FORESCOUT

Forescout

eyeExtend for Check Point Threat Prevention

Configuration Guide

Version 1.3

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

2020-02-26 15:29

Table of Contents

About the Check Point Threat Prevention Integration

Integrating with Check Point® Threat Prevention tools lets the Forescout platform 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 the Forescout platform steps in.

Sharing blade detection information with the Forescout platform 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 Forescout eyeExtend for Check Point Threat Prevention. 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 the Forescout platform vulnerability integration modules.

Carry out IOC Hunting

Scan all Windows endpoints for IOCs reported to the Forescout platform by Check Point in order to identify threats and perform actions on potentially infected endpoints. For example, use 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

Forescout eyeExtend for Check Point Threat Prevention 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 Forescout Policies

Handle Advanced Threat Detection with the IOC Scanner Plugin

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

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

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

React in Real-Time to Threats with Forescout Policies

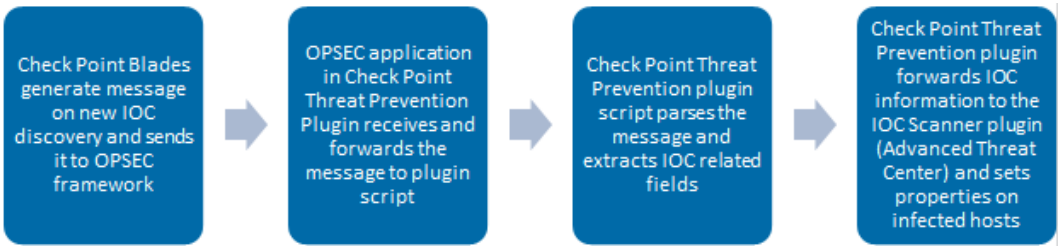
Respond to threats by rolling out Forescout platform policy templates that handle:

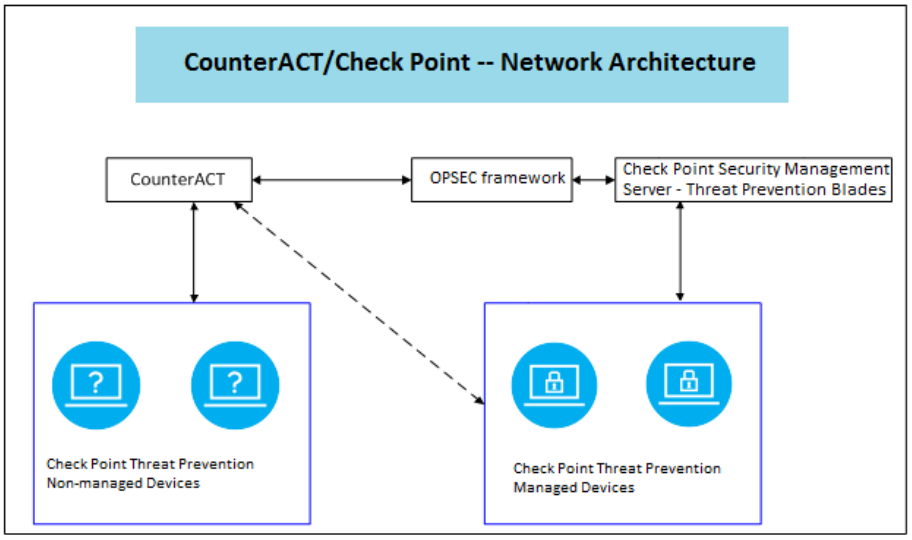
- ***Anti-Bot Detections***: See Check Point Anti-Bot Threat Detections Policy Template for details.
- ***Anti-Virus Detections***: See Check Point Anti-Virus Threat Detections Policy Template for details.
- ***Threat Emulation Detections***: See Check Point Threat Emulation Threat Detections Policy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

How It Works

When a threat is detected, the Check Point LEA Server sends a message containing details to the configured 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.

Forescout eyeExtend for Check Point Threat Prevention 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 Forescout Console to configure Forescout eyeExtend for Check Point Threat Prevention to listen for messages from the Check Point appliances.
3. Forescout eyeExtend for Check Point Threat Prevention 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 Forescout eyeExtend for Check Point Threat Prevention script. The Check Point Threat Prevention module parses these messages.
5. Forescout eyeExtend for Check Point Threat Prevention sends the IOC details to the IOC Scanner 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 Forescout 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 policy templates as described in the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide*.

