



# ForeScout

## eyeExtend for Symantec Endpoint Protection

### Configuration Guide

**Version 1.3.1**



## 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](mailto:documentation@forescout.com)

## Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-08-05 14:25

## Table of Contents

<b>About the Symantec Endpoint Protection Integration .....</b>	<b>4</b>
<b>About eyeExtend for Symantec Endpoint Protection .....</b>	<b>6</b>
<b>How to Work with eyeExtend for Symantec Endpoint Protection.....</b>	<b>9</b>
<b>Install eyeExtend for Symantec Endpoint Protection.....</b>	<b>13</b>
<b>Set Up Web Services Client Application .....</b>	<b>14</b>
<b>Configure eyeExtend for Symantec Endpoint Protection.....</b>	<b>19</b>
<b>Create Symantec Endpoint Protection Policies Using Templates .....</b>	<b>25</b>
Create an Anti-Virus Compliance Policy .....	26
Create a Host Infected Policy .....	31
Create a Host Integrity Compliance Policy .....	35
Create an Intrusion Protection Compliance Policy .....	39
Create a Network Threat Protection Compliance Policy .....	43
Create an Online Network for Advanced Response Compliance Policy .....	47
Create a Scan on IOC Alert Policy .....	51
Create Custom Symantec Policies .....	55
<b>Symantec Endpoint Protection Policy Properties .....</b>	<b>55</b>
<b>Symantec Endpoint Protection Policy Actions.....</b>	<b>57</b>
<b>Display Symantec Endpoint-Related Data.....</b>	<b>58</b>

# About the Symantec Endpoint Protection Integration

Symantec™ Endpoint Protection is a security software suite that supports Windows, macOS™/OS X® and Linux® operating systems. Symantec Endpoint Protection consists of endpoint agent software and a manager server. Symantec Endpoint Protection offers a comprehensive endpoint protection platform that provides:

- Anti-virus protection
- Anti-spyware protection
- Intrusion prevention
- Firewall
- Application white/black-listing
- Malware Behavioral Analysis

Forescout eyeExtend for Symantec Endpoint Protection integrates the Forescout platform with the Symantec Endpoint Protection Manager, providing a much tighter and more comprehensive integration covering use cases with the additional features of the Symantec Endpoint Protection Suite.

The Symantec Endpoint Protection Manager has information about the endpoints it manages that may be of use to the Forescout administrator. Examples include information about operating systems, logged on users, and whether the endpoint has anti-virus installed.

This integration lets you:

- Control individual Symantec Endpoint Protection components on all supported operating systems.
- Control network access of endpoints based on Symantec compliance. For example, quarantine a device to a Remediation or Quarantine VLAN until it becomes compliant.
- Ensure endpoints are enrolled with Symantec Endpoint Protection Manager.
- Trigger a full system Symantec Endpoint Protection antivirus scan based on threats reported from other malware detection or Advanced Threat Detection (ATD) products that may be installed in your environment.

## About Certification Compliance Mode

Forescout eyeExtend for Symantec Endpoint Protection supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*.

## Use Cases

This section describes use cases supported by Forescout eyeExtend for Symantec Endpoint Protection. To understand how this eyeExtend module helps you achieve these goals, see [About eyeExtend for Symantec Endpoint Protection](#).

### ***Quarantine on Malware Discovery***

The Symantec Endpoint Protection Manager can be configured with policies that dictate what should happen to an endpoint if malware is discovered on it. Options include the ability to notify the logged-in user, email the administrator, and quarantine or delete the offending file. As an endpoint agent, network-based remediation or quarantining is lacking from this arsenal. By integrating with the Forescout platform, the remediation actions available upon discovery of malware on an endpoint are more comprehensive and extended down to the network layer. See [Create a Network Threat Protection Compliance Policy](#).

### ***Agent Presence Detection & Enrollment with Symantec Endpoint Protection***

All endpoints in a Symantec Endpoint Protection environment should be running a valid Symantec Agent. The Forescout platform can determine whether endpoints have the correct agent installed and running. An endpoint without the agent installed and running can be remediated by the Forescout platform either by automatically enrolling with Symantec Endpoint Protection Manager or by redirecting the user to a portal, where the user is prompted to download and install the Agent before continuing. See [HPS Applications](#).

### ***Corporate Compliance: Ensure Symantec Endpoint Protection Real Time Protection Features are Running***

All corporate endpoints in a Symantec Endpoint Protection environment should not just be running a valid Symantec Agent – they should be configured with the desired features, such as up-to-date anti-virus definitions, and with network threat detection activated. The Forescout platform can determine whether corporate endpoints have the correct agent configurations and report or remediate accordingly. An endpoint that is not in the desired state needs to be remediated by having the necessary components activated and policies updated. See [Create Symantec Endpoint Protection Policies Using Templates](#).

### ***Scan on Third-Party Malware Detection***

When there is reason to suspect the presence of a virus or malware on the corporate network, it may be desirable to enact all available defenses on the corporate endpoints. Although the Symantec Endpoint Protection anti-virus software may be configured to run regular scans, and otherwise perform real-time checking, an extreme situation may call for a full hard disk scan on sensitive endpoints. When the Forescout platform becomes aware of the potential of an Advanced Persistent Threat (APT), virus, or malware by some other third-party tool, using the Symantec anti-virus to scan Symantec-managed endpoints in the network may be one of many measures taken to combat the threat. See [Create a Scan on IOC Alert Policy](#).

### ***Scan non-Symantec Managed Endpoints upon Malware Discovery***

The Forescout platform can be used to react to a problem that Symantec Endpoint Protection discovers on an endpoint. Symantec communicates with the Forescout platform about the threat, and via integration with the IOC Scanner, the Forescout platform can now scan non-Symantec managed endpoints for that same threat. The end result of this use case relates to scanning for the detected malware on non-Symantec Managed Endpoints. See [Indications of Compromise \(IOC\) Scanner](#).

### Additional Symantec Endpoint Protection Documentation

Refer to Symantec Endpoint Protection online documentation for more information about the Symantec Endpoint Protection solution:

<https://techdocs.broadcom.com/>

## About eyeExtend for Symantec Endpoint Protection

Forescout eyeExtend for Symantec Endpoint Protection integrates the Forescout platform with Symantec Endpoint Protection so that you can:

- Use the compliance templates to create policies that detect information about endpoints. If the endpoint is non-compliant, a series of corrective actions takes place and Symantec reports the results to the Forescout platform.
  - [Create an Anti-Virus Compliance Policy](#) – Detects which endpoints have the Symantec Agent installed and running with Auto-Protect enabled.
  - [Create a Host Integrity Compliance Policy](#) – Based on compliance information, the Forescout operator can attempt to remediate or quarantine non-compliant endpoints.
  - [Create a Host Infected Policy](#) – Detects whether an endpoint is infected or not. If infected, the Host Infected policy instructs what actions to take.
  - [Create an Intrusion Protection Compliance Policy](#) – Converts the Intrusion Prevention System configurations from Symantec into compliance information in the Forescout platform.
  - [Create a Network Threat Protection Compliance Policy](#) – Offers the ability to enable Network Threat Protection on endpoints where it is not enabled.
  - [Create an Online Network for Advanced Response Compliance Policy](#) – When an endpoint is not compliant due to the status of the SONAR component, Symantec reports it to the Forescout platform.
- Create policies using other Symantec-related templates:
  - [Create a Scan on IOC Alert Policy](#) – When other Advanced Threat Detection integrations within the Forescout platform detect a threat, that threat is ingested and triggers a scan on Symantec-managed endpoints.
- [Create Custom Symantec Policies](#) that use properties provided by this module, and other Forescout properties and actions, to deal with issues not covered in other policy templates.
- View threats reported by Forescout eyeExtend for Symantec Endpoint Protection and automatically add them to the IOC repository. These IOCs are used by the IOC Scanner Plugin for Advanced Threat Detection (ATD) and recovery. Refer to the [IOC Scanner Plugin Configuration Guide](#) for more information.
- Use Forescout inventory tools to display all threats Symantec Agent status information reported by Symantec and the corresponding endpoints on which they have been found.

To use the module, you should have a solid understanding of Symantec Endpoint Protection concepts, functionality and terminology, and understand how the Forescout platform 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

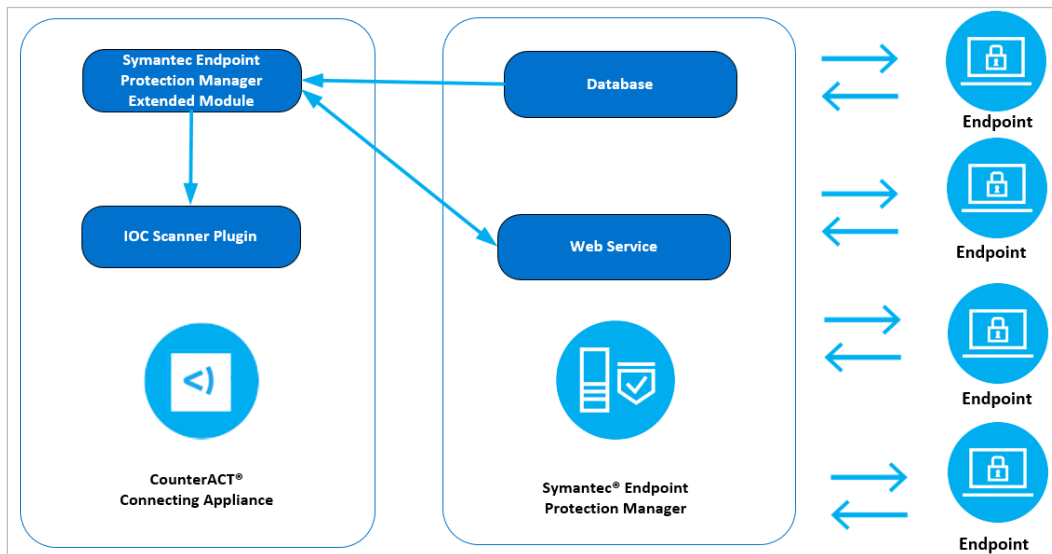
This section provides a basic overview of Symantec Endpoint Protection architecture:

- [Concepts](#) – basic integration concepts.
- [Components](#)– devices in your network that participate in the integration.
- [Considerations](#)– setup details and common network structure issues to keep in mind when you implement this module.

