ForeScout® Extended Module for Carbon Black
Configuration Guide

Version 1.0
# Table of Contents

## About the Carbon Black Integration ................................................................. 4
   Advanced Threat Detection with the IOC Scanner Plugin .................................. 4
   Use Cases ............................................................................................................. 5
   Carbon Black Agent and Compliance .................................................................. 5
   Carbon Black Response Accelerate and Automate Policy-Driven Threat Response ............................................................... 5
   Carbon Black and CounterACT Threat Intelligence Sharing .................................. 5
   Additional Carbon Black Module Features ......................................................... 5
   Trusted Software Publisher .................................................................................. 5
   Additional Carbon Black Documentation ......................................................... 6

## About This Module .............................................................................................. 6

## Concepts, Components, Considerations .............................................................. 7
   Concepts .............................................................................................................. 7
      Deployment Options ......................................................................................... 7
   Components ........................................................................................................ 8
   Considerations .................................................................................................... 9
   What to Do ........................................................................................................... 10

## Requirements ...................................................................................................... 10
   CounterACT Software Requirements .................................................................. 10
   Carbon Black Requirements .............................................................................. 11
   Supported Systems Requirements ..................................................................... 11
   About Support for Dual Stack Environments .................................................. 11

## ForeScout Module Licensing Requirements ....................................................... 11
   Per-Appliance Licensing Mode .......................................................................... 12
   Centralized Licensing Mode ............................................................................. 13
   More License Information ................................................................................. 14

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

## Configure the Module ........................................................................................ 15
   Get an Authorization Token .............................................................................. 15
   Response Server ............................................................................................... 16
   Protection Server ............................................................................................... 16
   Add Carbon Black Response Connection (Optional) ........................................... 16
      Configure Syslog Messages from Carbon Black Response Server (Optional) ... 20
   Add Carbon Black Protection Connection (Optional) ....................................... 20
   Test Your Carbon Black Configurations ......................................................... 23

## Run Carbon Black Policy Templates ..................................................................... 24
   Carbon Black Agents Installed Policy Template .............................................. 25
   Carbon Black Endpoint Threat Hunting Policy Template .................................. 29
Carbon Black Network Threat Hunting Policy Template........................................... 34

**Create Custom Carbon Black Policies** ................................................................. 38
  Policy Properties................................................................................................. 39
  Carbon Black Protection Agent Properties ......................................................... 39
  Carbon Black Protection Computer Properties .................................................. 40
  Carbon Black Response Computer Vitals ............................................................ 41
  Carbon Black Response Sensor Vitals ................................................................. 42
  Policy Actions...................................................................................................... 43

**Using the Carbon Black Extended Module** ......................................................... 43
  Access the Inventory ............................................................................................ 43
  Access the Home Tab ........................................................................................... 44

**Additional CounterACT Documentation** ............................................................ 45
  Documentation Downloads ................................................................................... 45
  Documentation Portal ........................................................................................... 46
  CounterACT 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 with ForeScout CounterACT® will enhance Carbon Black’s abilities through:

- Verify Carbon Black Response and Protection agents are installed, operational and communicating properly with their respective Carbon Black instances.
- 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 CounterACT. 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, Considerations.

Advanced Threat Detection with the IOC Scanner Plugin

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

- A centralized repository of all threats and their IOCs (indicators of compromise) reported to CounterACT by third-party endpoint detection and response (EDR), and other threat prevention systems, or added manually.
- Mechanisms that scan all Windows endpoints for threat and IOC information reported to CounterACT, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- **ATD Stage 1 (Carbon Black Module): 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 CounterACT actions based on the severity of detected threats.

In addition to this initial response, all threats reported by this module are automatically submitted to the IOC Scanner Plugin. The IOC Scanner parses the threat to yield indicators of compromise (IOCs) - measurable events or state properties that can be used as a "fingerprint" to identify the threat. The IOC Scanner Plugin uses these IOCs to mount further scan/analyze/remediate stages of CounterACT’s ATD response, as follows:
• **ATD Stage 2 (IOC Scanner Plugin): Real-time hunt for endpoints of interest based on threats and IOCs, 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 *IOC Scanner Plugin Configuration Guide*.

**Use Cases**

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

**Carbon Black Agent and Compliance**

ForeScout improves security hygiene by verifying that Carbon Black agents are installed, running, and operating properly on supported corporate endpoints. ForeScout 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 Template](#).