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Supported Vendor Requirements
- Networking Requirements

Forescout Requirements

The module requires the following Forescout releases and other components.

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Check Point Threat Prevention. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- Core Extensions Module version 1.2 with the IOC Scanner Plugin running.

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.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

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 configured in the Forescout platform to receive messages and to support communication between the Forescout platform and the Check Point Threat Prevention service:

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

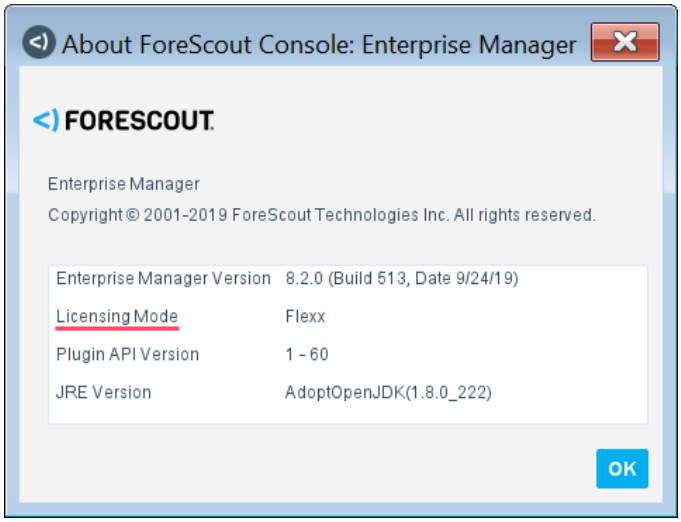
Forescout eyeExtend (Extended Module) Licensing Requirements

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

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

To identify your licensing mode:

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



Per-Appliance Licensing Mode

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

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

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

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

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

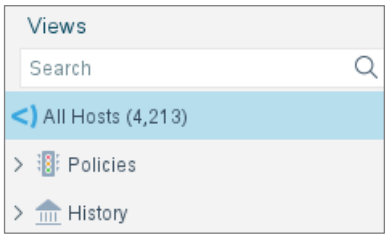
Requesting a License

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

Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.

To view the number of currently detected devices:

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



Flexx Licensing Mode

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

No demo license is automatically installed during system installation.

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

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

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

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

Configure Check Point to Forescout Server Communication

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

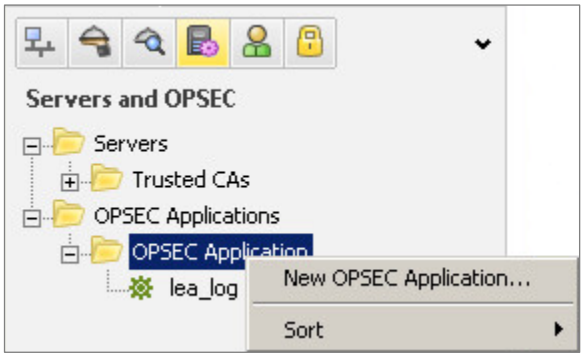
You must complete the entire Check Point server setup (Steps 1 through 13 below) before configuring the module.

To set up communication:

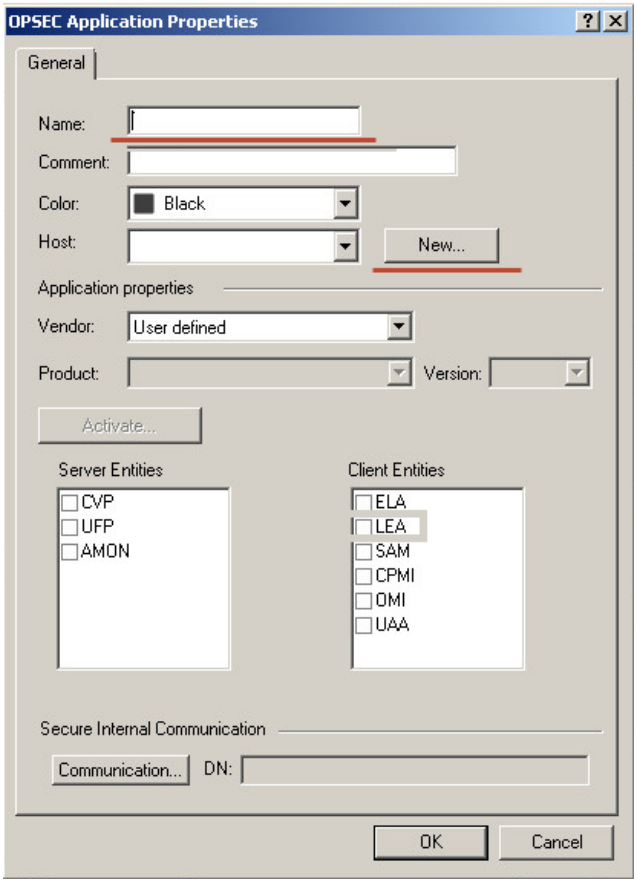
1. In the Check Point SmartDashboard, log in to the Check Point Security Management Console.

