ForeScout

CounterACT™ Check Point Threat Prevention Module

Configuration Guide

Version 1.0.0

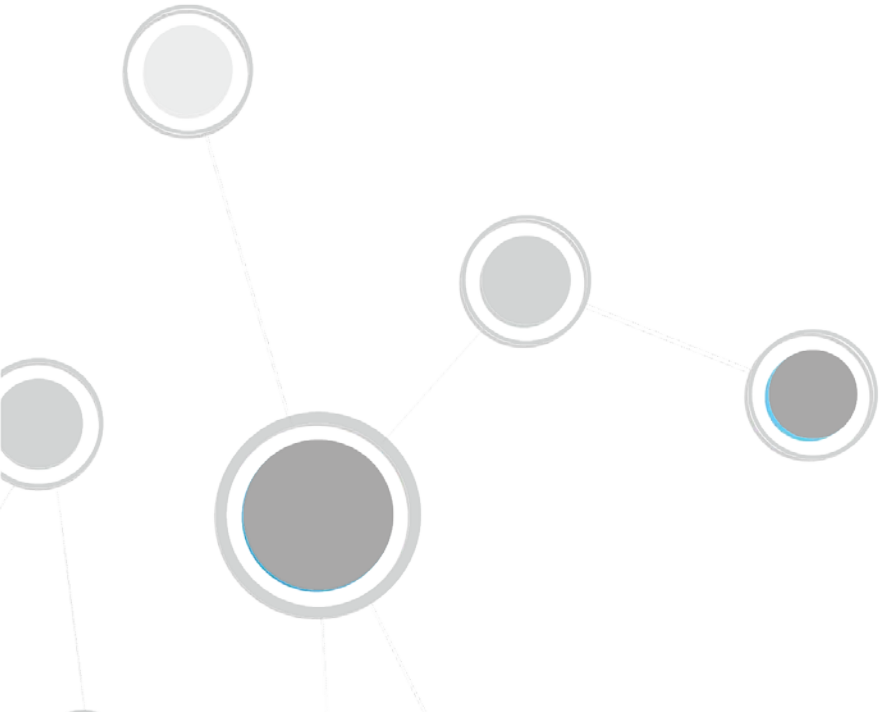


Table of Contents

About the Check Point Threat Prevention Integration

Integrating with Check Point Threat Prevention tools allows CounterACT to receive important threat information and IOCs based on the following Check Point blade detections:

- Anti-Bot: Detects bot-infected machines and prevents bot damages by blocking bot cybercriminal Command and Control center communications.
- Antivirus: Stops incoming malicious files at the gateway before the user is affected with real-time virus signatures and anomalies.
- Threat Emulation: Prevents infections from undiscovered exploits as well as zero-day and targeted attacks. This solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior.

Check Point Threat Prevention solutions fortify network security by blocking bot Command and Control communications and stopping unknown malware, viruses and file transfers.

However, if infected endpoints are connected to the corporate network they may still spread malware, and this is where CounterACT steps in.

Sharing blade detection information with CounterACT helps security teams simplify and accelerate the process of identifying, analyzing and responding to events that threaten network security.

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.

Close the Security Cycle – Real-Time Response

Receive alerts from Check Point on threats detected and quickly perform actions ensure that the network is safe. For example, notify security teams, block endpoints and trigger vulnerability scans using a CounterACT vulnerability integration modules.

Carry out IOC Hunting

Scan all Windows endpoints for IOCs reported to CounterACT by Check Point in order to identify threats and perform actions on potentially infected endpoints. For example, use CounterACT policies to run policy actions that rapidly:

- Contain infected endpoints, for example limit or block network access. This prevents lateral movement of the infection to other endpoints.
- Control infected endpoints, for example by killing suspicious processes.
- Notify stakeholders by, for example, sending an email to corporate security teams with details about which threats were detected on which endpoints.

Additional Check Point Threat Prevention Documentation

Refer to Check Point's online documentation for more information about the Check Point Threat Prevention solution:

https://www.checkpoint.com/support-services/

About This Module

The Check Point Threat Prevention Module leverages information retrieved from mission-critical Check Point software tools. Use the module to:

- Handle Advanced Threat Detection with the IOC Scanner Plugin
- React in Real-Time to Threats with CounterACT Policies

Handle 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.

For more information about IOC-based threat detection and remediation, see the *IOC Scanner Plugin Configuration Guide*.

React in Real-Time to Threats with CounterACT Policies

Respond to threats by rolling out CounterACT policy templates that handle:

- ***Anti-Bot Detections***: See Check Point Anti-Bot Threat Detections Policy Template for details.
- ***Anti-Virus Detections***: See Check Point Anti-Virus Threat Detections Policy Template for details.
- ***Threat Emulation Detections***: See Check Point Threat Emulation Threat Detections Policy Template for details.

Additional Check Point Threat Prevention Documentation

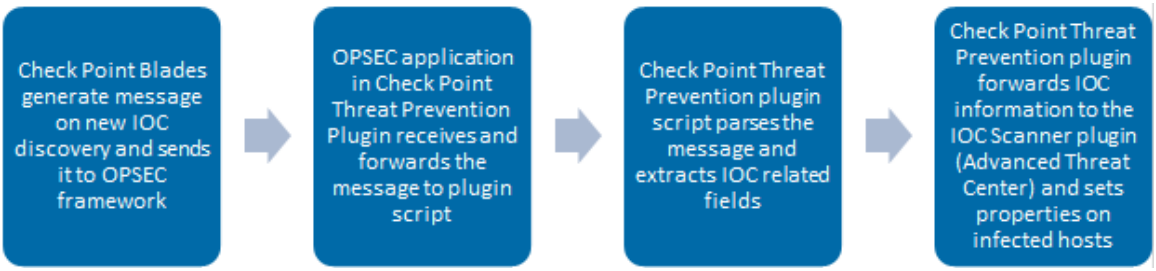
Refer to Check Point's online documentation for more information about the Check Point Threat Prevention solution:

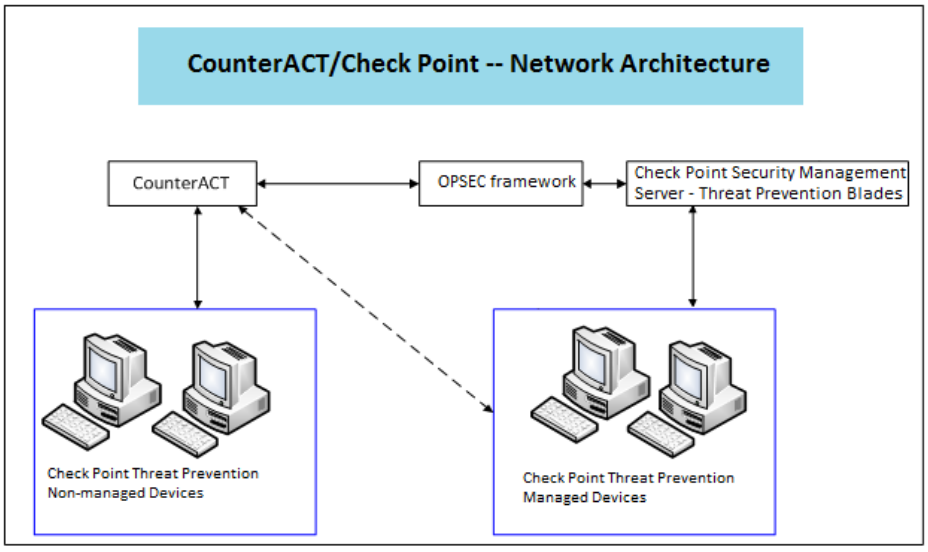
https://www.checkpoint.com/support-services/

How It Works

When a threat is detected, the Check Point LEA Server sends a message containing details to the configured CounterACT LEA client. The message is then parsed for threat information including a timestamp of the event, protection name and type, malware name and activity, operating system, file name and hash.

The Check Point Threat Prevention module then passes the parsed IOC information to the IOC Scanner Plugin which converts the data into properties associated with the endpoint where the threat was discovered as well as properties on other endpoints which can be used to trigger policy actions.





Workflow

1. The administrator uses Check Point SmartDashBoard to register the CounterACT Appliance as host in the Check Point Security Management Server.
2. The administrator uses the CounterACT Console to configure the Check Point Threat Prevention module to listen for messages from the Check Point appliances.
3. The Check Point Threat Prevention module pulls the certificate from the Check Point Security Management Server and starts a LEA client application. (Each Check Point appliance is configured separately)
4. Messages are sent from the Check Point appliance to the LEA client by calling an event handler in the LEA client. The messages are then passed to the Check Point Threat Prevention Module script. The Check Point Threat Prevention module parses these messages.
5. The Check Point Threat Prevention Module sends the IOC details to the IOC Scanner 2.0.0 Plugin.
6. The module sets a host property on the IP address indicated in the original message (as the infected host) with details of the IOC.

What to Do

This section lists the steps you should take to set up your system when integrating with Check Point Threat Prevention:

1. Verify that you have met system requirements. See Requirements.
2. Configure Check Point to CounterACT Server Communication.
3. Install the Module.
4. Configure the Module.
5. Test the Module.
6. (Optional) Run Check Point Threat Prevention Policy Templates, and/or Create Custom Check Point Threat Prevention Policies.
7. (Optional) Run IOC Scanner Templates as described in the IOC Scanner Plugin Configuration Guide.

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- Supported Vendor Requirements
- Networking Requirements

CounterACT Software Requirements

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

- CounterACT version 7.0.0
- Service Pack 2.3.2 or above.
  If the DNS Query Extension Plugin for detecting and parsing DNS messages is installed, SP 2.3.2 is required. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- An active Maintenance Contract for the module.
- IOC Scanner Plugin version 2.0.0

Supported Vendor Requirements

The module supports the following Check Point Threat Prevention components:

- Check Point Security Management Server R77.20 and R77.30
- Check Point Security Management Server R80 with R77.30 Gateway

Administrator access must be defined.

Networking Requirements

This section describes the networking requirements for this integration.

Check Point Ports

The following ports must be open on the Check Point Server and set in CounterACT in order to receive messages and to support communication between CounterACT and the Check Point Threat Prevention service:

- 18210 – to pull the certificate from the Check Point Security Management Server
- 18184 – for LEA Server communication.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin 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.

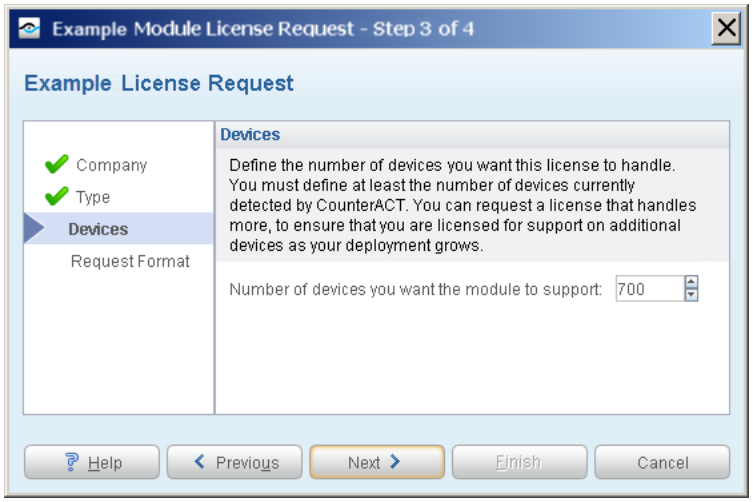
When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

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

Requesting a License

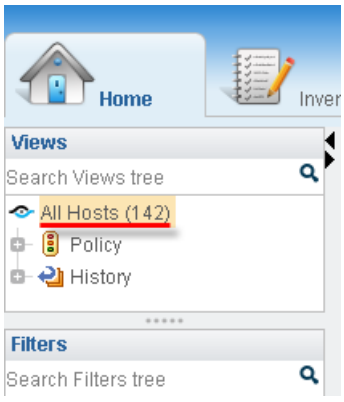
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that 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:

8. Select the **Home** tab.
9. 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.



More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

Configure Check Point to CounterACT Server Communication

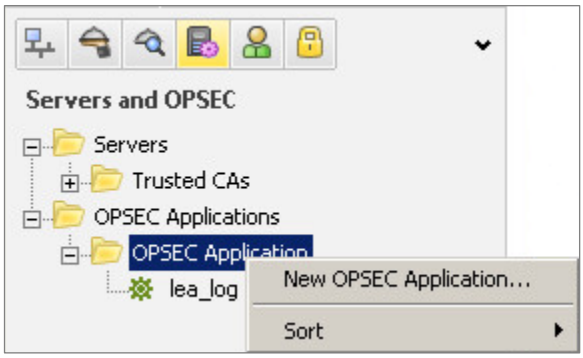
Before configuring the module in CounterACT, set up communication between the Check Point Security Management Server and CounterACT.