### Concepts

This section addresses core concepts related to Symantec Endpoint Protection.

#### *Logical Representation of Forescout eyeExtend for Symantec Endpoint Protection*



#### *Base Integration and eyeExtend Module Integration*

A base integration of Symantec with the Forescout platform is offered through the Windows Applications Plugin. It includes anti-virus compliance only for Windows systems, ensuring the Symantec Agent is installed and the real-time detection component is running. Existing actions include trigger live update and start the Symantec real-time protection Agent.

Unlike the base integration, which integrates directly with the agent on the endpoint, this eyeExtend module integrates with Symantec Endpoint Protection Manager. It provides a much tighter and more comprehensive integration that covers additional use cases and additional features of the Symantec Endpoint Protection Suite.

### *The Forescout Platform Queries Symantec for Endpoint Information*

When the Symantec Agent runs on corporate endpoints, it provides the Symantec server with endpoint information, such as the state of various Symantec components, as well as generic information such as the name of the user logged into the endpoint. This module presents this endpoint information in the Forescout platform as host properties, which can be included in the Forescout platform policy conditions. To evaluate these properties, the Forescout platform queries the Symantec server via database queries and their web service.

### *Regular Polling Intervals*

The Forescout platform polls the Symantec Manager at regular intervals for some core information, while other information is retrieved on demand.

### *Actions on Endpoints via Queries*

Actions are performed on endpoints by sending queries to the Symantec web service.

### *Deployment Configuration*

Each CounterACT® Appliance can connect to one or more Symantec Endpoint Protection Managers. The connecting Appliance manages all communication with the Symantec Manager for the endpoints managed by the given Symantec Manager. This is irrespective of the scope of IP addresses managed within the Forescout platform by that CounterACT Appliance. In deploying, you should balance the following:

- Minimize bandwidth between the Forescout platform and Symantec by using a connecting CounterACT Appliance that is logically close to the Symantec Endpoint Protection Manager.
- Minimize inter-appliance communication by matching up as much as possible the range of IP addresses managed Symantec Endpoint Protection Manager with the connecting CounterACT Appliance.

### **Components**

This section addresses components that help provide optimal integration of Forescout eyeExtend for Symantec Endpoint Protection.

### *HPS Applications*

HPS Applications are a valuable addition to Forescout eyeExtend for Symantec Endpoint Protection. It lets the Forescout platform see and control the Symantec Agent running on Windows endpoints, even on endpoints where the agent is not managed by the Symantec Endpoint Protection Manager. Specifically, the Forescout platform can detect the following:

- Whether the Symantec Agent is installed
- Whether the real-time detection component of the agent is running
- The latest virus definitions update date

It can also perform the following actions:

- Start the anti-virus real-time protection component of the Symantec Agent
- Trigger an update of virus definitions

HPS Applications achieve this by interacting directly with managed endpoints.

### *Indications of Compromise (IOC) Scanner*

Forescout eyeExtend for Symantec Endpoint Protection works with the Indications of Compromise (IOC) Scanner, the Forescout platform's action center for Advanced Threat Detection (ATD) and response. The IOC Scanner Plugin provides:

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

### **Considerations**

This section addresses additional considerations.

#### *Severity Levels*

Symantec severity levels are mapped to the Forescout platform severity levels.

<b>Symantec Severity Category</b>	<b>Forescout Severity Level</b>
1	Low
2	Medium
3	High
4	Critical
5	Critical

## **How to Work with eyeExtend for Symantec Endpoint Protection**

This topic describes how to work with the module and module requirements.

### **What to Do**

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See [Requirements](#).
2. [Install eyeExtend for Symantec Endpoint Protection](#).
3. [Set Up Web Services Client Application](#).
4. [Configure eyeExtend for Symantec Endpoint Protection](#).
5. [Create Symantec Endpoint Protection Policies Using Templates](#)
6. (Optional) [Create Custom Symantec Policies](#).

## Requirements

Verify that the following requirements are met:

- [ForeScout Requirements](#)
- [ForeScout eyeExtend \(Extended Module\) Licensing Requirements](#)
- [Symantec Endpoint Protection Requirements](#)

## ForeScout Requirements

The module requires the following ForeScout releases and other components:

- ForeScout version 8.1.
- A module license for ForeScout eyeExtend for Symantec Endpoint Protection. See [ForeScout eyeExtend \(Extended Module\) Licensing Requirements](#).
- The Core Extensions Module version 1.1, with the IOC Scanner Plugin running.
- The Windows Applications Content Module (recommended but not required.) Windows Applications is only needed if you want to detect endpoints that have a Symantec Anti-Virus installed but not managed by the Symantec Endpoint Protection Server.

## ForeScout eyeExtend (Extended Module) Licensing Requirements

This ForeScout eyeExtend module 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

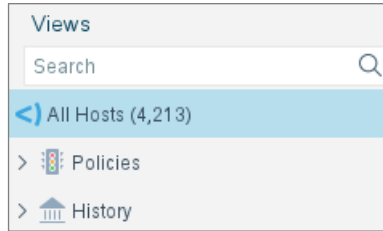
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request 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 modules. 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 modules. 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 modules, packaging individual licensed modules are supported. The eyeExtend Connect Module is an eyeExtend module 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.

### Symantec Endpoint Protection Requirements

The Symantec requirements are as follows:

- Symantec Endpoint Protection Manager version 12.1.6, 14.0.1, or 14.2 installed.
- 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](#).
- Configured to use a SQL Server Database (the embedded database option is not supported).

- The Forescout platform needs to be registered as a Symantec Endpoint Protection Web Services Client Application.

### About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this eyeExtend 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 eyeExtend module.

## Install eyeExtend for Symantec Endpoint Protection

This topic describes how to download and 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.

## Set Up Web Services Client Application

This topic describes the procedures for setting up the Symantec Endpoint Protection Manager Web Services. Perform the following procedures in the order indicated:

- [Register an Application with Symantec Endpoint Protection Manager Web Services](#)
- [Authorize the Forescout Platform to Call Symantec Web Services and Get OAuth Access Token](#)

### Register an Application with Symantec Endpoint Protection Manager Web Services

Before you can work with Symantec Endpoint Protection Manager Web Services, a web services client application must be registered with each of the instances of the Symantec Endpoint Protection Manager that the web services client will manage. Registration is performed on the Symantec Endpoint Protection Manager server and requires a Symantec Endpoint Protection Manager Administrator account. Registration is performed only once for each instance of Symantec Endpoint Protection Manager.

#### To register an application:

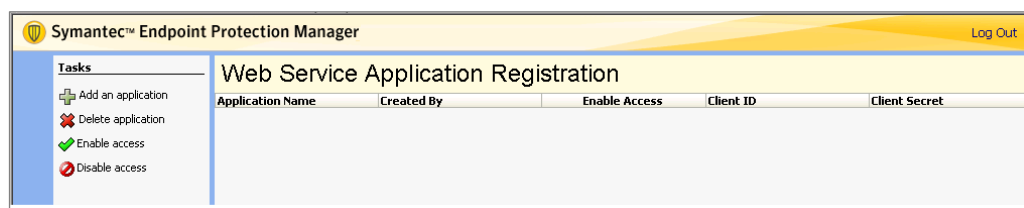
1. Log in as an administrator to the instance of Symantec Endpoint Protection Manager at the following URL:

`https://<hostname>:<port_number>/sepm/viewLoginRMM.do`

Construct the URL by populating specific items with your information:

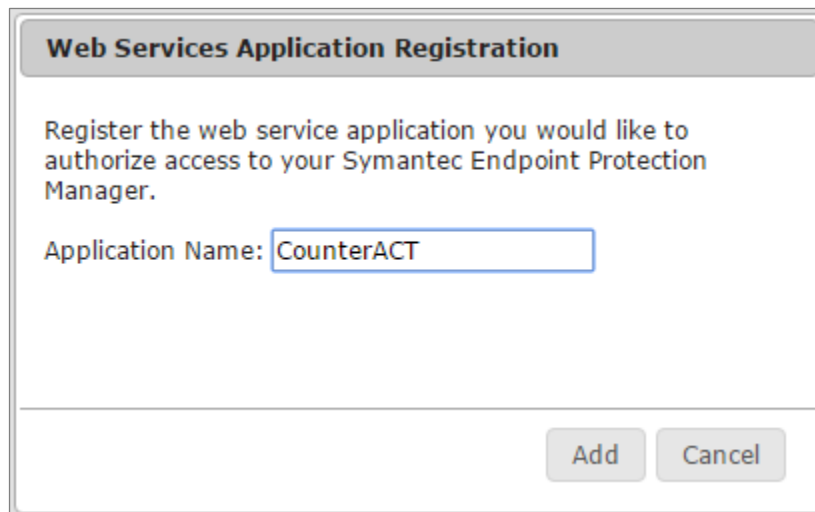
<b>&lt;hostname&gt;</b>	Enter the IP address or hostname of the installed instance of Symantec Endpoint Protection Manager.
<b>&lt;port_number&gt;</b>	Enter the web services port of the installed instance of Symantec Endpoint Protection Manager. The default port number is 8446.

2. Press **<Enter>**.



3. Select **Add an application** and enter the application information.

4. Provide a name for the application that will connect to Symantec Endpoint Protection.



**Web Services Application Registration**

Register the web service application you would like to authorize access to your Symantec Endpoint Protection Manager.

Application Name:

5. When the Web Service is registered, the Client ID and the Client Secret are displayed.

Symantec™ Endpoint Protection Manager

Log Out

Tasks

- Add an application
- Delete application
- Enable access
- Disable access

Web Service Application Registration

Application Name	Created By	Enable Access	Client ID	Client Secret
CounterACT	admin			
	admin			
	admin			

6. Copy the Client ID and the Client Secret to a safe place for future reference.
7. In the Web Service Application page, select **Enable access**.
8. Proceed to [Authorize the Forescout Platform to Call Symantec Web Services and Get OAuth Access Token](#).