2. Go to the Servers and OPSEC window to define the host and the OPSEC Application.

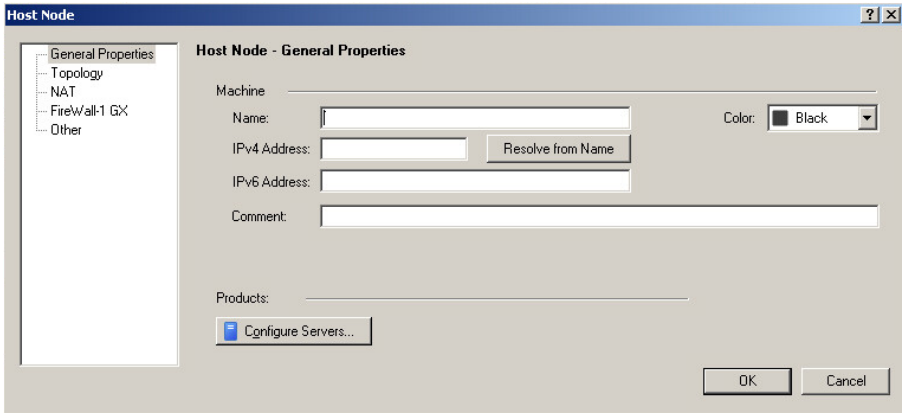
3. Right-click **OPSEC Application** and select **New OPSEC Application**.



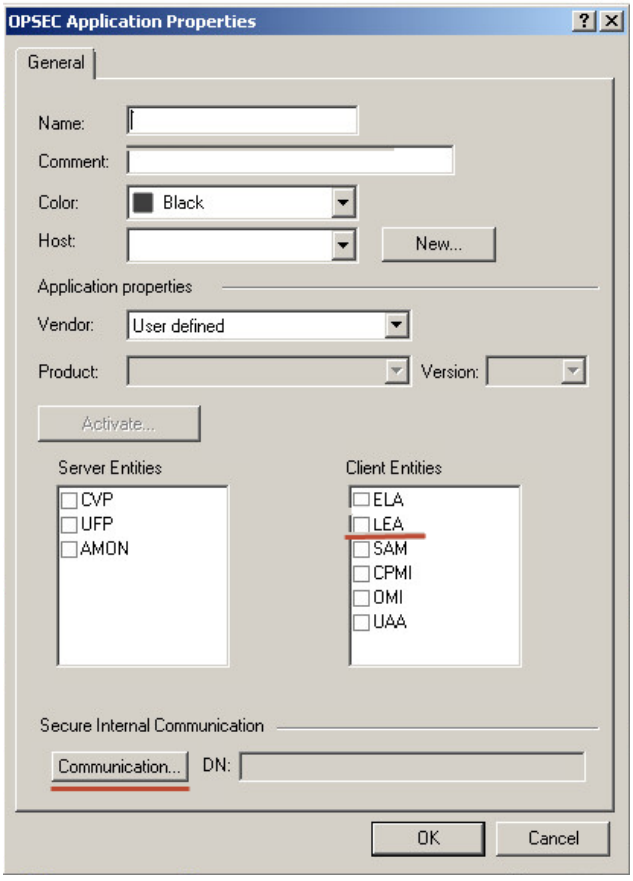
4. In the OPSEC Application Properties dialog, enter a **Name**.