You must complete the entire Check Point server setup (Steps 1 through 13 below) before configuring the module in CounterACT.

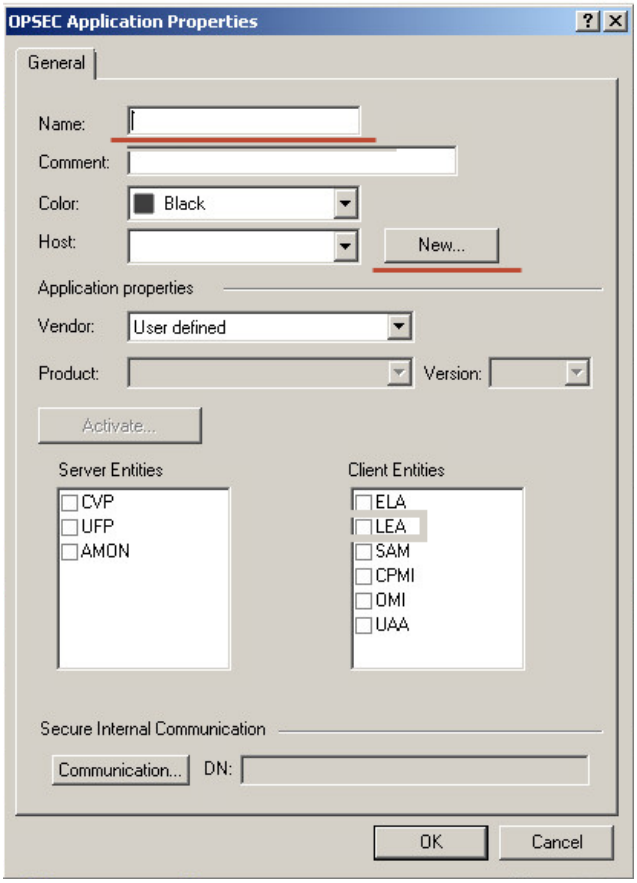
To set up communication:

1. In the Check Point SmartDashboard, log in to the Check Point Security Management Console.

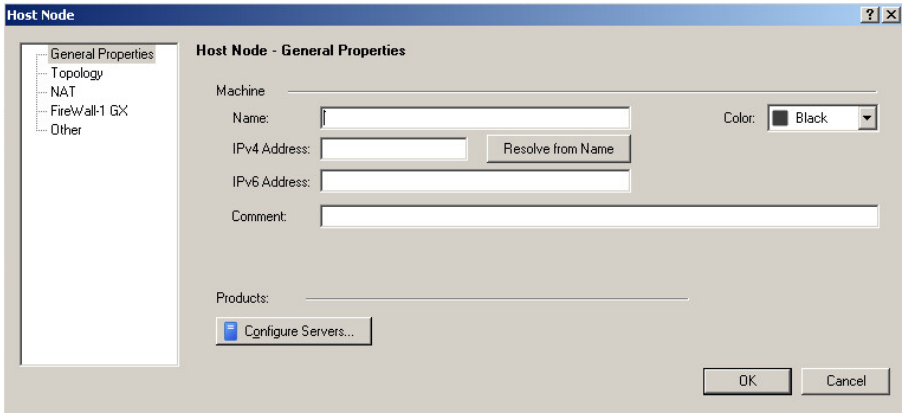
2. Go to the **Servers and OPSEC** window to define the host and the OPSEC Application.
3. Right-click **OPSEC Application** and select **New OPSEC Application**.



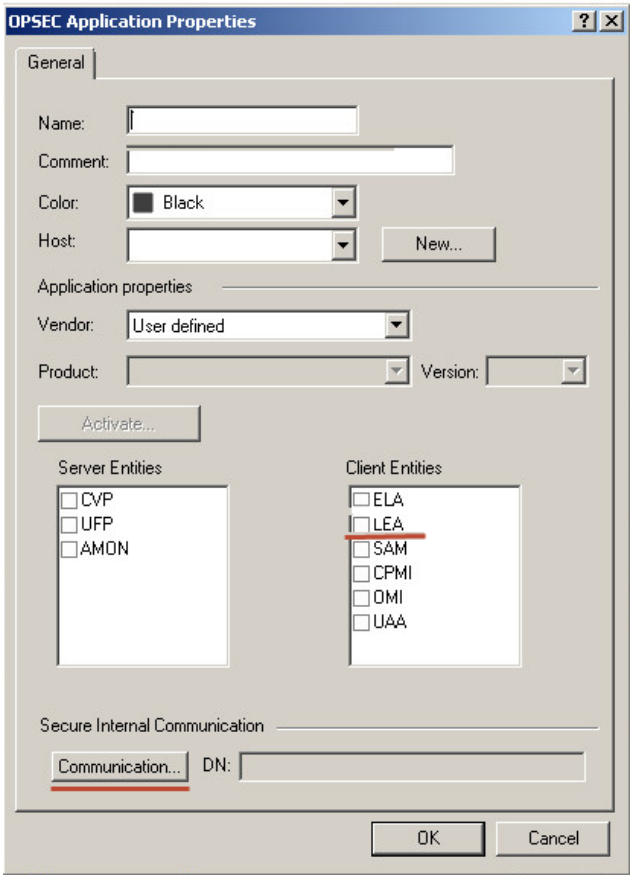
4. In the OPSEC Application Properties dialog, enter a **Name**.



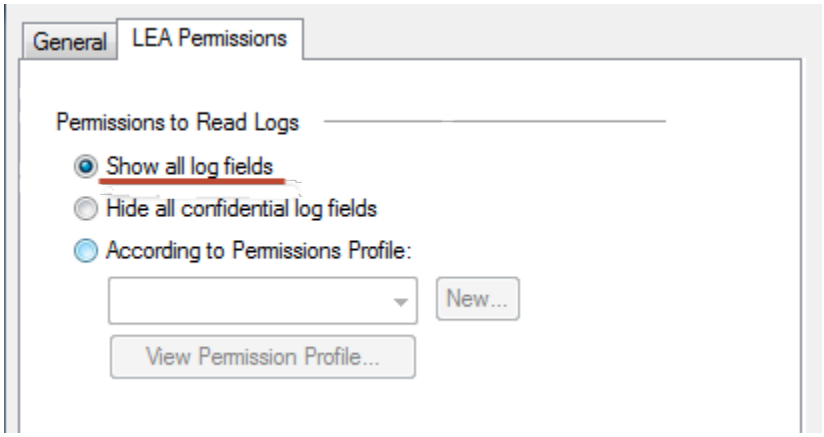
5. If the CounterACT appliance is not a known host that appears in the Vendor drop-down menu, click **New** to create a new host. The **Host Node** dialog appears.