### Authorize the Forescout Platform to Call Symantec Web Services and Get OAuth Access Token

After you register an application with Symantec Endpoint Protection Manager Web Services, you need to authorize that application to call the Symantec Web Services.

You also need to copy the OAuth Access Token from the authorization code. OAuth (Open Authorization) is an open standard for token-based authentication and authorization on the Internet. OAuth allows an end user's account information to be used by third-party services without exposing the user's password. OAuth acts as an intermediary on behalf of the end user, providing the service with an access token that authorizes specific account information to be shared.

The following two procedures depend on the Symantec Endpoint Protection Manager version. The first procedure is for versions lower than 14.2. The second procedure is for version 14.2.

**To authorize an application and obtain the access token on versions below 14.2:**

1. In the browser window that opened after you registered the application, construct the URL by populating specific items with your information:

```
https://<hostname>:<port_number>/sepm/oauth/authorize?response_type=code&client_id=<client_id>&redirect_uri=https://<hostname>:<port_number>/sepm
```

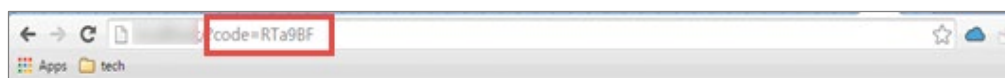
<hostname>	Enter the IP address or hostname of the installed instance of Symantec Endpoint Protection Manager.
<port_number>	Enter the web services port of the installed instance of Symantec Endpoint Protection Manager. The default port number is 8446.
<client_id>	Enter the Client ID that was provided when the application was registered.

2. Log in to the Symantec Endpoint Protection Manager Web Services as an administrator.



3. Select **Authorize**.

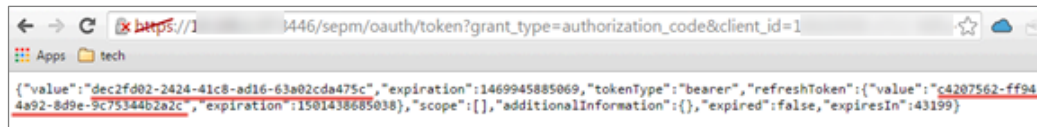
The return page may display as an empty (blank) page. However, the code is visible in the page's URL. In the example shown, the URL contains a code number: RTa98F. Copy the code number to a safe place.




4. In the browser window where you authorized the Symantec Web Service access, open a new browser page and enter the following URL, replacing the <hostname>, <port>, <clientid>, <clientsecret>, and <code> with those that you have collected.

```
https://<hostname>:<port>/sepm/oauth/token?grant_type=authorization_code&client_id=<clientid>&client_secret=<clientsecret>&redirect_uri=https://<hostname>:<port_number>/sepm&code=<code>
```

The returned page is in JSON format. The access token is in the value field. The refresh token is in the `refreshToken` value field. For example:



5. Copy these values to a safe place. You will need to enter them in the CounterACT device configuration. See [Configure eyeExtend for Symantec Endpoint Protection](#).

 *The hostname, port, client ID, client secret, and code need to be stored securely.*

### To authorize an application and obtain the access token on version 14.2:

1. In the browser window that opened after you registered the application, construct the URL by populating specific items with your information:

```
https://<hostname>:<port_number>/sepm/oauth/authorize?response_type=code&client_id=<client_id>
```

<hostname>	Enter the IP address or hostname of the installed instance of Symantec Endpoint Protection Manager.
<port_number>	Enter the web services port of the installed instance of Symantec Endpoint Protection Manager. The default port number is 8446.
<client_id>	Enter the Client ID that was provided when the application was registered.

2. Log in to the Symantec Endpoint Protection Manager Web Services as an administrator.



**3. Select **Authorize**.**

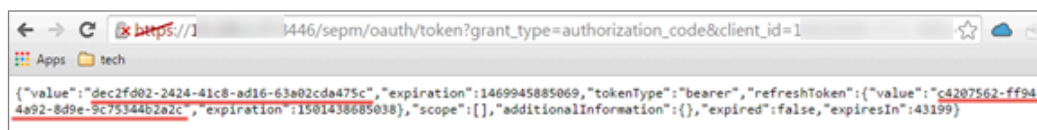
The return page may display as an empty (blank) page. However, the code is visible in the page's URL. In the example shown, the URL contains a code number: RTa98F. Copy the code number to a safe place.




**4. In the browser window where you authorized the Symantec Web Service access, open a new browser page and enter the following URL, replacing the <hostname>, <port\_number>, <client\_id>, <client\_secret>, and <code> with those that you have collected.**

**`https://<hostname>:<port_number>/sepm/oauth/token?grant_type=authorization_code&client_id=<client_id>&client_secret=<client_secret>&code=<code>`**

The returned page is in JSON format. The access token is in the value field. The refresh token is in the **refreshToken** value field. For example:



**5. Copy these values to a safe place. You will need to enter them in the CounterACT device configuration. See [Configure eyeExtend for Symantec Endpoint Protection](#).**

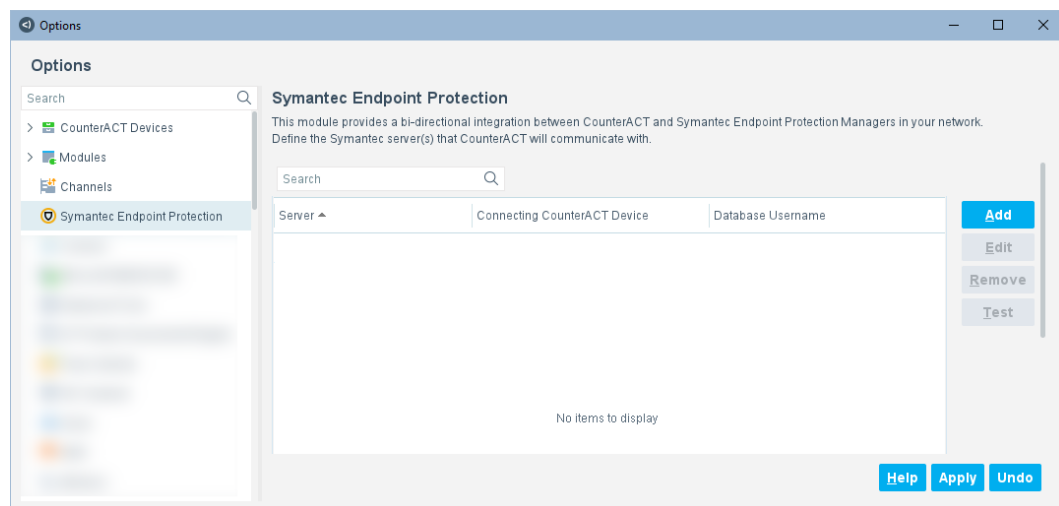
 *The hostname, port\_number, client\_id, client\_secret, and code need to be stored securely.*

# Configure eyeExtend for Symantec Endpoint Protection

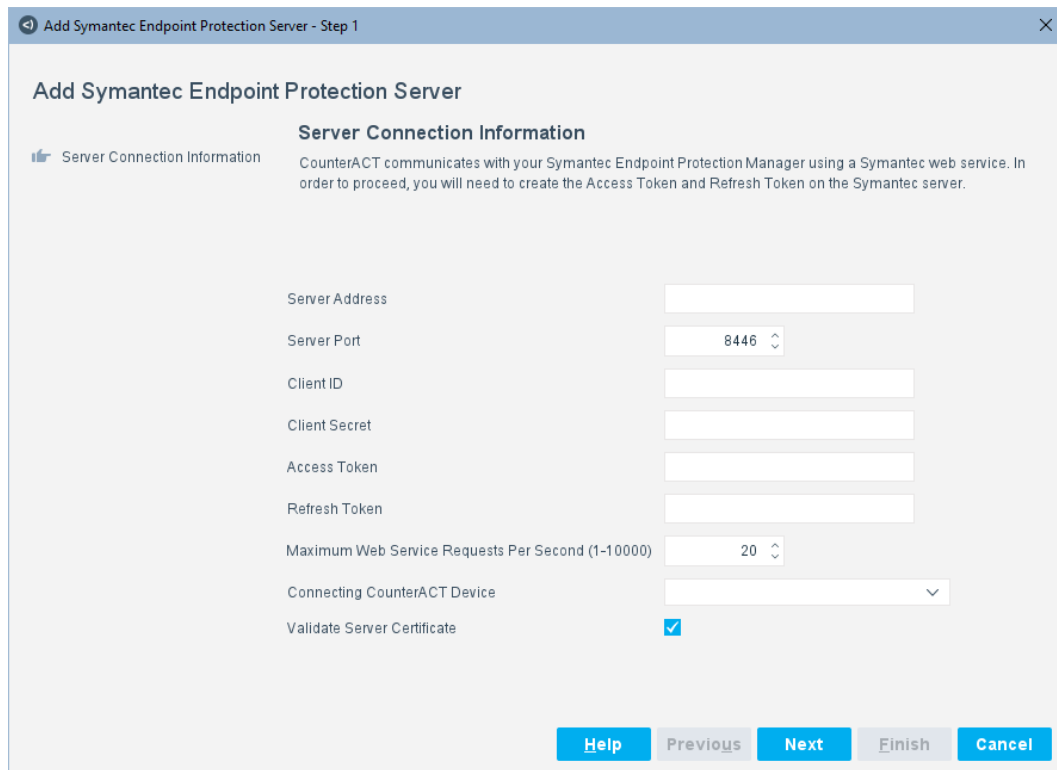
Configure the module to ensure that the Forescout platform can communicate with the Symantec Endpoint Protection suite. You can only have one connection to the Symantec Endpoint Protection Manager server.

## To configure the module:

1. In the Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Select **Modules**.
3. In the Modules pane, select **Symantec Endpoint Protection**, and select **Configure**.