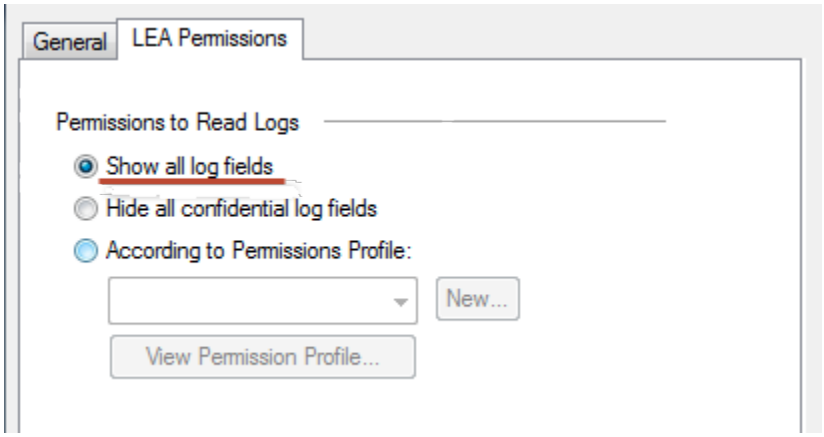
5. If the CounterACT Appliance is not a known host that is displayed in the Vendor drop-down menu, select **New** to create a new host.



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**.

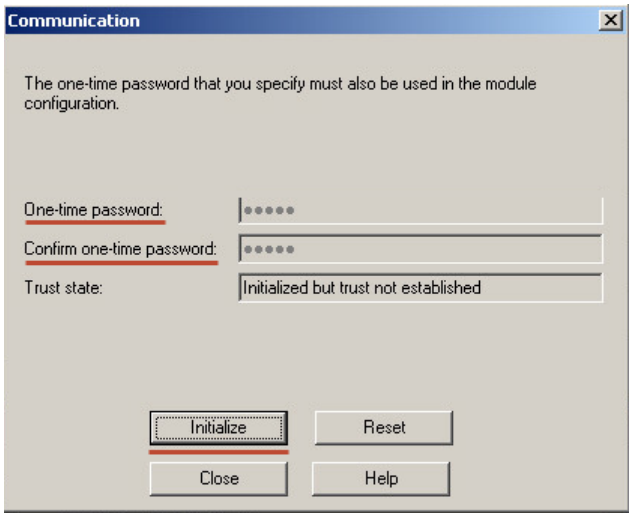


8. Select the LEA Permissions tab.
9. Select **Show all log fields**.



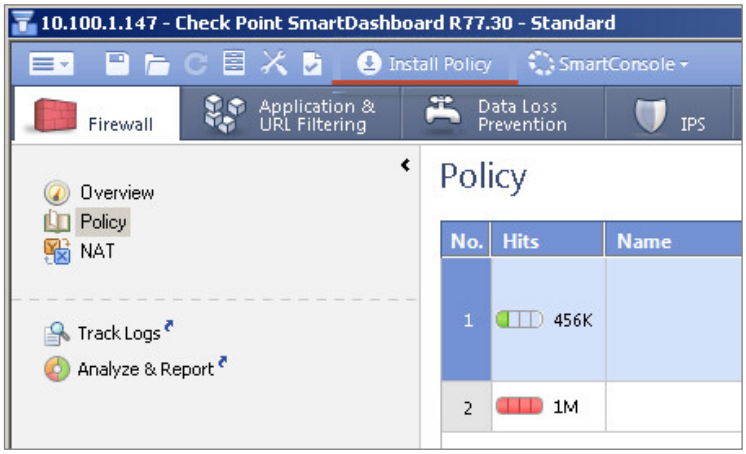
10. Select the General tab.

11. Select **Communication**.



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 Forescout Requirements.

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Flexx Licensing Mode***

   To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

   The installation begins immediately after selecting Install and cannot be interrupted or canceled.

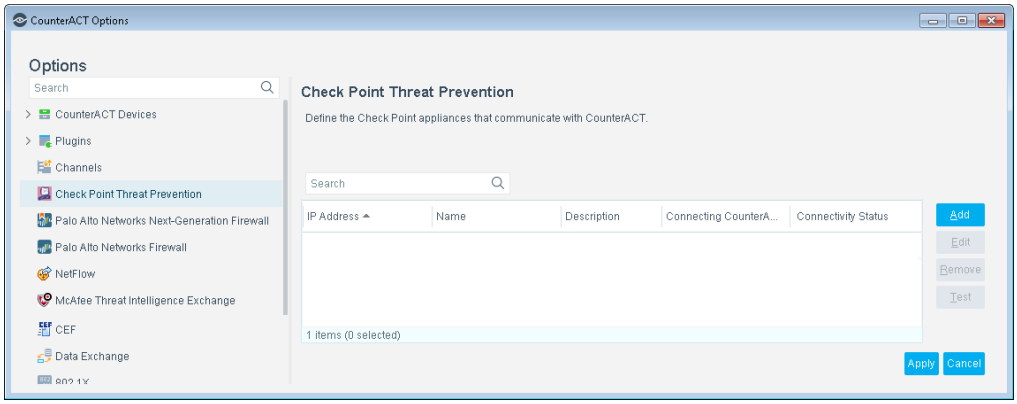
   In modules that contain more than one component, the installation proceeds automatically one component at a time.
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