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

When Carbon Black identifies malware or malicious behavior, it informs ForeScout in near real-time. Based on threat severity and your policy, ForeScout 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 ForeScout network actions allows you to reduce your mean time to respond (MTTR) and limit the impact of threats. See [Carbon Black Endpoint Threat Hunting Policy Template](#).

**Carbon Black and CounterACT Threat Intelligence Sharing**

Carbon Black identifies malware and IOCs through advanced techniques and notifies ForeScout upon detection. ForeScout 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, ForeScout can restrict, isolate or block network access for compromised devices. See [Carbon Black Network Threat Hunting Policy Template](#).

**Additional Carbon Black Module Features**

**Trusted Software Publisher**

During the Carbon Black Module configuration, you can approve trusted publishers, *ForeScout Technologies Inc. (with period)* and *ForeScout Technologies Inc (without period)*. Alternately, you can remove these publishers from approval on CounterACT
Carbon Black Protection server configuration. See Add Carbon Black Protection Connection (Optional).

**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**

The CounterACT operator/user will be able to:

- Configure a Connecting Appliance that is dedicated to communicating with Carbon Black Response and Carbon Black Protection, in order to aggregate and minimize traffic.
- Configure the Carbon Black Module to communicate with the Carbon Black Response and Carbon Black Protection servers.
- Optionally 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 using the Test button. The user will be presented with information collected from the test, such as the number of sensors installed and visible.
- IOCs from Carbon Black are automatically added to the IOC Scanner table upon IOC detections.
- View IOCs related to threats reported by 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 CounterACT Core Extensions Module: IOC Scanner Plugin Configuration Guide for more information.
- Use CounterACT 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 understanding of how CounterACT policies and other basic features work. Additionally, you should have a solid understanding of how to leverage threat intelligence distributed by IOCs.
Concepts, Components, Considerations

This section provides a basic overview of the Carbon Black/CounterACT 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**

Integration lets you connect one or more CounterACT Appliance(s) 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 **connecting CounterACT Appliance cluster**. This appliance cluster will handle 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 logical URL or IP address and user credentials.

**Deployment Options**

There are two topologies that can be used to set up multiple CounterACT Appliances to 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 prompts initiates queries whenever required. This is often the topology for remote sites.
A **CounterACT Connecting Appliance cluster** is a group of one or more 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 Console of changes in managed device configuration, providing a real-time view of device status.

- **Carbon Black Response** is the most precise IR and threat hunting solution, allowing you to get the answers you need faster than any other tool. 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 the most 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, point-of-sale devices, and others 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 the ones that are managing or monitoring devices based on the network segments assigned to a particular CounterACT Appliance. When these appliances communicate with Carbon Black, they go through the CounterACT Connecting Appliance cluster(s).

**Devices on the network** these are considered the hardware assets whose information has to be exchanged between CounterACT and Carbon Black. When these devices enters the network, CounterACT monitors them and provides information.

With this as the context, when the ForeScout Extended Module 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 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 advance settings.

## Considerations

This section addresses any additional ForeScout Extended Module for Carbon Black considerations.

When deploying CounterACT 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 run time directory to ensure CounterACT can successfully interrogate an endpoint.

Note: This Module will white list ForeScout certificates (See [Trusted Software Publisher](#)), but this feature will not create whitelist exceptions for CounterACT dynamically generated batch files (*.bat) as batch files are not signed by ForeScout.

For more information, see the [CounterACT HPS Inspection Engine Configuration Guide](#).
What to Do

Perform the following to carry out the integration.

1. Verify that requirements are met. See Requirements for details.
3. You are required to have either the Carbon Black Response server OR the Carbon Black Protection server.
   a. Define target Carbon Black Response server. Assign CounterACT Appliances to it. See Add Carbon Black Response Connection (Optional) for details.
   OR
   b. Define target Carbon Black Protection server. Assign CounterACT Appliances to it. See Add Carbon Black Protection Connection (Optional) for details.
4. Create policies for CounterACT to update Carbon Black assets. See Run Carbon Black Policy Templates.
5. When the configurations have been tested and the policies created, you are ready to start Using the Carbon Black Extended Module.

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Module Licensing Requirements
- Carbon Black Requirements
- Supported Systems Requirements

CounterACT Software Requirements

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

- CounterACT version 8.0.0
- A module license for the Carbon Black Module. See ForeScout Module Licensing Requirements.
- IOC Scanner Plugin version 2.1.0 or above
Carbon Black Requirements

The Carbon Black Module requires the following components:

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

Supported Systems Requirements

The Carbon Black Extended Module works on the following platform:

- Carbon Black Event Forwarder version 3.2.0 - supports Syslog output type with TLS encryption & authentication support.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, IPv6 addresses are not yet supported by this 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 component.