4. Select **Add** to define a Symantec Endpoint Protection server to communicate with the Forescout platform.



5. Configure the following settings:

<b>Server Address</b>	Enter the server address, a Fully Qualified Domain Name (FQDN), or the IPv4 address of the Symantec server that sends notifications to the Forescout platform.
<b>Server Port</b>	Enter the Symantec server port.
<b>Client ID</b>	Enter the client ID of the Symantec web services port. The default value is 8446.
<b>Client Secret</b>	Enter the OAUTH client credentials.
<b>Access Token</b>	Enter the OAUTH access token to make web service API calls. You can generate the access key manually. See <a href="#">Authorize the Forescout Platform to Call Symantec Web Services and Get OAuth Access Token</a> .
<b>Refresh Token</b>	Enter the OAUTH refresh token that refreshes the access token when it expires. An access token lasts 12 hrs. There is no control mechanism to increase or adjust the expiration. However, when the old token expires, Forescout eyeExtend for Symantec Endpoint Protection automatically gets a new access token using the Refresh Token. See <a href="#">Authorize the Forescout Platform to Call Symantec Web Services and Get OAuth Access Token</a> .

<b>Maximum Web Service Requests Per Second (1-10000)</b>	Enter the number of web service requests per second (rate limiting). It is recommended to leave the default setting and only adjust later if troubleshooting the integration is required.
<b>Connecting CounterACT Device</b>	Select a CounterACT device to apply the server configurations to. Do not select the Enterprise Manager to be the connecting CounterACT device.
<b>Validate Server Certificate</b>	<p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> <li>Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance</li> <li>Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance</li> </ul> <p>Use the Certificates &gt; Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>

## 6. Select **Next**.

Add Symantec Endpoint Protection Server - Step 2 of 2

### Add Symantec Endpoint Protection Server

☒ Server Connection Information  
☐ Database Server Connection Information

#### Database Server Connection Information

Define the Symantec Enterprise Manager Database server that CounterACT will use. If the Windows authentication is used, the user domain and name can be entered as the Database Administrator username.


Database Server   
☐ Server Instance   
☒ Port

Database Name   
 Database Administrator username   
 Database Administrator password   
 Verify Database Administrator password   
 Polling Interval Minutes (0-60)

7. Configure the following settings.

<b>Database Server</b>	Enter the SQL server database (required) that Forescout eyeExtend for Symantec Endpoint Protection uses. Then configure one of the following: <ul style="list-style-type: none"> <li>▪ <b>Server Instance</b> – Enter a customized name of the SQL Instance. For example: Forescout_SQL_Instance</li> <li>▪ <b>Port</b> – Select the SQL server database port number. The default is 1433.</li> </ul>
<b>Database Name</b>	Enter the name of the SQL server database.
<b>Database Administrator username</b>	Enter the administrator username used to access the SQL server database. Both Windows authentication and SQL authentication are supported. <ul style="list-style-type: none"> <li>▪ For Windows authentication, the database administrator username is user domain name followed by backslash and then username. For example, <b>forescout\john.smith</b>.</li> <li>▪ For SQL authentication, the username is the SQL username, for example, <b>sa</b>.</li> </ul>
<b>Database Administrator password</b>	Enter the administrator password used to access the SQL server database. When the administrator password is changed, the Refresh Token expires, and you need to regenerate a new Access Token and Refresh Token.
<b>Verify Database Administrator password</b>	Re-enter the administrator password.
<b>Polling Interval Minutes (0-60)</b>	Database polling can be disabled by setting the interval to 0. Disabling polling stops Forescout eyeExtend for Symantec Endpoint Protection from discovering new endpoints and the detailed information about an infected endpoint. This information (name, filename, hash, hash type and severity) is sent to the IOC scanner during the polling, if the host is infected, or when the Host Infected property is resolved.

8. Select **Finish**. An entry for the Symantec server is added to the list in the Symantec Endpoint Protection pane.
9. (Optional) Repeat these steps to define additional Symantec Endpoint Protection Managers.
10. In the Symantec Endpoint Protection pane, select **Apply**. An Enterprise Manager Console dialog box opens.
11. Select **Yes** to save the module configuration, and then select **Close**.

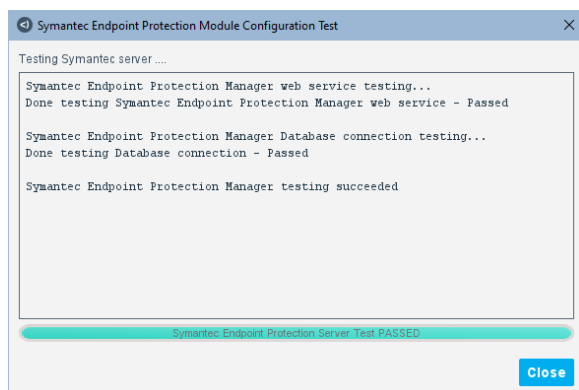
 *The best practice is to perform a test after setting up a connection. See [Test the Module](#).*

## Test the Module

It is recommended to test communication with Symantec servers after setting up a connection.

### To run the test:

1. In the Symantec Endpoint Protection pane, select a server, and select **Test**.



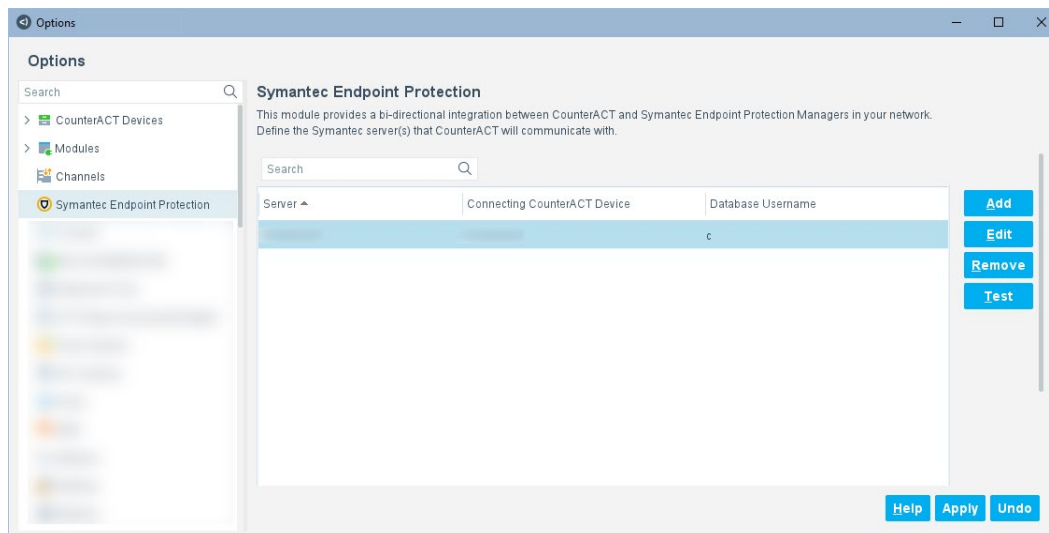
2. After viewing the test results, select **Close**.

## Edit a Server

You can edit a server configuration.

### To edit a server configuration:

1. In the Symantec Endpoint Protection pane, select a configured server.



**2. Select Edit.**

**Edit Symantec Endpoint Protection Server**

Server Connection Information    Database Server Connection Information

**Server Connection Information**

CounterACT communicates with your Symantec Endpoint Protection Manager using a Symantec web service. In order to proceed, you will need to create the Access Token and Refresh Token on the Symantec server.

Server Address:

Server Port: 8446

Client ID:

Client Secret:

Access Token:

Refresh Token:

Maximum Web Service Requests Per Second (1-10000): 20

Connecting CounterACT Device:

Validate Server Certificate: ☒

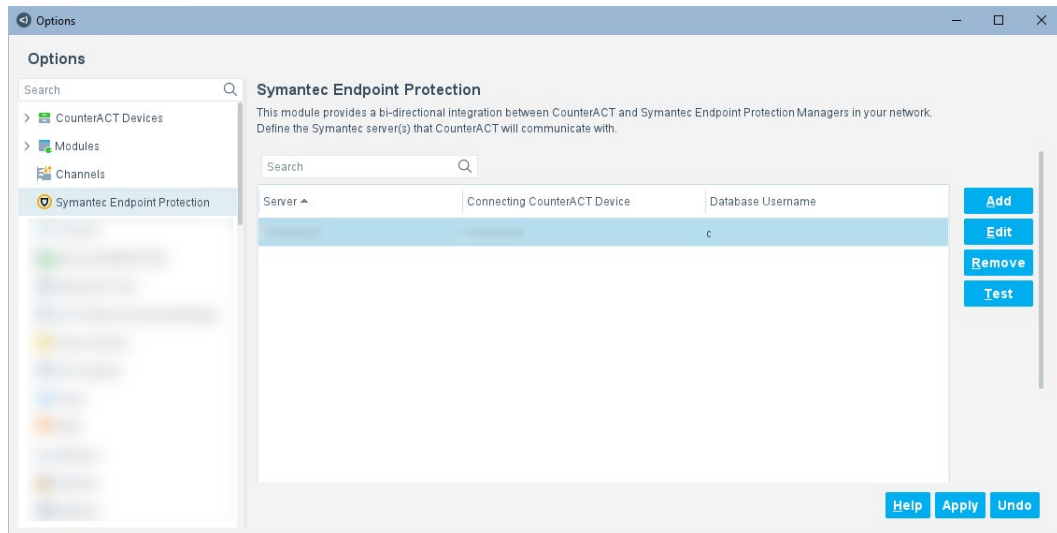
Help OK Cancel

**3. Edit the parameters in the Server Connection Information and Database Server Connection Information tabs.****4. Select OK.****5. In the Symantec Endpoint Protection pane, select Apply.****Remove a Server**

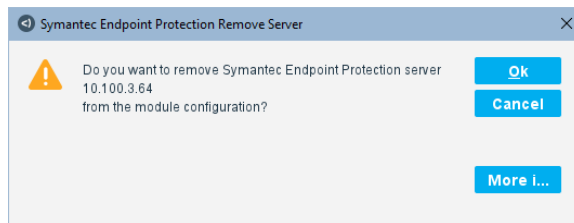
You can remove a server configuration.

**To remove a server configuration:**

1. In the Symantec Endpoint Protection pane, select a configured server.



2. Select **Remove**.



3. For more information, select **More Info**.
4. Select **OK**.
5. In the Symantec Endpoint Protection pane, select **Apply**.