6. Select **General Properties** in the left pane and enter the **Name** and **IPv4** address of the CounterACT appliance used to receive messages from this Check Point Security Management Server and select **OK**.
7. Under **Client Entities** select **LEA**.

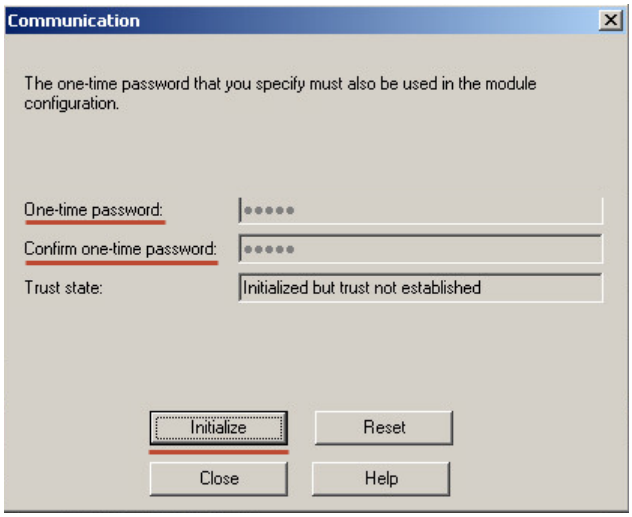


8. Select the **LEA Permissions** tab.
9. Select **Show all log fields**.



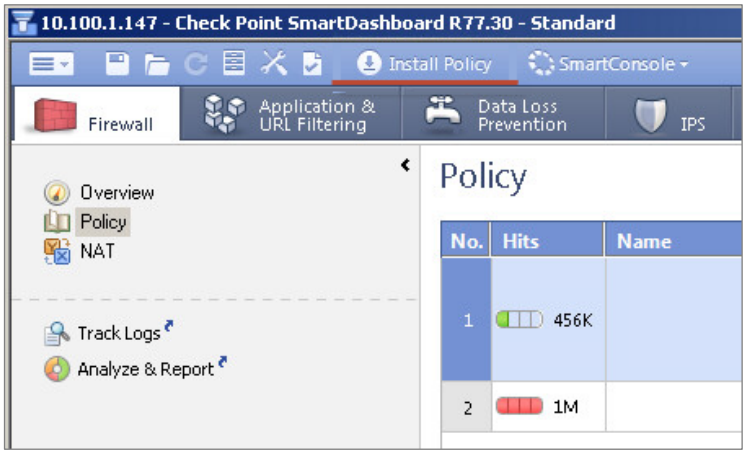
10. Select the **General** tab.

11. Select **Communication**. The **Communication** dialog opens.



12. Enter a one-time password and select **Initialize**.

13. Select **Close** and install the policy.



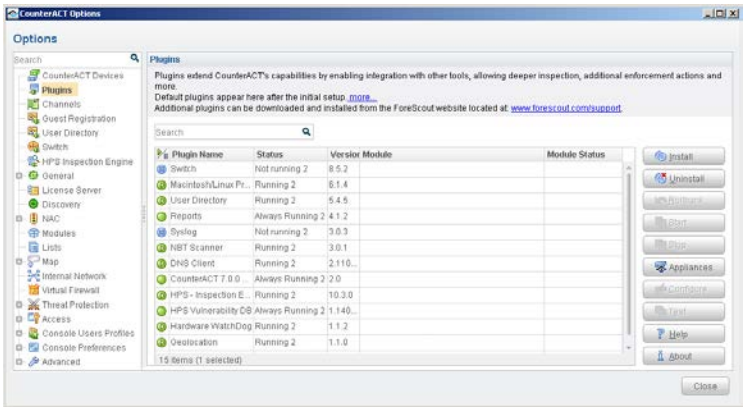
Install the Module

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

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Navigate to the Customer Support, ForeScout Modules page and download the plugin `.fpi` file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.

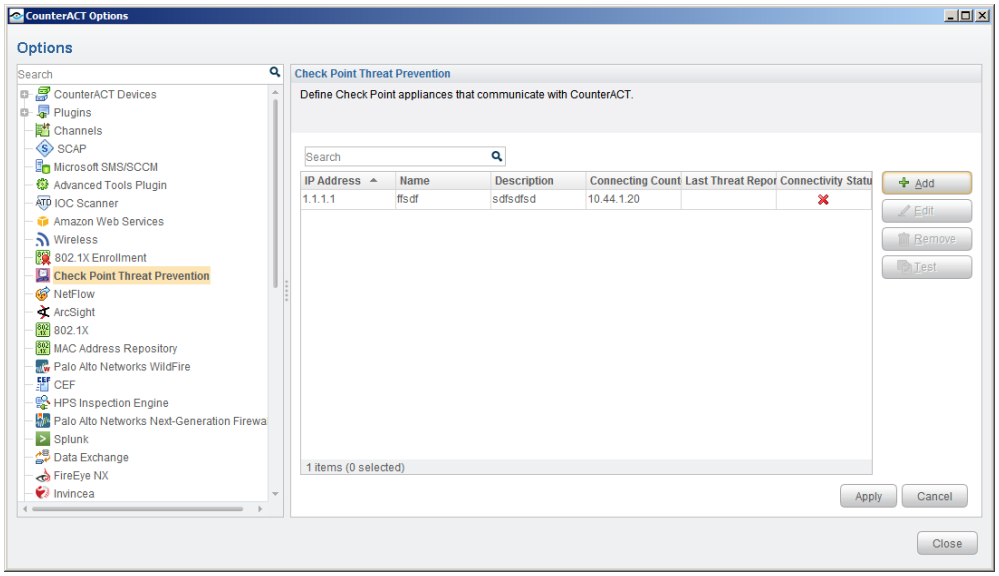


5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin `.fpi` file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and then select **Install**.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select **Close**. The plugin is displayed in the Plugins pane. The **Module Status** column indicates the status of your license. See ForeScout Module License Requirements and the *CounterACT Console User Manual* for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select **Start**. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select **OK**. The plugin runs on the selected devices.