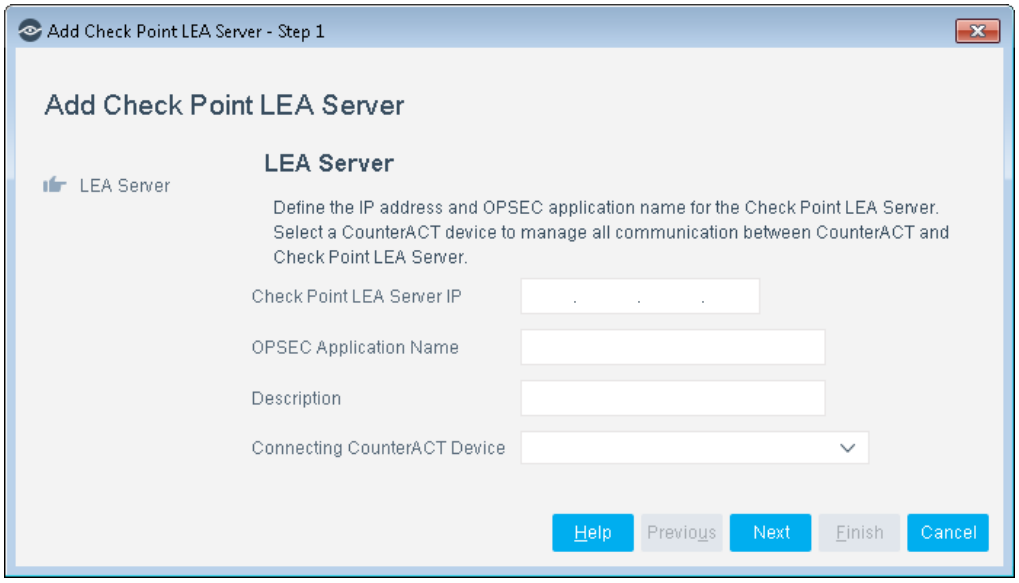
Configure the Module

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

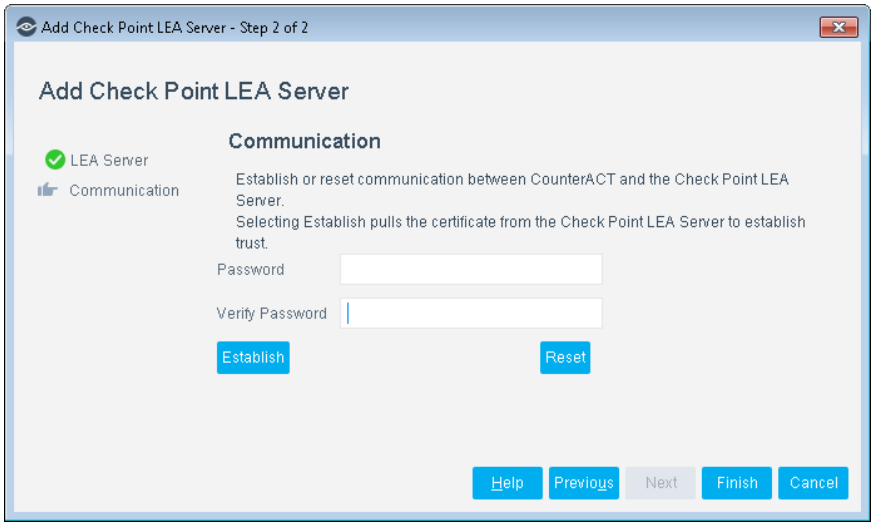
1. Select **Options** from the **Tools** menu and then select the **Modules** folder.
2. In the Modules pane, select **Check Point Threat Prevention** and select **Configure**.