## Create Symantec Endpoint Protection Policies Using Templates

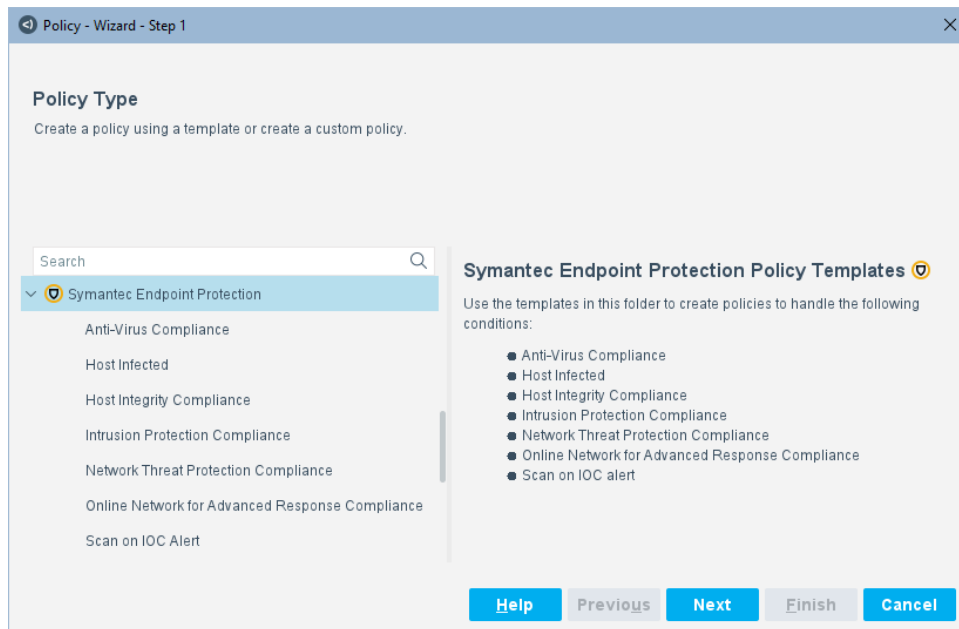
Forescout templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.


Predefined actions, which are 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.

This topic describes how to use templates to create policies to detect and manage endpoints. See the following:

- [Create an Anti-Virus Compliance Policy](#)
- [Create a Host Infected Policy](#)

- [Create a Host Integrity Compliance Policy](#)
- [Create an Intrusion Protection Compliance Policy](#)
- [Create a Network Threat Protection Compliance Policy](#)
- [Create an Online Network for Advanced Response Compliance Policy](#)
- [Create a Scan on IOC Alert Policy](#)
- [Create Custom Symantec Policies](#)



 *It is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to [Policy Templates](#) and [Policy Management](#) in the Forescout Administration Guide.*

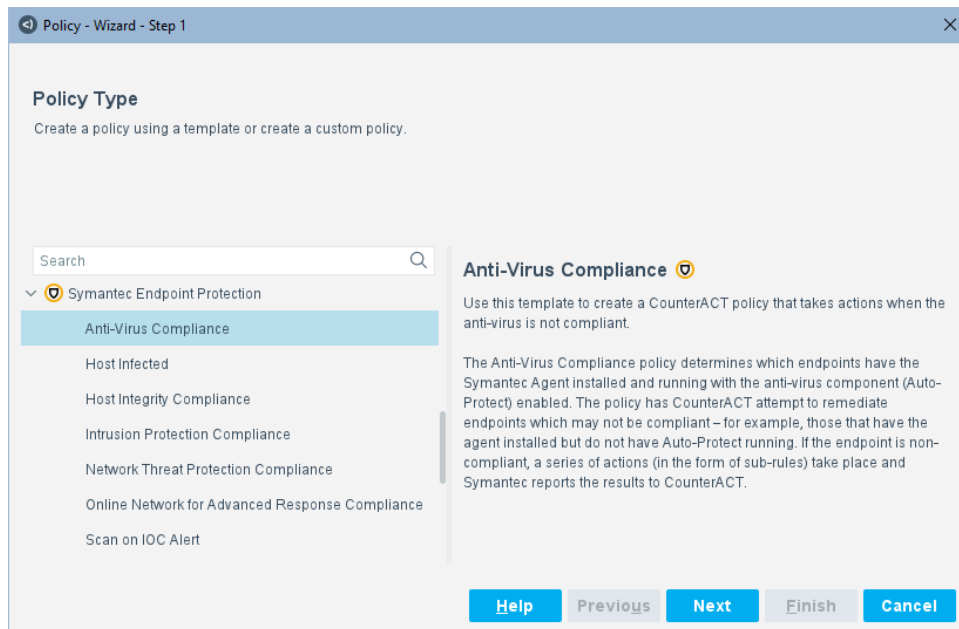
## Create an Anti-Virus Compliance Policy

Symantec Endpoint Protection provides anti-virus protection by proactively scanning endpoints for known and unknown threats, such as viruses, worms, Trojan horses, and adware. The Anti-Virus Compliance policy determines which endpoints have the Symantec Agent installed and running with the anti-virus component (Auto-Protect) enabled. The policy has the Forescout platform attempt to remediate endpoints which may not be compliant; for example, those that have the agent installed but do not have Auto-Protect running. If the endpoint is non-compliant, a series of actions (in the form of sub-rules) take place and Symantec reports the results to the Forescout platform.

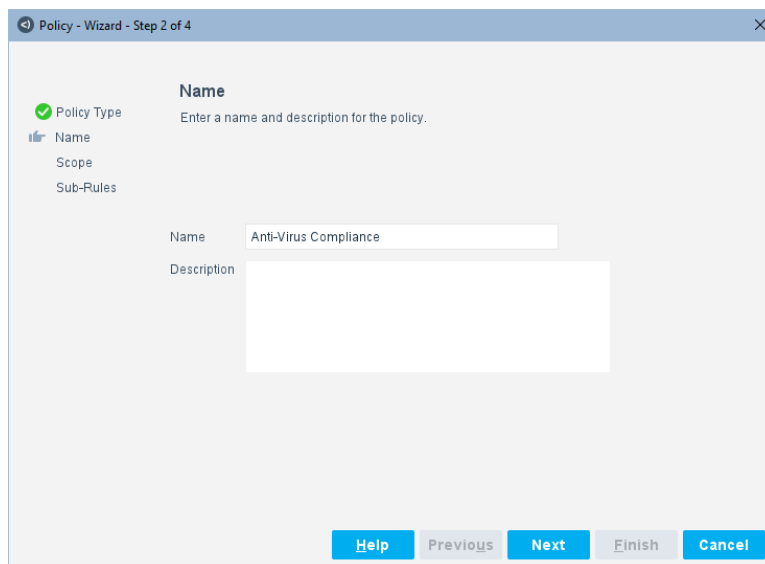
### To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.

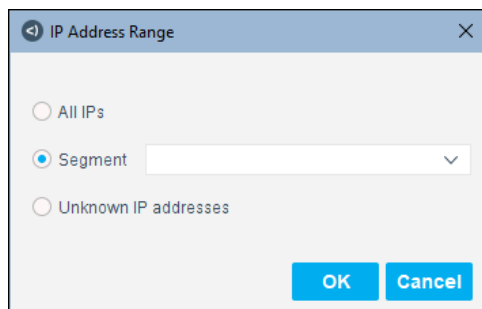
3. Expand the **Symantec Endpoint Protection** folder and select **Anti-Virus Compliance**.



4. Select **Next**.



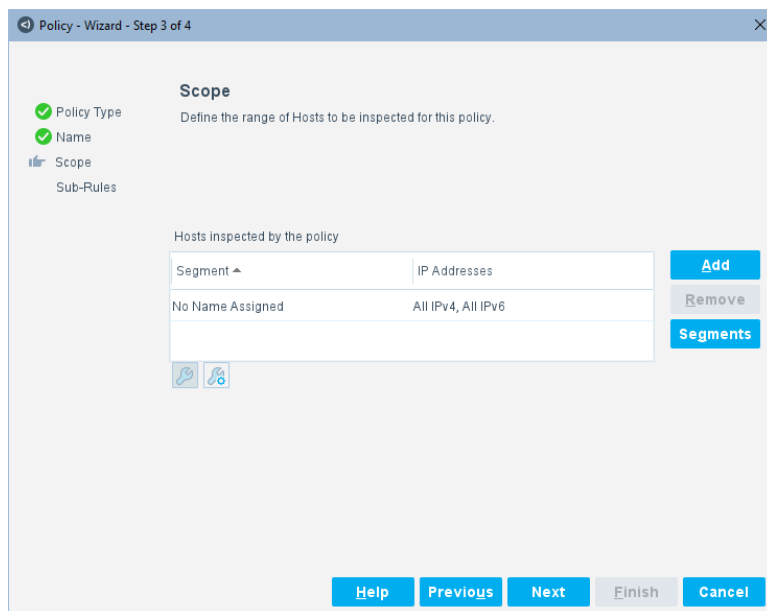
5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

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

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



## 9. Select **Next**.

**Policy - Wizard - Step 4 of 4**

☒ Policy Type  
☒ Name  
☒ Scope  
☒ Sub-Rules

**Sub-Rules**

Use this screen to review policy sub-rule definitions.  
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

	Name	Conditions	Actions	Exceptions
1	Symantec - Auto-Protect running and up-to-date	Symantec - Auto-Protection Status: On AND NOT Symantec - Anti-Virus ...		
2	Symantec - Auto-Protect running but definitions older than 1 week	Symantec - Auto-Protection Status: On	<input checked="" type="checkbox"/>	
3	Symantec - Auto-Protect installed but not running	Symantec - Auto-Protection Status: Off	<input checked="" type="checkbox"/>	
4	Symantec Managed but no recent activity	Symantec - Last Synchronization Time: Older than 1 week, Older than 1 ...		
5	Symantec Managed but Auto-Protect not installed	Symantec - Host Managed: AND Symantec - Auto-Protection Status: No...	<input checked="" type="checkbox"/>	
6	Not managed by Symantec - but Symantec Anti-Virus installed	Windows Antivirus Installed: Symantec AND Member of Group: Windows		
7	Symantec Anti-Virus not installed nor running	No Conditions		

**Add**  
Edit  
Remove  
Duplicate  
Up  
Down

**Help** **Previous** **Next** **Finish** **Cancel**

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Symantec – Auto-Protect running and up-to-date**) to open a Sub-Rule dialog box.