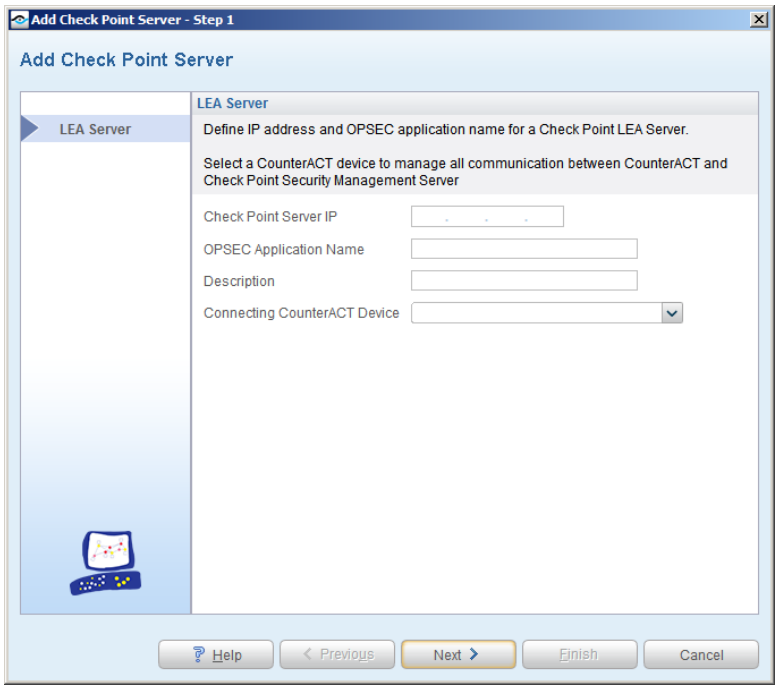
Configure the Module

Configure the module to ensure that CounterACT can communicate with the Check Point Threat Prevention service.

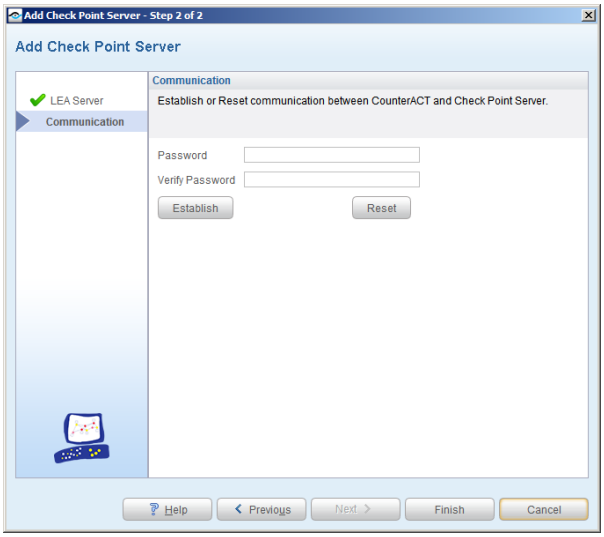
1. Select **Options** from the **Tools** menu and then select the **Plugins** folder.
2. In the **Plugins** pane, select the Check Point Threat Prevention Plugin and select **Configure**.



3. Select **Add**. The Add Check Point Server dialog box opens.



4. Enter the **Check Point Server IP** and **OPSEC Application Name**. The OPSEC Application name is the one created in the Check Point SmartDashboard.
5. Select a **Connecting CounterACT Device** and select **Next**.



6. Enter the one-time password created in the Check Point SmartDashboard and select **Establish**. This certificate is used to enable communication between CounterACT and the Check Point Security Management Server.
7. Select **Apply**. This reboots this module and updates the configuration. The Connectivity Status column displays the current link status after this reboot.

Test the Module

Test the module communication with the Check Point service.

To test the connection:

1. To test communication with Check Point Threat Prevention servers, select a server, and select **Test**. To pass the test, Check Point sends fixed data packets within a timeout period. The Connectivity Status column should also be updated with the current link status.
2. After viewing the test results, select **Close**.

Run Check Point Threat Prevention 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:

- Check Point Anti-Bot Threat Detections Policy Template
- Check Point Anti-Virus Threat Detections Policy Template
- Check Point Threat Emulation Threat Detections Policy Template

Check Point Anti-Bot Threat Detections Policy Template

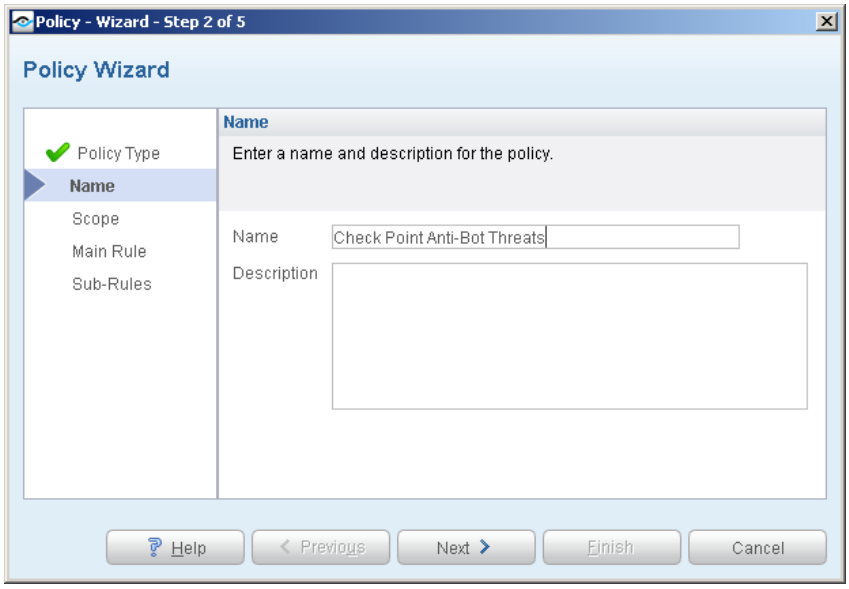
Use this template to create a CounterACT policy that responds to threats that are detected by the Check Point Anti-Bot blade and reported to CounterACT. You can define different responses to threats based on their severity as reported by Check Point Anti-Bot Threat Detections.

To use the Check Point Anti-Bot Threat Detections policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Check Point Threat Prevention** folder and select **Check Point Anti-Bot Threat Detections**. The Check Point Anti-Bot Threat Detections pane opens.
4. Select **Next**. The Name pane opens.