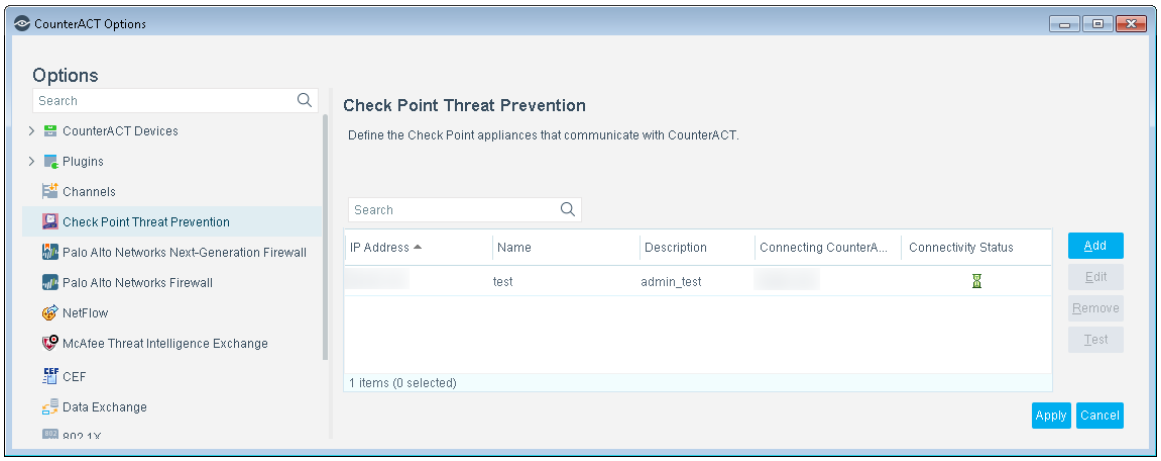
3. Select **Add**.



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 the Forescout platform 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

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

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with 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

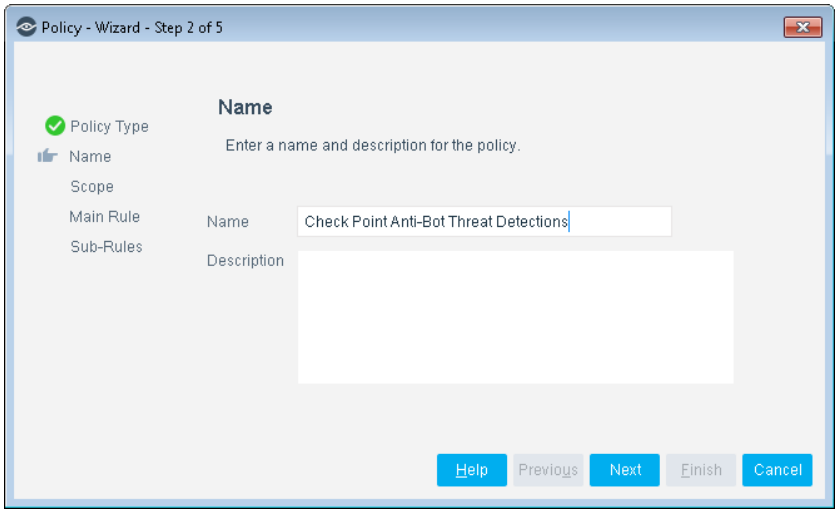
Use this template to create a Forescout platform policy that responds to threats that are detected by the Check Point Anti-Bot blade and reported to the Forescout platform. You can define different responses to threats based on their severity as reported by Check Point Anti-Bot Threat Detections.

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

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

Name the Policy

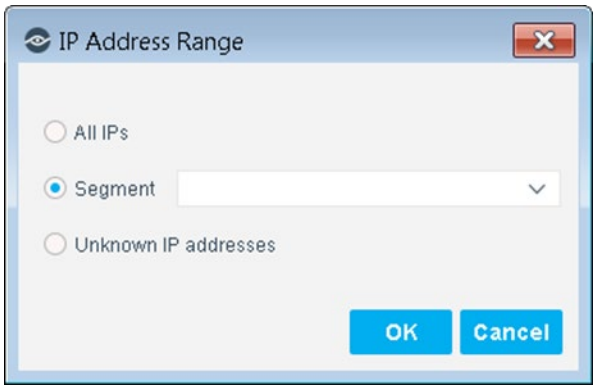
The Name pane lets you define a unique policy name and useful policy description. Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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

Define Which Endpoints Will Be Inspected - Policy Scope

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



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.

- **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 groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range is displayed in the Scope pane.
9. Select **Next**. The Main Rule 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 the Forescout platform 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 the Forescout platform 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 Anti-Virus Threat Detections Policy Template

Use this template to create a Forescout platform policy that responds to threats that are detected by the Check Point Anti-Virus blade and reported to the Forescout platform. 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 Console and select **Policy**.
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**.