Policy: 'Anti-Virus Compliance'-->Sub-Rule: 'Symantec - Auto-Protect running an...' X



**Name**

Name Symantec - Auto-Protect running and up-to-date **Edit**

Description Symantec - Auto-Protect running and up-to-date

**Condition**

A host matches this rule if it meets the following condition:

Advanced view  

Not	(	Criteria	)	And/Or	Add
<input type="checkbox"/>		Symantec - Auto-Protection Status - ...		AND	Edit
<input checked="" type="checkbox"/>		Symantec - Anti-Virus Definition Date...			Remove
					Up
					Down

**Actions**

Actions are applied to hosts matching the above condition.

Enable	Action	Details	Add
			Edit
			Remove

No items to display

**Advanced**

Recheck match Every 8 hours, All admissions **Edit**

Exceptions None.

**Help** **OK** **Cancel**

Sub-rules let you automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

The Sub-rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the endpoint is checked for Anti-Virus Compliance. The rules are predefined to take action based upon the endpoint being non-compliant with Symantec Anti-Virus. Due to the Anti-Virus Compliance policy scope, action is triggered on any endpoint that meets the default requirements.

Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. For example, one sub-rule catches endpoints which have nothing installed. Another sub-rule finds endpoints that have the agent installed, but not running.

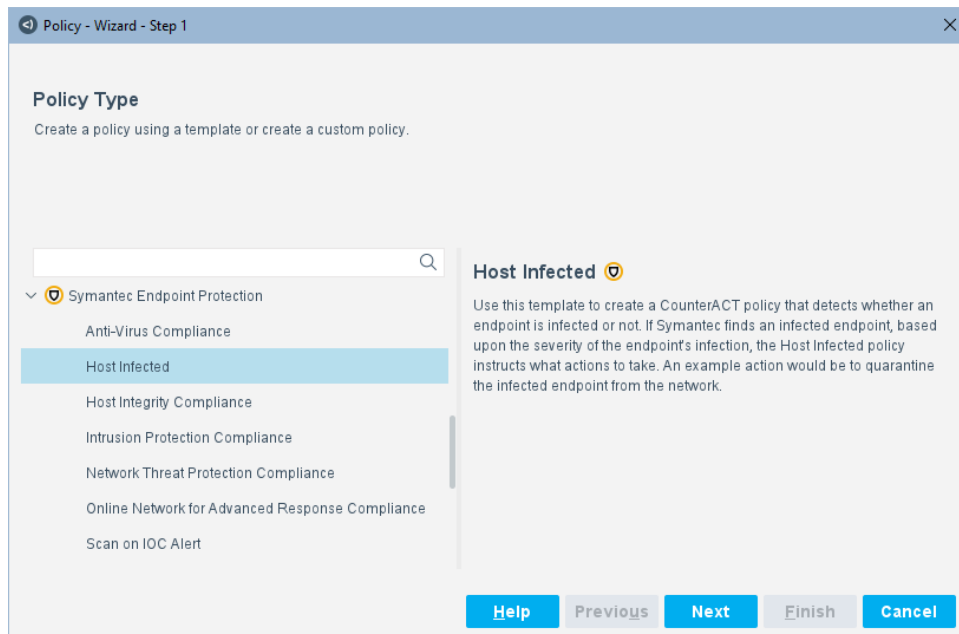
11. Review the sub-rule conditions and actions.
12. To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).
13. To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

## Create a Host Infected Policy

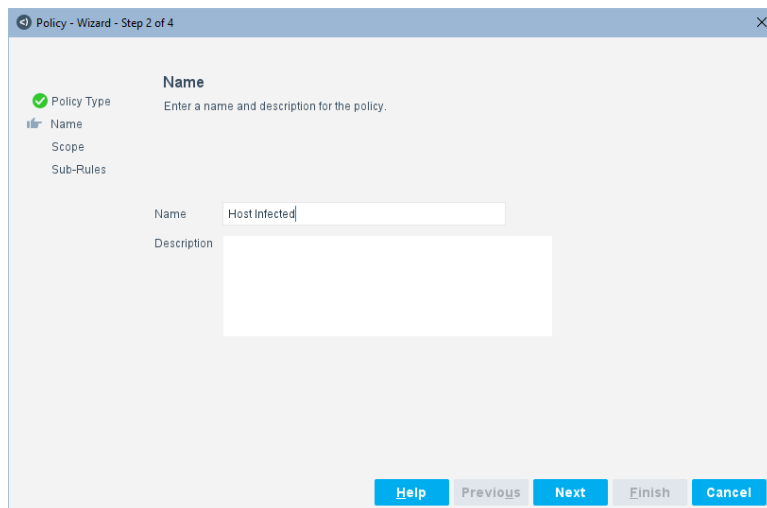
Symantec Endpoint Protection detects whether an endpoint is infected or not. If Symantec finds an infected endpoint, based upon the severity of the endpoint's infection, the Host Infected policy instructs what actions to take. For example, the policy action might quarantine the infected endpoint from the network.

### To create a policy:

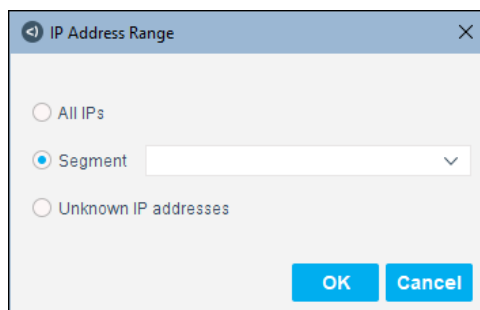
1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Host Infected**.



#### 4. Select **Next**.



5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

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

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

The screenshot shows the 'Policy - Wizard - Step 3 of 4' dialog box with the 'Scope' tab selected. The left sidebar shows 'Policy Type' and 'Name' as completed steps, and 'Scope' and 'Sub-Rules' as the current steps. The main area is titled 'Scope' and contains the instruction 'Define the range of Hosts to be inspected for this policy.' Below this, a section 'Hosts inspected by the policy' contains a table with two rows: 'Segment' with 'IP Addresses' and 'No Name Assigned' with 'All IPv4, All IPv6'. To the right of the table are 'Add', 'Remove', and 'Segments' buttons. At the bottom are 'Help', 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

9. Select **Next**.

The screenshot shows the 'Policy - Wizard - Step 4 of 4' dialog box with the 'Sub-Rules' tab selected. The left sidebar shows 'Policy Type', 'Name', and 'Scope' as completed steps, and 'Sub-Rules' as the current step. The main area is titled 'Sub-Rules' and contains the instruction 'Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.' Below this, a table lists seven sub-rules. To the right of the table are 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', and 'Down' buttons. At the bottom are 'Help', 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

Name	Conditions	Actions	Exceptions
1 Not Infected, and No Recent Infections	NOT Symantec - Host Infected: AND ALL Symantec - Host Infection Informa...		
2 Not Infected Now, But Recently Infected	NOT Symantec - Host Infected:		
3 Low Severity Infection	Symantec - Host Infected: AND ALL Symantec - Host Infection Information : ...		
4 Medium Severity Infection	Symantec - Host Infected: AND ALL Symantec - Host Infection Information : ...		
5 High Severity Infection	Symantec - Host Infected: AND ALL Symantec - Host Infection Information : ...		
6 Critical Severity Infection	Symantec - Host Infected: AND ALL Symantec - Host Infection Information : ...		
7 Infected for Over a Week	No Conditions		

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Not Infected, and No Recent Infections**) to open a Sub-Rule dialog box.

The screenshot shows a dialog box titled "Policy: 'Host Infected' --> Sub-Rule: 'Not Infected, and No Recent Infections'". The dialog is divided into several sections:

- Name:** Shows the rule name "Not Infected, and No Recent Infections" and a description "None." with an "Edit" button.
- Condition:** States "A host matches this rule if it meets the following condition:". It includes a dropdown menu set to "All criteria are True" and a list of criteria:
  - Criteria
  - NOT Symantec - Host Infected
  - ALL Symantec - Host Infection Information - Symantec - Host Infection ...
 Buttons for "Add", "Edit", and "Remove" are on the right.
- Actions:** States "Actions are applied to hosts matching the above condition.". It features a table with columns "Enable", "Action", and "Details". The table is currently empty, showing "No items to display". Buttons for "Add", "Edit", and "Remove" are on the right.
- Advanced:** Includes "Recheck match" set to "Every 8 hours, All admissions" and "Exceptions" set to "None.", with an "Edit" button.

At the bottom are "Help", "OK", and "Cancel" buttons.

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The rules are predefined to take action based upon the severity of the endpoint's infection. Due to the Host Infected policy scope, action is triggered on any endpoint that meets the default requirements.

The sub-rules of this policy take action based upon the severity of the endpoint's infection.

- 11.** Review the sub-rule conditions and actions.
- 12.** To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).
- 13.** To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).