Name the Policy

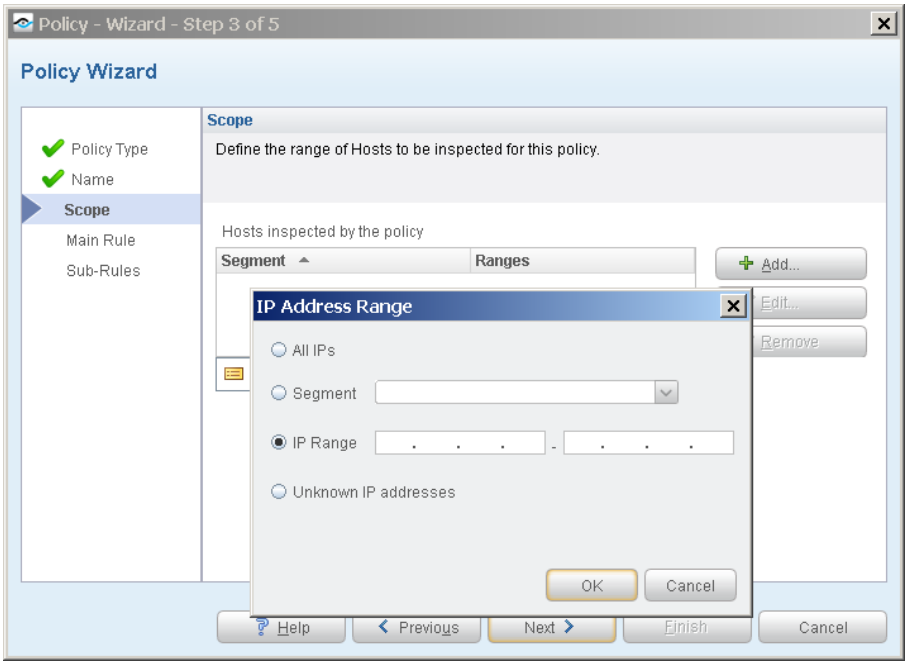
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.
6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

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 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 page.
   - **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.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens.

How Endpoints Are Detected and Handled

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

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy detects all threats detected by the Check Point Anti-Bot blade reported to CounterACT in the last week.

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

Sub-Rules

The sub-rules of this policy detect threats based on their reported severity.

- For threats with *Critical* and *High* severity:

 An optional **Switch Block** action is available.

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

- For threats with *Medium, Low and Very Low* severity:

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

2. Select **Finish** to create the policy.
3. On the Policy Manager, select **Apply** to save the policy.

Check Point Anti-Virus Threat Detections Policy Template

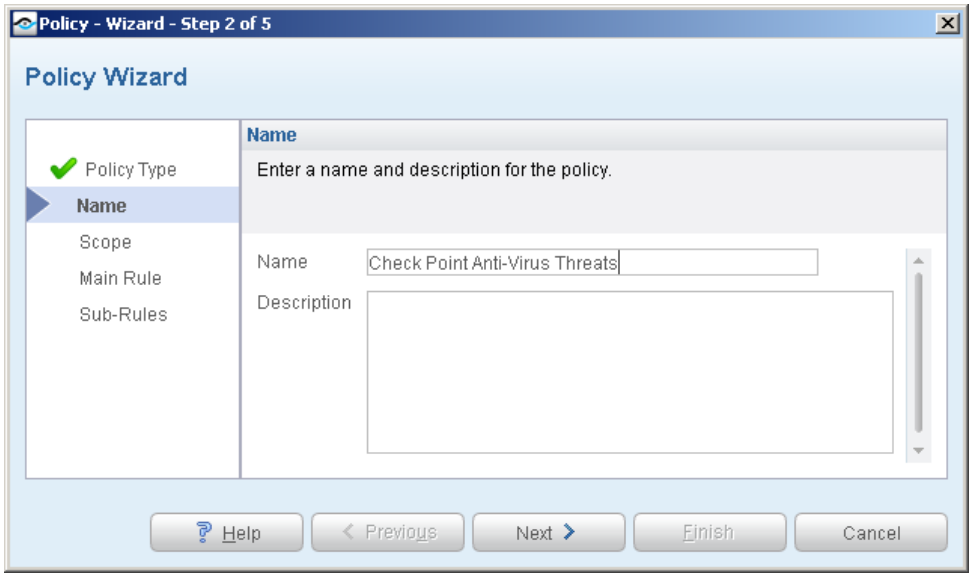
Use this template to create a CounterACT policy that responds to threats that are detected by the Check Point Anti-Virus blade and reported to CounterACT. You can define different responses to threats based on their severity as reported by Check Point Anti-Virus Threat Detections.

To use the Check Point Anti-Virus Threat Detections policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Check Point Threat Prevention** folder and select **Check Point Anti-Virus Threat Detections**. The Check Point Anti-Virus Threat Detections pane opens.
4. Select **Next**. The Name pane opens.

Name the Policy

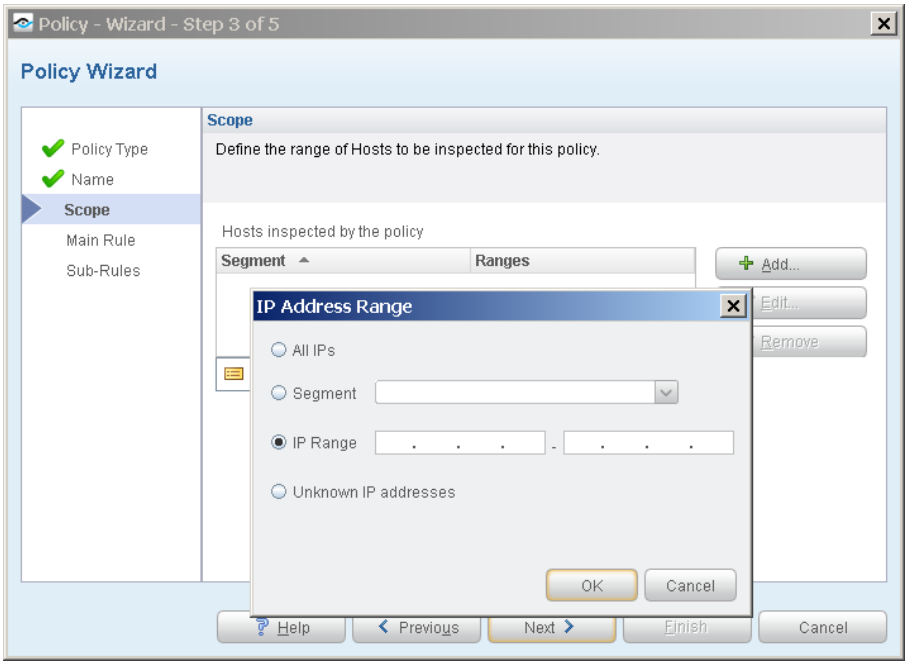
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.
6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

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 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 page.
   - **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.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens.

