements.

**Access the Home Tab**

To access the Home tab:

1. In the Console, select **Home**.
2. In the Views tree, expand your Carbon Black folder.
3. Select an item in the Detections pane. The Profile, Compliance, and All policies tabs display the information related to the host selected.

Refer to the Forescout Console User’s Manual or the Console Online Help for information about working with the Inventory.

**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 Technical Documentation Page, and 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 Support Portal](#)

*Software downloads are also available from these portals.*
To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page
The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:
- Go to https://www.Forescout.com/company/technical-documentation/

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:
- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal
The Downloads page on the Forescout Customer Support 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 Customer Support Portal:
- Go to 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.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

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 Administration Guide from the Help menu.
**Plugin Help Files**

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin and then select **Help**.

**Documentation Portal**

- Select **Documentation Portal** from the **Help** menu to access the **Documentation Portal**.