Name the Policy

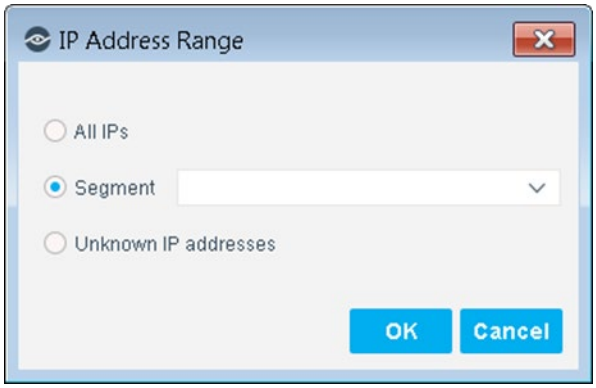
The Name pane lets you define a unique policy name and useful policy description. Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

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

Define Which Endpoints Will Be Inspected - Policy Scope

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



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **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 groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range is displayed in the Scope pane.
9. Select **Next**. The Main Rule 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 the Forescout platform 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 the Forescout platform 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

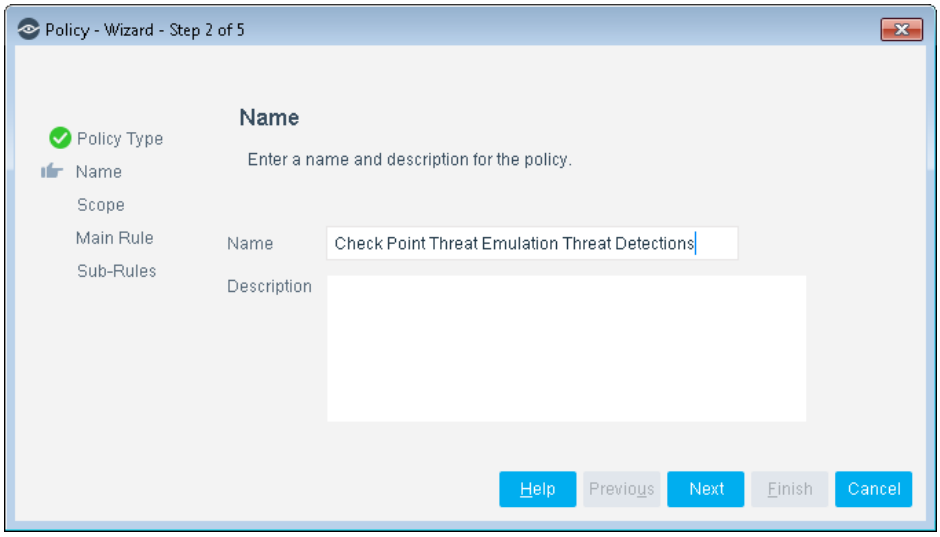
Use this template to create a Forescout platform policy that responds to threats that are detected by the Check Point Threat Emulation blade and reported to the Forescout platform. You can define different responses to threats based on their severity as reported by Check Point Threat Emulation Threat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

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

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

Name the Policy

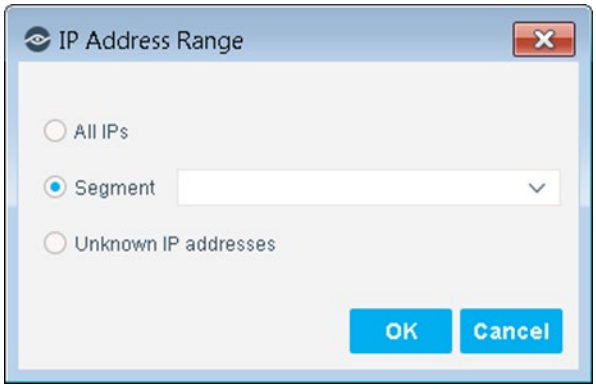
The Name pane lets you define a unique policy name and useful policy description. Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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

Define Which Endpoints Will Be Inspected - Policy Scope

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



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.

– **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 groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range is displayed in the Scope pane.
9. Select **Next**. The Main Rule 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 the Forescout platform 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 the Forescout platform 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 Templates

This module works with the IOC Scanner Plugin – The Forescout platform'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, refer to the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide*.