How Endpoints Are Detected and Handled

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

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy detects all threat detections reported to CounterACT in the last week.

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

Sub-Rules

The sub-rules of this policy detect threats based on their reported severity.

- For threats with *Critical* and *High* severity:

 An optional **Switch Block** action is available.

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

- For threats with *Medium, Low and Very Low* severity:

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

11. Select **Finish** to create the policy.
12. On the Policy Manager, select **Apply** to save the policy.

Check Point Threat Emulation Threat Detections Policy Template

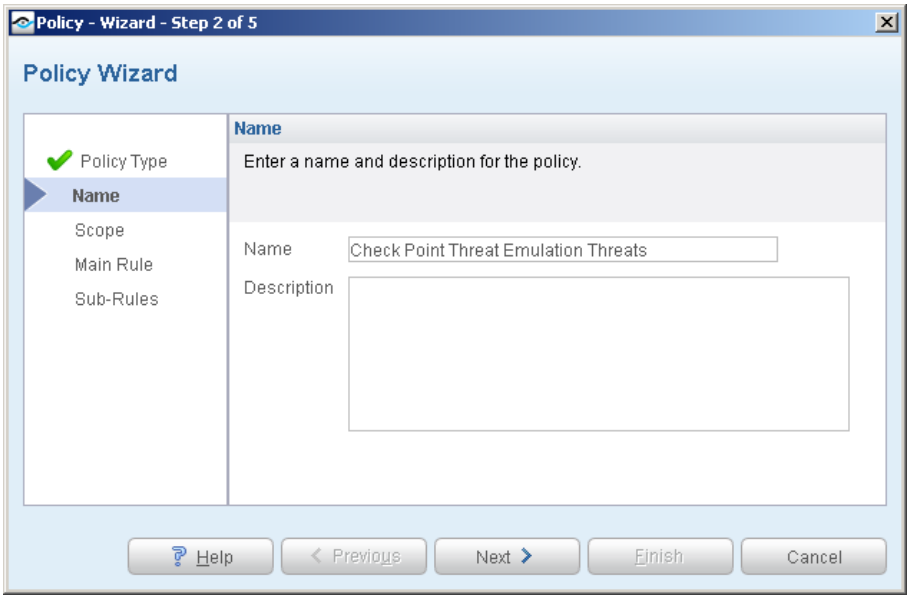
Use this template to create a CounterACT policy that responds to threats that are detected by the Check Point Threat Emulation blade and reported to CounterACT. You can define different responses to threats based on their severity as reported by Check Point Threat Emulation Threat Detections.

To use the Check Point Threat Emulation Threat Detections policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Check Point Threat Prevention** folder and select **Check Point Threat Emulation Threat Detections**. The Check Point Threat Emulation Threat Detections pane opens.
4. Select **Next**. The Name pane opens.

Name the Policy

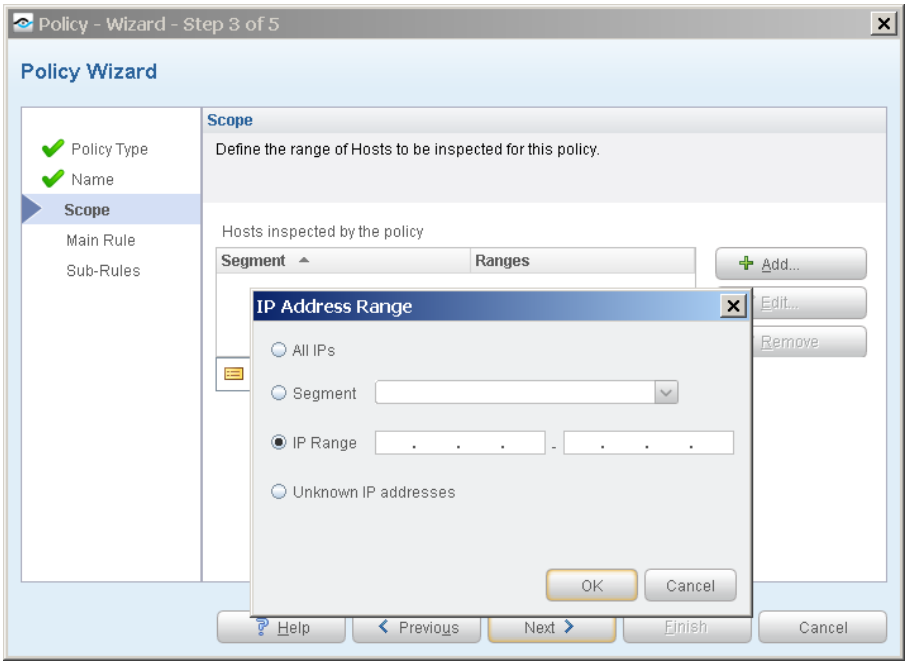
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.
6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

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 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 page.
   - **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.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens.

How Endpoints Are Detected and Handled

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

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy detects all threat detections reported to CounterACT in the last week.

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

Sub-Rules

The sub-rules of this policy detect threats based on their reported severity.

- For threats with *Critical* and *High* severity:

 An optional **Switch Block** action is available.

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

- For threats with *Medium, Low and Very Low* severity:

 An optional **Send Email** action is available.

 An optional **HTTP Notification** action is available.

By default, these actions are disabled.

11. Select **Finish** to create the policy.
12. On the Policy Manager, select **Apply** to save the policy.

Advanced Threat Detection with the IOC Scanner Module Templates

This module works with the IOC Scanner Plugin – CounterACT's action center for Advanced Threat Detection (ATD) and response. For more information about IOC Scanner policy templates and IOC-based threat detection and remediation, see the IOC Scanner Plugin Configuration Guide.