ForeScout Module Licensing Requirements

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

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

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

Select Options > Licenses to see whether you have a ForeScout CounterACT See license listed in the table.
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

**Per-Appliance Licensing Mode**

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

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

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

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

*This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the CounterACT Administration Guide for more information.*

**Requesting a License**

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

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.
To view the number of currently detected devices:

1. Select the **Home** tab.

2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.

**Centralized Licensing Mode**

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

- *No demo license is automatically installed during system installation.*

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

Each Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the See license.
Integration Modules, which package together groups of related licensed modules, are not supported when operating in Centralized Licensing Mode. Only Extended Modules, packaging individual licensed modules are supported. The Open Integration Module is an Extended Module even though it packages more than one module.

More License Information

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

Install the Module

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

To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - Per- Appliance Licensing Mode
   - Customer Portal, Downloads Page - Centralized Licensing Mode
   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.

2. Download the module .fpi file.

3. Save the file to the machine where the CounterACT Console is installed.

4. Log into the CounterACT Console and select Options from the Tools menu.

5. Select Modules. The Modules pane opens.

6. Select Install. The Open dialog box opens.

7. Browse to and select the saved module .fpi file.

8. Select Install. The Installation screen opens.

9. Select I agree to the License Agreement to confirm that you have read and agree to the terms of the License Agreement, and select Install. The installation will not proceed if you do not agree to the license agreement.

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

   In modules that contain more than one component, the installation proceeds automatically one component at a time.

10. When the installation completes, select Close to close the window. The installed module is displayed in the Modules pane.
Some components are not automatically started following installation.

### Identifying Your Licensing Mode in the Console

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

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

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

### Configure the Module

Configure the module to ensure that CounterACT can communicate with the Carbon Black servers.

- **Before proceeding, make sure that the Carbon Black Module is installed on your targeted CounterACT Appliance.**

To complete configuration of some of these connections, perform the following configuration steps on the Carbon Black instance:

- Get an Authorization Token
- Add Carbon Black Response Connection (Optional)
- Add Carbon Black Protection Connection (Optional)
- Test Your Carbon Black Configurations

### Get an Authorization Token

This section addresses getting the Authorization for Carbon Black Response and Carbon Black Protection.
Response Server

1. Login 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 displays, copy it. You will need this API token when you Add Carbon Black Response Connection (Optional).

Protection Server

1. Login to https://<IP address of Carbon Black Protection server>/user-details.php.
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 checkbox.
5. When the API Token displays, copy it. You will need this API token when you Add Carbon Black Protection Connection (Optional).

Add Carbon Black Response Connection (Optional)

This section addresses the configuration of your CounterACT Appliance to a Carbon Black Response server. Once you have this set up, you will have threat intelligence in the form of IOCs that identify malicious code.

To add Carbon Black Response targets for CounterACT:

1. In the CounterACT Console toolbar, select Options from the Tools menu.
2. Select Carbon Black from the Options pane. The right pane opens to the Carbon Black Response Connections tab.

4. Enter your configurations.

<table>
<thead>
<tr>
<th><strong>Server Address</strong></th>
<th>IP address of the Carbon Black Response server that sends notifications to CounterACT. The Carbon Black Response server must be able to handle the IP ranges of its assigned CounterACT devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Port</strong></td>
<td>Enter the port number used to access the Carbon Black Response 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 Response Server Certificate** | The checked box (default) adds certificate validation.  
- If the server certificate is a common commercial Certificate Authority issued certificate, the Carbon Black Module will set up the connection to the server.  
- If the server certificate is not a common commercial Certificate Authority issued certificate, the Carbon Black Module will not set up the connection to the server.  
OR  
If the box is un-checked, the Carbon Black Module will always setup the connection. It does not matter whether the server certificate is a common commercial Certificate Authority issued certificate or other. |

5. Select **Next**. The Assign CounterACT Devices pane displays.
6. Enter your configurations.

**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.

- **c.** Select **Available Devices** and then select an item in the Available Devices list.

- **d.** 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 by default - if they are not explicitly assigned to another connection appliance.

Select **Assign all devices by default** 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**. The Connecting Proxy Information pane displays.
## Use Proxy Server

If your environment routes internet communications through proxy servers, select this box.