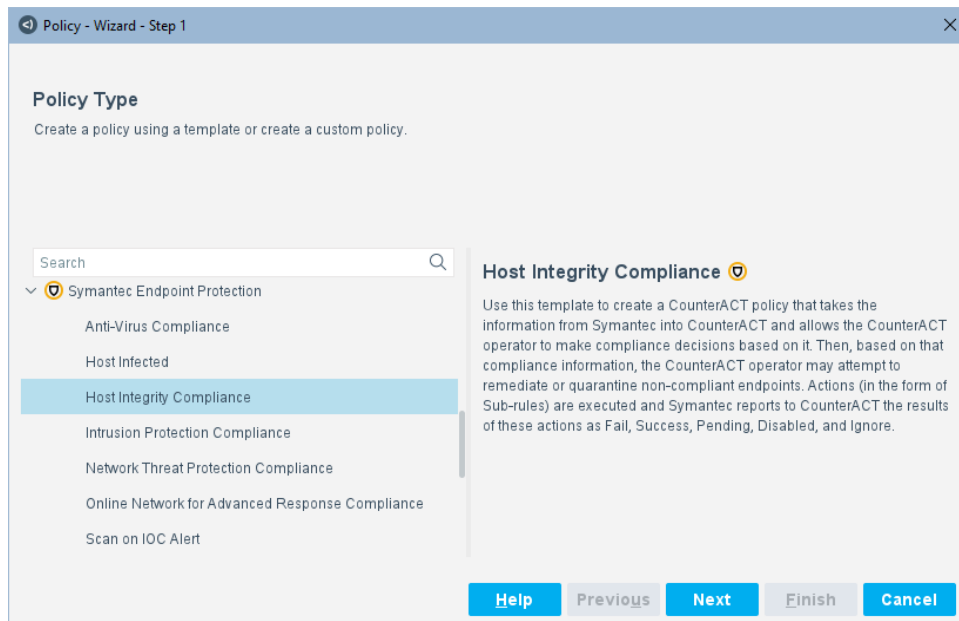
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

## Create a Host Integrity Compliance Policy

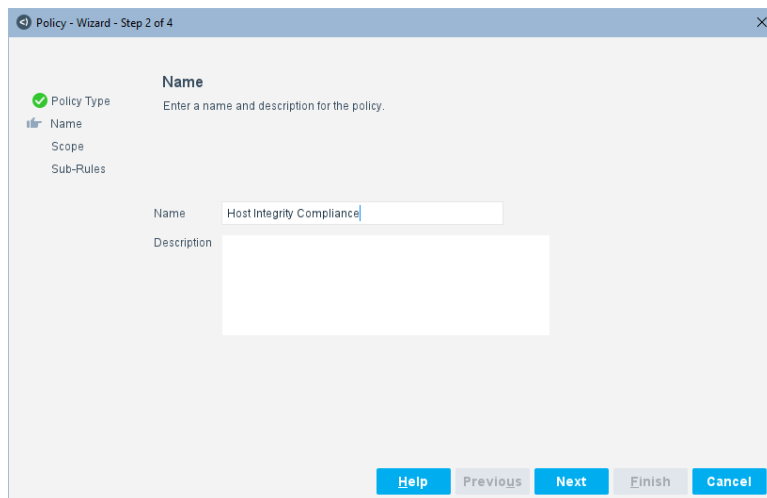
The Host Integrity Compliance policy takes the information from Symantec into the Forescout platform and lets the Forescout operator make compliance decisions based on it. Then, based on that compliance information, the Forescout operator may attempt to remediate or quarantine non-compliant endpoints. Actions (in the form of Sub-rules) are executed and Symantec reports to the Forescout platform the results of these actions as Fail, Success, Pending, Disabled, and Ignore.

### To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Host Integrity Compliance**.



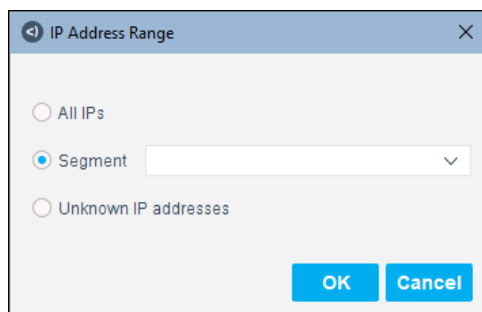
#### 4. Select **Next**.



5. Enter a name for the policy. Optionally, enter a description.

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

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



The following options are available:

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

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

The screenshot shows the 'Policy Wizard - Step 3 of 4' window. On the left, a sidebar lists 'Policy Type', 'Name', 'Scope', and 'Sub-Rules', with 'Scope' selected. The main area is titled 'Scope' and contains the instruction 'Define the range of Hosts to be inspected for this policy.' Below this, a table titled 'Hosts inspected by the policy' has two columns: 'Segment' and 'IP Addresses'. The first row shows 'No Name Assigned' and 'All IPv4, All IPv6'. To the right of the table are buttons for 'Add', 'Remove', and 'Segments'. At the bottom of the window are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

9. Select **Next**.

The screenshot shows the 'Policy Wizard - Step 4 of 4' window. On the left, a sidebar lists 'Policy Type', 'Name', 'Scope', and 'Sub-Rules', with 'Sub-Rules' selected. The main area is titled 'Sub-Rules' and contains the instruction 'Use this screen to review policy sub-rule definitions.' Below this, a table titled 'Sub-Rules' has four columns: 'Name', 'Conditions', 'Actions', and 'Exceptions'. The table lists five sub-rules. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', and 'Down'. At the bottom of the window are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

	Name	Conditions	Actions	Exceptions
1	Symantec Host Integrity Status: SUCCESS	Symantec - Host Integrity Status: Success		
2	Symantec Host Integrity Status: IGNORE	Symantec - Host Integrity Status: Ignore		
3	Symantec Host Integrity Status: PENDING	Symantec - Host Integrity Status: Pending		
4	Symantec Host Managed: FAILURE	Symantec - HostManaged:		
5	NotManaged by Symantec	No Conditions		

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Symantec Host Integrity Status: SUCCESS**) to open a Sub-Rule dialog box.

Policy: 'Host Integrity Compliance' --> Sub-Rule: 'Symantec Host Integrity Status: SU...' X

**Name**

Name Symantec Host Integrity Status: SUCCESS Edit

Description Symantec Host Integrity Status: SUCCESS

**Condition**

A host matches this rule if it meets the following condition:

All criteria are True ⚙️

Criteria	
Symantec - Host Integrity Status - Success	<span>Add</span> <span>Edit</span> <span>Remove</span>

**Actions**

Actions are applied to hosts matching the above condition.

Enable Action	Details	
No items to display		<span>Add</span> <span>Edit</span> <span>Remove</span>

**Advanced**

Recheck match Every 8 hours, All admissions Edit

Exceptions None.

Help OK Cancel

Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. The sub-rules of this policy detect the non-compliance of an endpoint's integrity.


Sub-rules let you automatically follow up with endpoints after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The rules are predefined to take action based upon the non-compliance of the endpoint's integrity. Due to the Host Integrity Compliance policy scope, action is triggered on any endpoint that meets the default requirements.

11. Review the sub-rule conditions and actions.
12. To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).
13. To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

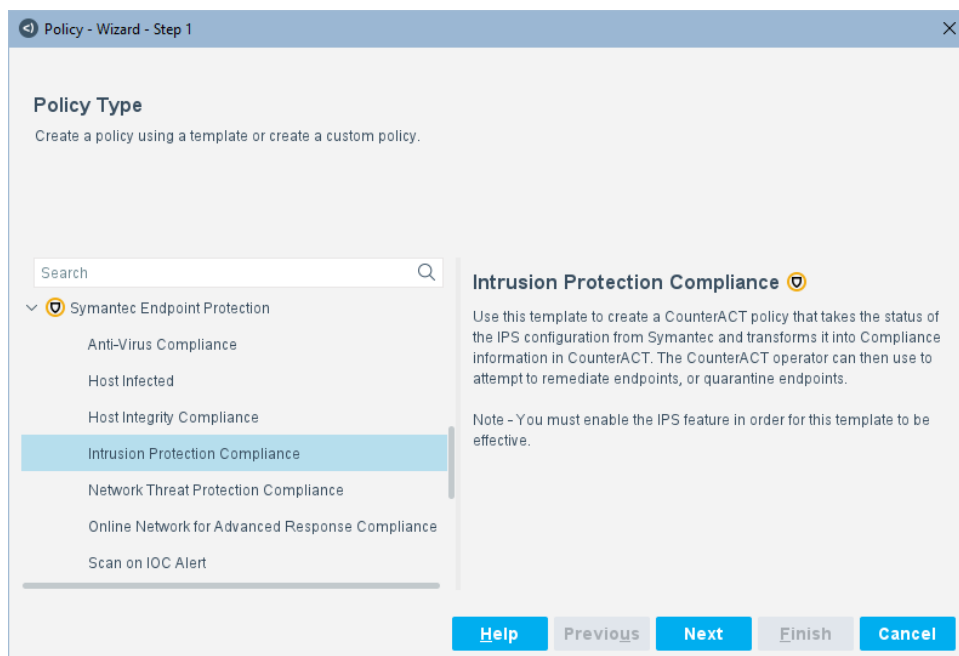
## Create an Intrusion Protection Compliance Policy

Use the Intrusion Protection Compliance policy to take the status of the IPS configuration from Symantec and transforms it into Compliance information in the Forescout platform. The Forescout operator can then use to attempt to remediate endpoints, or quarantine endpoints.

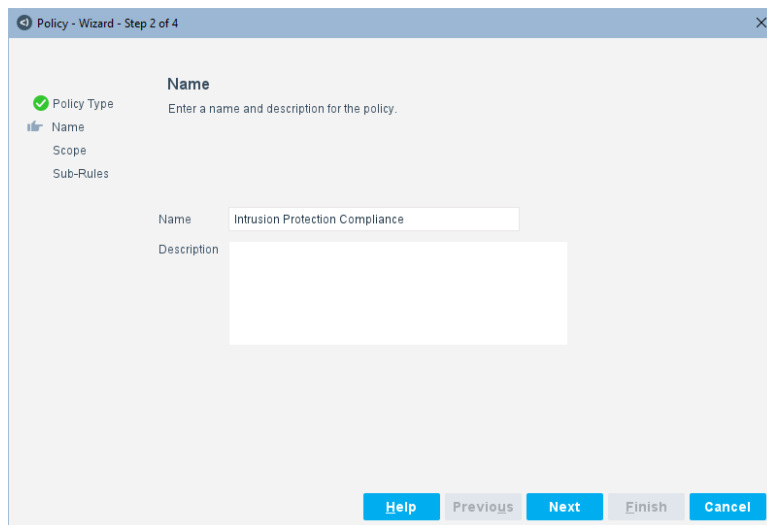
 *You must enable the IPS feature in order for this template to be effective.*

### To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Intrusion Protection Compliance**.

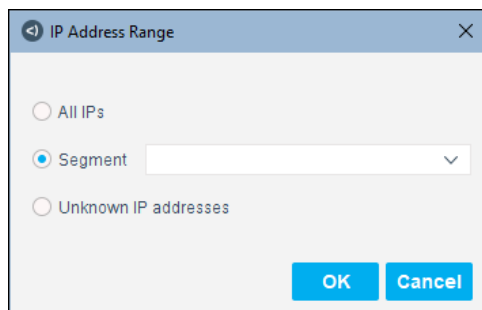


#### 4. Select **Next**.



The screenshot shows a wizard window titled "Policy - Wizard - Step 2 of 4". On the left, a sidebar lists "Policy Type" (checked), "Name", "Scope", and "Sub-Rules". The main area is titled "Name" and contains the instruction "Enter a name and description for the policy.". Below this, there are two input fields: "Name" (containing "Intrusion Protection Compliance") and "Description" (empty). At the bottom, there are five buttons: "Help", "Previous", "Next" (highlighted in blue), "Finish", and "Cancel".