Display Inventory Data

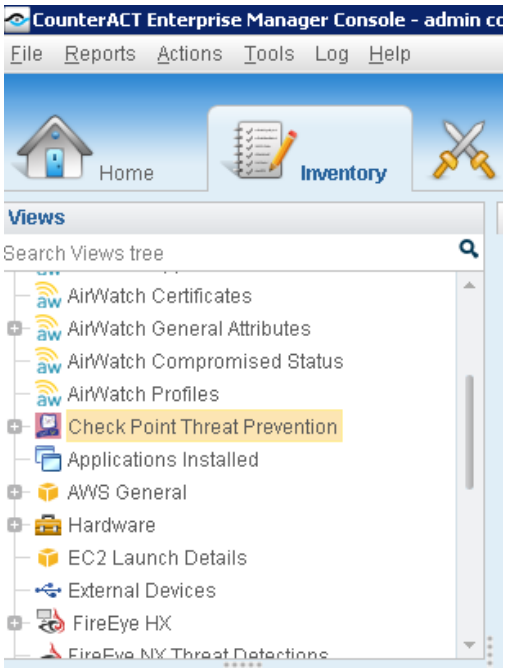
Use the CounterACT Inventory to view a real-time display of threats detected by Check Point Threat Prevention . The inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoint information reported by the Check Point Threat Prevention agent.

- View endpoints that have been detected with specific threats.
- Easily track Check Point Threat Prevention activity.
- Incorporate inventory detections into policies.

To access the inventory:

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the **Check Point Threat Prevention** folder.



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 how to work with the CounterACT Inventory.

Create Custom Check Point Threat Prevention 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 Check Point Threat Prevention Module.
- Remediate infected endpoints.

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

To create a custom policy:

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

Check Point Threat Prevention – Policy Properties

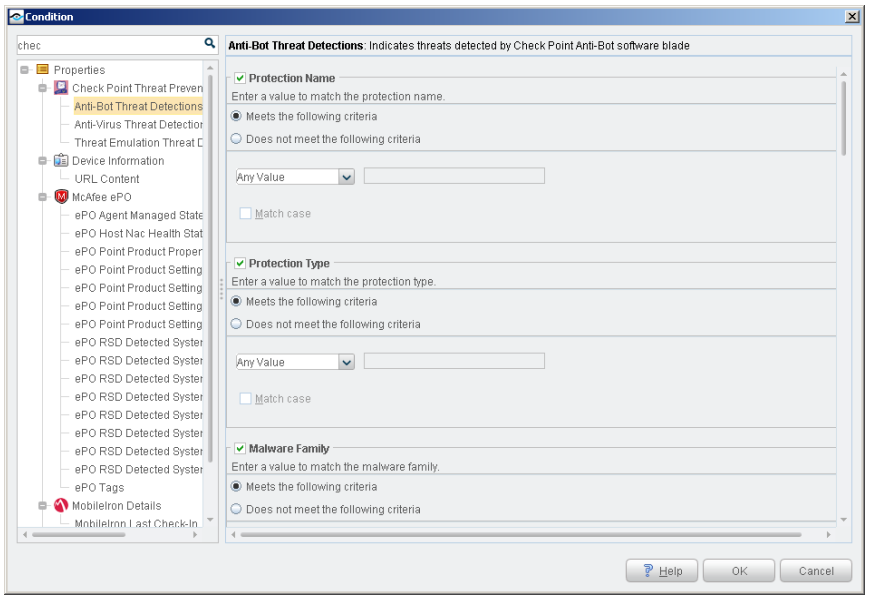
This section describes the properties that are available when you install this module.

To access Check Point Threat Prevention properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the Check Point Threat Prevention folder in the Properties tree.

The following properties are available:

- Anti-Bot Threat Detections
- Anti-Virus Threat Detections
- Threat Emulation Threat Detections



Anti-Bot Threat Detections

This property detects threats that the Check Point Anti-Bot Software Blade detected on the endpoint. You can use this property in CounterACT policies to provide an real-time response to threats. For example, create a policy that detects if Anti-Bot Threat Detections has detected a Critical severity threat, and trigger the required real-time response when an endpoint meets this condition. The threat information detected is:

- Protection Name
- Protection Type
- Malware Family
- Malware Activity
- Severity
- Confidence Level
- Protection ID
- Scope
- Source OS
- Resource
- Web Client Type

Anti-Virus Threat Detections

This property detects threats that Check Point Antivirus Software Blade detected on the endpoint. You can use this property in CounterACT policies to provide an real-time response to threats. For example, create a policy that detects if Anti-Virus Threat Detections has detected a Critical severity threat, and trigger the required real-time response when an endpoint meets this condition. The threat information detected is:

- Protection Name
- Protection Type
- Malware Activity
- Severity
- Confidence Level
- Protection ID
- Threat File Name
- Threat File MD5
- Scope
- Source OS
- Resource
- Web Client Type

Threat Emulation Threat Detections

Indicates threats that Check Point Threat Emulation detected on the endpoint. You can use this property in CounterACT policies to provide a real-time response to threats. For example, create a policy that detects if Threat Emulation Threat Detections has detected a Critical severity threat, and trigger the required real-time response when an endpoint meets this condition. The threat information detected is:

- Protection Name
- Protection Type
- Malware Activity
- Severity
- Confidence Level
- Verdict
- Threat File Name
- Threat File Size
- Threat File MD5
- Threat File SHA-1
- Threat File SHA-256
- Vulnerable OS
- Scope
- Resource
- Web Client Type

Related IOC Scanner Plugin Properties

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

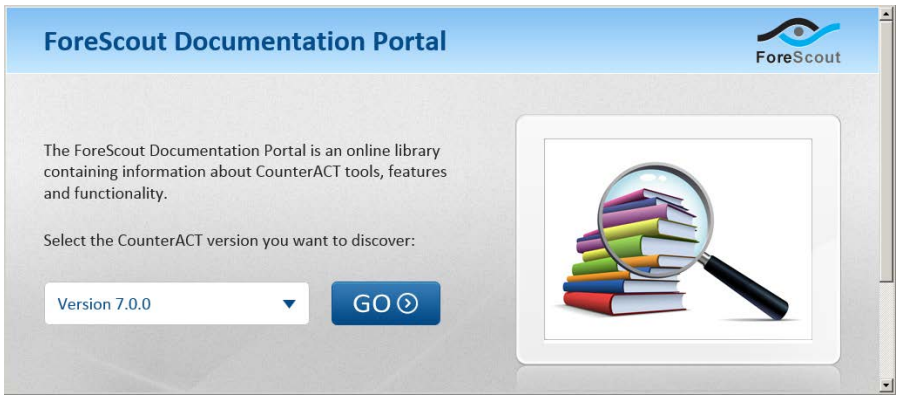
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



To access the Documentation Portal:

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

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:

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

CounterACT Console Online 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.

Console User Manual

1. Select **CounterACT Help** from the **Help** menu.

Help files

1. After the module is installed, select **Options** from the **Tools** menu and then select **Plugins**.

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

Documentation Portal

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

Legal Notice

2016-11-13 17:28