### Proxy Server

Enter the IP address of the proxy server.

### Proxy Server Port

Select the port number of the proxy server.

### Proxy Server Username

Enter the administrator username used to access the proxy server.

### Proxy Server Password

Enter the administrator password used to access the proxy server.

### Verify Proxy Server Password

Re-enter the administrator password.

8. Select **Finish**. The server appears in the Carbon Black Response Server tab.

9. If you do not want to configure syslog messages from the Carbon Black Response server, continue to the Add Carbon Black Protection Connection (Optional)
Configure Syslog Messages from Carbon Black Response Server (Optional)

You will need to configure syslog messages from Carbon Black Response server to CounterACT.

1. Access the CB Response Server.
2. Open file `cb-coreservices.conf`; the full path name is `/etc/rsyslog.d/cb-coreservices.conf`
3. Add `/ append to this line:
   ```
   if $programname == 'cb-notifications' then /var/log/cb/
   notifications/cb-allnotifications.log;CbLogFormatWithPID
   ```
   with
   ```
   & @<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 *CounterACT Syslog Plugin Configuration Guide*.
5. Save the file.
6. Restart the Carbon Black Response syslog service by selecting `service rsyslog restart`.

Add Carbon Black Protection Connection (Optional)

Whitelisting exists for files signed by ForeScout Technologies Inc. This is configured automatically.

**To add Carbon Black Protection targets for CounterACT:**

1. In the CounterACT Console toolbar, select **Options** from the Tools menu.
2. Select **Carbon Black** from the Options pane. The right pane opens to display two tabs: Carbon Black Response Connections and Carbon Black Protections Connections.
3. Select the **Carbon Black Response Protections** tab and then select **Add**. The Add Carbon Black Protection Server wizard opens.
4. Enter your configurations.

<table>
<thead>
<tr>
<th>Table Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Address</strong></td>
<td>IP address of the Carbon Black Protection server that sends notifications to CounterACT. The Carbon Black Protection server must be able to handle the IP ranges of its assigned CounterACT devices.</td>
</tr>
<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>
<tr>
<td><strong>Validate Protection Server Certificate</strong></td>
<td>The checked box (default) adds certificate validation. &lt;ul&gt;&lt;li&gt;If the server certificate is a common commercial Certificate Authority issued certificate, the Carbon Black Module will set up the connection to the server.&lt;/li&gt;&lt;li&gt;If the server certificate is not a common commercial Certificate Authority issued certificate, the Carbon Black Module will not set up the connection to the server.&lt;/li&gt;&lt;/ul&gt; OR &lt;ul&gt;&lt;li&gt;If the box is un-checked, the Carbon Black Module will always setup the connection. It does not matter whether the server certificate is a common commercial Certificate Authority issued certificate or not.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td><strong>Trust ForeScout Technologies Inc. as a Publisher</strong></td>
<td>When checked (default), you approve ForeScout Technologies Inc. (with period) and ForeScout Technologies Inc (without period) as trusted publishers. When un-checked, you remove these publishers from approval.</td>
</tr>
</tbody>
</table>
5. Select **Next**. The Assign CounterACT Devices pane displays.

6. Enter your configurations.

| 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.
| a. Select **Available Devices** and then select an item in the Available Devices list.
| b. 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 by default - if they are not explicitly assigned to another connection appliance.
| Select **Assign all devices by default** 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**. The Connecting Proxy Information pane displays.

![Add Carbon Black Protection Server (Step 3 of 3)](image)

<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>

8. Select **Finish**. The server appears in the Carbon Black Protections Server tab.

**Test Your Carbon Black Configurations**

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 through 3.

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

Run Carbon Black Policy Templates

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

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

The following templates are available for detecting and managing endpoints:

- Carbon Black Agent Installed Policy Template
- Carbon Black Endpoint Threat Hunting Policy Template
- Carbon Black Network Threat Hunting Policy Template
Carbon Black Agents Installed Policy Template

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 CounterACT 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 use the Carbon Black Agents Installed policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
4. Select **Next**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.
5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.


**Define which Devices will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box lets you define a range of hosts to be inspected for this policy.

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

![IP Address Range Dialog Box]

The following options are available:

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

8. Select OK. The added range appears in the Scope pane.

9. (Optional) To review and modify default policy logic before you create the policy, select Next. The Main Rule pane displays.

**How Devices are Detected and Handled**

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

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

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

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

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

Main Rule

The main rule of this policy detects Windows endpoints that are managed using Remote Inspection.
11. You can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.

12. Select **Next**. The Sub-Rules pane displays.

### Sub-Rules

The sub-rules of the Carbon Black Agents Installed policy list the items CounterACT is to check when applying the Sub-Rule.