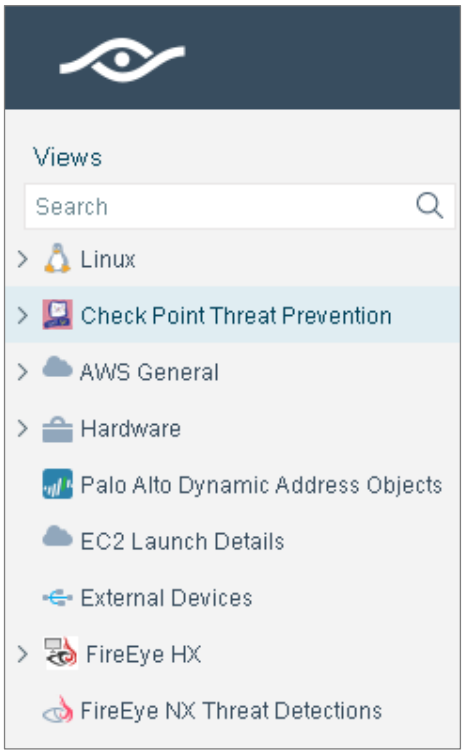
Display Inventory Data

Use the 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 **Inventory** from the Console toolbar.
2. Go to the **Check Point Threat Prevention** folder.



Refer to *Working at the Console>Working with Inventory Detections* in the *Forescout Administration Guide* or the Console Online Help for information about how to work with the Inventory.

Create Custom Check Point Threat Prevention Policies

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

Policies and Rules, Conditions and Actions

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

- Conditions based on host property values. The Forescout platform detects endpoints with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.
- Actions can be applied to endpoints that match the conditions of the rule.

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

- Scan potentially compromised Windows endpoints for IOCs reported by Forescout eyeExtend for Check Point Threat Prevention.
- Remediate infected endpoints.

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

To create a custom policy:

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

Check Point Threat Prevention – Policy Properties

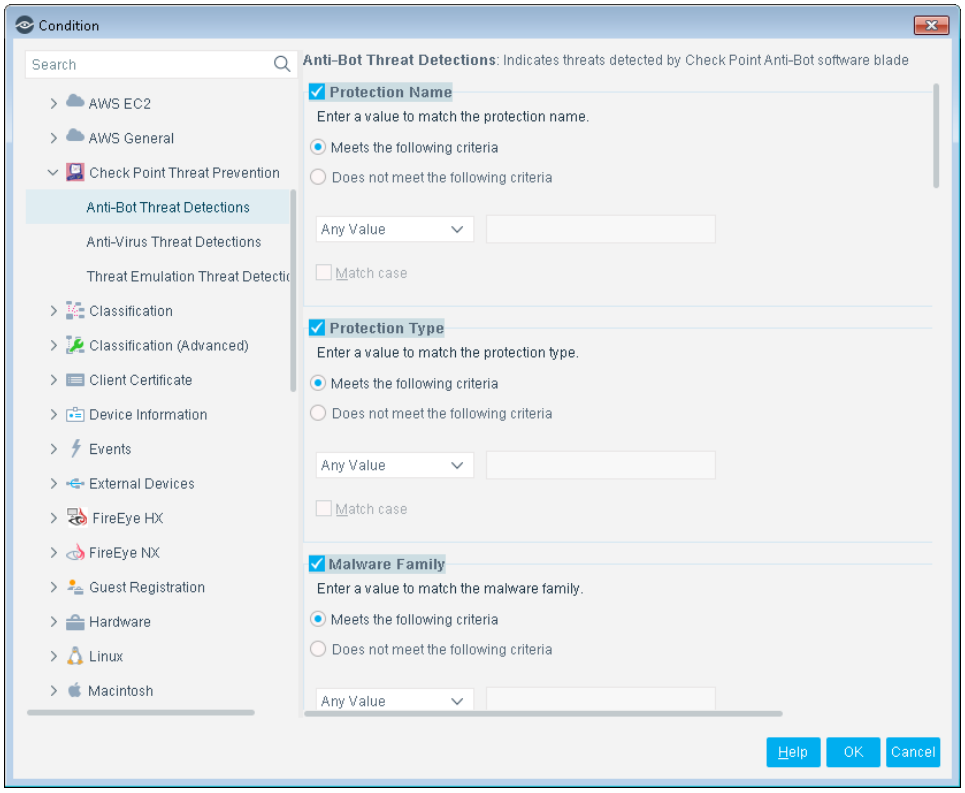
This section describes the properties that are available when you install this module.

To access Check Point Threat Prevention properties:

1. Go 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 Forescout platform 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 Forescout platform 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 Forescout platform 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 *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide* for property details.

Additional Forescout Information

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

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

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

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

To access the Technical Documentation Page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Documentation Portal

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