14. You can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** section.

15. Select **OK**. In the Policy: [Name of Carbon Black Agents Installed policy] Sub-Rule: Carbon Black Protection Agent dialog box, select **OK**.

16. Repeat steps 13 - 15 to make changes in other sub-rules.

17. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

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

### Carbon Black Endpoint Threat Hunting Policy Template

The purpose of this template is to set policy and enforcement with CounterACT based on parameters as reported by Carbon Black. This policy checks whether there have been threats recently reported to CounterACT by Carbon Black. Carbon Black generates threat intelligence and shares the IOCs with CounterACT about the compromised endpoint. Based on the policy condition(s), CounterACT can remediate or restrict the endpoints. The user can also specify what 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 use the Carbon Black Endpoint Threat Hunting policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the Carbon Black folder and select **Carbon Black Endpoint Threat Hunting**.
4. Select **Next**. The policy wizard opens to the **Name** pane.
Name the Policy

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

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

Naming Tips

− Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
− The name should indicate what the policy verifies and what actions are taken.
− The name should indicate whether policy criteria must be met or not met.
− Avoid having another policy with a similar name.

6. Select Next. The Scope pane and IP Address Range dialog box displays.

Define Which Hosts Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

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

The following options are available:

− 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. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

− All IPs: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.

- **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.

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

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

9. Select **OK**. The added range displays in the Scope pane.

10. Select **Next**. The Sub-Rule pane displays.

### How Devices are Detected and Handled

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

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

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

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

### Main Rule

The main rule of this policy uses the Carbon Black Endpoint Threat Hunting property to select all endpoints for which CounterACT received a Carbon Black Threat Detection report within the last day.
11. You can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** section. The Main Rule and Sub-Rules panes are also available when you edit an existing policy.

12. Select **Next**. The Sub-Rules pane displays.

14. You can Add conditions and actions. A list of these items can be found in the Policy Properties section.

15. Select OK. In the Policy: [Name] Sub-Rule: Carbon Black Threat Detections - Critical dialog box, select OK.

16. Repeat steps 12 - 14 to make changes in other sub-rules.

17. In the Sub-Rules pane of the Policy Wizard, select Finish.

18. On the CounterACT Console, select Apply to save the policy.

**Carbon Black Network Threat Hunting Policy Template**

The purpose of this template is to provide:

- Comprehensive network and endpoint detection tactics with discrete response
- Expand threat hunting to include non-traditional and non-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 CounterACT and blocked via network firewall or network quarantine.

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

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

Review the CounterACT® IOC Scanner Plugin Configuration Guide.

To use the Carbon Black Network Threat Hunting policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Carbon Black folder and select Carbon Black Network Threat Hunting.
4. Select Next. The policy wizard opens to the Name pane.
Name the Policy

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

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

   ** Naming Tips **
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - The name should indicate what the policy verifies and what actions are taken.
   - The name should indicate whether policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

6. Select Next. The Scope pane and IP Address Range pane displays.

Define Which Hosts Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

7. Use The IP Address Range dialog box to define which endpoints are inspected.
The following options are available:

- **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 displays in the Scope pane.

9. Select **Next**. The Sub-Rule pane displays.

**How Devices are Detected and Handled**

Policy rules instruct CounterACT 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.

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

**Sub-Rules**

The sub-rules of the Carbon Black Network Threat Hinting policy lists the items CounterACT is to check when applying the Main Rule.

12. You can Add conditions and actions. A list of these items can be found in the Policy Properties section.

13. Select OK. In the Policy: [Name] Sub-Rule: Warn-IOC Detected dialog box, select OK.

14. Repeat steps 12 - 14 to make changes in other sub-rules.

15. In the Sub-Rules pane of the Policy Wizard, select Finish.

16. On the CounterACT Console, select Apply to save the policy.

Create Custom Carbon Black Policies

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

Policies and Rules, Conditions and Actions

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

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

- Actions can be applied to endpoints that match the conditions of the rule.

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

- Scan potentially compromised Windows endpoints for IOCs reported by the Carbon Black Module.

- RemEDIATE infected endpoints.

These items are available when you install the IOC Scanner Plugin.
To create a custom policy:

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

Policy Properties

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

To access Carbon Black properties:

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

1. In the Condition dialog box, expand **Cb Protection Agent Properties**.
2. Select a Carbon Black Protection property and configure it.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Status</td>
<td>Detailed status of policy on the Carbon Black Protection Agent.</td>
</tr>
<tr>
<td>Agent Installed</td>
<td>Indicate whether the Carbon Black Protection sensor is installed on the endpoint.</td>
</tr>
</tbody>
</table>

3. When finished, 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 (OS, MAC address, etc.) that a Carbon Black Protection Agent is installed on.

1. In the Condition dialog box, expand **Cb Protection Computer Properties.**
2. Select a Carbon Black Protection property and configure it.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Connected</td>
<td>Indicate if this computer is connected.</td>
</tr>
<tr>
<td>Days Offline</td>
<td>Number of days this computer was offline.</td>
</tr>
<tr>
<td>Computer IDs</td>
<td>Indicate the unique computer ID, name, description, and customized tag.</td>
</tr>
<tr>
<td>Computer Inactive</td>
<td>Indicate if this computer was uninstalled or disabled.</td>
</tr>
<tr>
<td>Local Approval</td>
<td>Indicate if this computer is in local approval mode.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Operating System name.</td>
</tr>
<tr>
<td>Platform</td>
<td>Choose platform ID and virtualization status.</td>
</tr>
<tr>
<td>Computer Policies</td>
<td>Indicate 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>Display the list of last logged-in users.</td>
</tr>
</tbody>
</table>

3. When finished, 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.

1. In the Condition dialog box, expand **Cb Response Computer Vitals**.

2. Select a Carbon Black Response property and configure it.
Computer Name
Indicate the NetBIOS and DNS names of this computer.

Computer SID
Display the security identifier machine of this host.

Threat Detections
Indicate the information of the IOC detected on the Carbon Black Response server. This includes IOC name, date, filename, hash, hash type and threat severity.

Network Adapters
Display a pipe-delimited list of IP and MAC pairs for each network interface.

OS Version
Display the human-readable string of the installed operating system.

3. When finished, 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 (ID, status, version, etc.) 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 and configure it.

<table>
<thead>
<tr>
<th>Group ID</th>
<th>The Group ID this Response Sensor is assigned to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Check-in</td>
<td>Indicate the last communication with this computer in server-local time and zone.</td>
</tr>
<tr>
<td>Network Isolation</td>
<td>Indicate the Carbon Black Response network isolation status.</td>
</tr>
<tr>
<td>Next Expected Check-in</td>
<td>Indicate the next expected communication from this computer in server-local time and zone.</td>
</tr>
</tbody>
</table>
### Sensor Health Status
Indicate the Carbon Black Response Sensor’s self-reported health status.

### Sensor Health Score
Indicate 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.

### Sensor ID
Display the Response Sensor’s identification number.

### Sensor Installed
Indicate whether the Carbon Black Response Sensor is installed on the endpoint.

### Sensor Version
Indicate the Carbon Black Response Sensor version and build ID from the API / Builds / Endpoint.

3. When finished, 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 [CounterACT IOC Scanner Plugin Configuration Guide](#) for property details.

**Policy Actions**
There are no actions in the Carbon Black Module, however, there are CounterACT actions available for detecting and handling endpoints. You can also create custom policies using other plugins or extended modules.

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

To access the inventory:

1. Log in to the CounterACT Console and select the **Inventory** tab.
2. In the Views pane, expand the **Carbon Black** folder.
If you did not configure to show the property in the Inventory tab, your Carbon Black properties will not display in the Views pane of the Inventory tab.

3. In the left pane, select the Carbon Black icon to expand it and then select any of the items in the list to view its properties.

4. Check that the properties match the configuration requirements.

Access the Home Tab

To access the Home tab:

1. In the CounterACT Console, select the Home tab.
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 Working at the Console>Working with Inventory Detections in the CounterACT Console User's Manual or the Console Online Help for information about working with the CounterACT Inventory.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

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

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

Software downloads are also available from these portals.
To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

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

To access the Product Updates Portal:
2. Select the CounterACT version you want to discover.

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

To access documentation on the ForeScout Customer Portal:
2. Select Downloads or Documentation.

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

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

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools
Access information directly from the CounterACT Console.

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

CounterACT Administration Guide
Select CounterACT Help from the Help menu.

Plugin Help Files
1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.

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

**Documentation Portal**

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

**Identifying Your Licensing Mode in the Console**

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

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

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

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

2018-06-28 14:27