5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The screenshot shows a dialog box titled "IP Address Range". It has three radio buttons: "All IPs", "Segment" (selected), and "Unknown IP addresses". The "Segment" option has a dropdown menu next to it, which is currently open, showing a list of segments. At the bottom, there are two buttons: "OK" (highlighted in blue) and "Cancel".

The following options are available:

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

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

Policy - Wizard - Step 3 of 4

**Scope**  
Define the range of Hosts to be inspected for this policy.

Policy Type  
Name  
Scope  
Sub-Rules

Hosts inspected by the policy

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

Add Remove Segments

Help Previous Next Finish Cancel

9. Select **Next**.

Policy - Wizard - Step 4 of 4

**Sub-Rules**  
Use this screen to review policy sub-rule definitions.  
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Policy Type  
Name  
Scope  
Sub-Rules

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Symantec Intrusion Protection Enabled	Symantec - IPS Status: On		
2	Symantec Intrusion Protection Disabled by Policy	Symantec - IPS Status: Off by admin policy		
3	Symantec Intrusion Protection Disabled	Symantec - IPS Status: Off		
4	Symantec Intrusion Protection Not Installed	Symantec - HostManaged:		
5	NotManaged by Symantec	No Conditions		

Add Edit Remove Duplicate Up Down

Help Previous Next Finish Cancel

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Symantec Intrusion Protection Enabled**) to open a Sub-Rule dialog box.

**Policy: 'Intrusion Protection Compliance'-->Sub-Rule: 'Symantec Intrusion Protection Enabled'**

**Name**  
 Name: Symantec Intrusion Protection Enabled  
 Description: Symantec Intrusion Protection Enabled  
 Edit

**Condition**  
 A host matches this rule if it meets the following condition:  
 All criteria are True  
 Criteria:  
 Symantec - IPS Status - On  
 Add, Edit, Remove

**Actions**  
 Actions are applied to hosts matching the above condition.  
 Enable Action: Details  
 No items to display  
 Add, Edit, Remove

**Advanced**  
 Recheck match: Every 8 hours, All admissions  
 Exceptions: None  
 Edit

Help, OK, Cancel

Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. The sub-rules of this policy check if an endpoint is still in compliance with Intrusion Protection. If a non-compliance is discovered, an alert is sent to the Forescout platform.

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The rules are predefined to detect if the endpoint has non-compliance with Intrusion Protection. Due to the Intrusion Protection Compliance policy scope, action is triggered on any endpoint that meets the default requirements.

- 11.** Review the sub-rule conditions and actions.
- 12.** To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).

13. To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

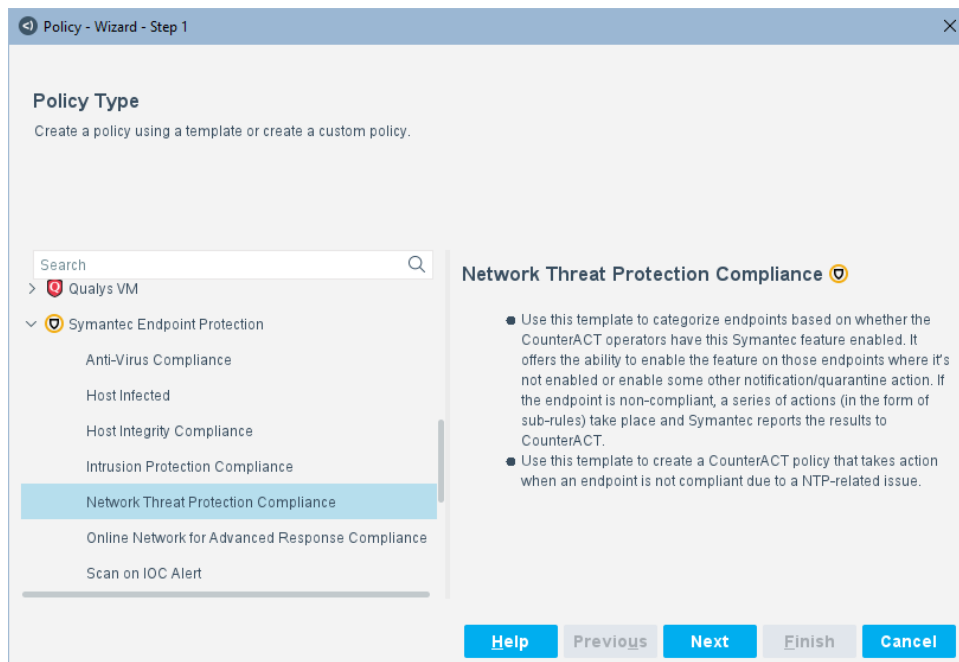
## Create a Network Threat Protection Compliance Policy

Use the Network Threat Protection (NTP) Compliance policy to categorize endpoints based on whether the Forescout operators have this Symantec feature enabled. It offers the ability to enable the feature on those endpoints where it is not enabled or enable some other notification/quarantine action. If the endpoint is non-compliant, a series of actions (in the form of sub-rules) take place and Symantec reports the results to the Forescout platform.

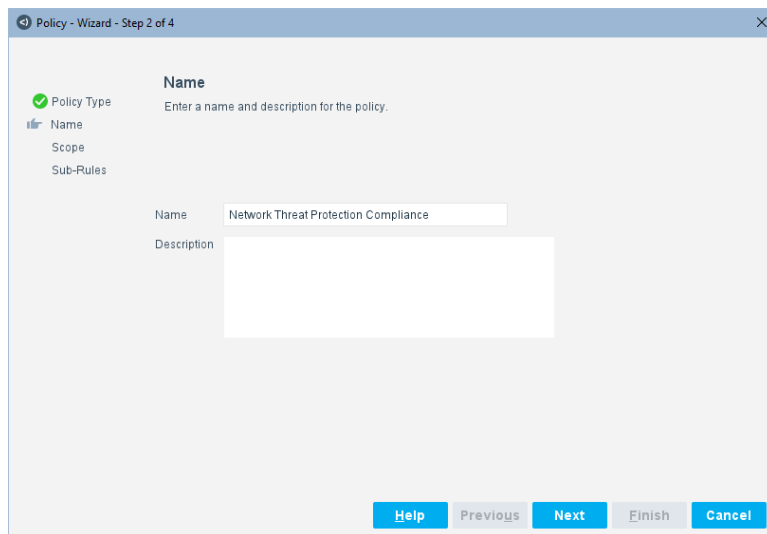
Use this template to create a Forescout platform policy that takes action when an endpoint is not compliant due to a NTP-related issue.

### To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Network Threat Protection Compliance**.



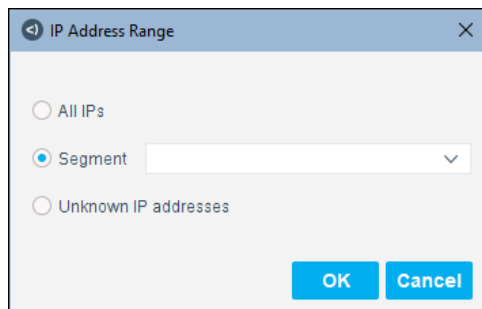
#### 4. Select **Next**.



5. Enter a name for the policy. Optionally, enter a description.

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

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



The following options are available:

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

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

The screenshot shows the 'Policy - Wizard - Step 3 of 4' window with the 'Scope' tab selected. The left sidebar shows 'Policy Type', 'Name', 'Scope', and 'Sub-Rules' with 'Scope' highlighted. The main area is titled 'Scope' and contains the instruction 'Define the range of Hosts to be inspected for this policy.' Below this, a section 'Hosts inspected by the policy' contains a table with two columns: 'Segment' and 'IP Addresses'. The table has one row with 'No Name Assigned' and 'All IPv4, All IPv6'. To the right of the table are buttons 'Add', 'Remove', and 'Segments'. At the bottom are buttons 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

9. Select **Next**.

The screenshot shows the 'Policy - Wizard - Step 4 of 4' window with the 'Sub-Rules' tab selected. The left sidebar shows 'Policy Type', 'Name', 'Scope', and 'Sub-Rules' with 'Sub-Rules' highlighted. The main area is titled 'Sub-Rules' and contains the instruction 'Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.' Below this, a section 'Sub-Rules' contains a table with four columns: 'Name', 'Conditions', 'Actions', and 'Exceptions'. The table has three rows: 1. 'Symantec Network Threat Protection Enabled' with condition 'Symantec - Network Threat Protection Enabled:' and an action icon. 2. 'Symantec Network Threat Protection Disabled' with condition 'Symantec - Host Managed:' and an action icon. 3. 'Not Managed by Symantec' with condition 'No Conditions' and an action icon. To the right of the table are buttons 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', and 'Down'. At the bottom are buttons 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Name	Conditions	Actions	Exceptions
1 Symantec Network Threat Protection Enabled	Symantec - Network Threat Protection Enabled:		
2 Symantec Network Threat Protection Disabled	Symantec - Host Managed:		
3 Not Managed by Symantec	No Conditions		

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Symantec Network Threat Protection Enabled**) to open a Sub-Rule dialog box.

The screenshot shows a dialog box titled "Policy: 'Network Threat Protection Compliance'-->Sub-Rule: 'Symantec Network T...". The dialog is divided into several sections:

- Name:** Displays "Symantec Network Threat Protection Enabled" with an "Edit" button.
- Description:** Displays "Symantec Network Threat Protection Enabled".
- Condition:**
  - Text: "A host matches this rule if it meets the following condition:"
  - Dropdown: "All criteria are True"
  - Criteria list: Contains "Symantec - Network Threat Protection Enabled". To the right of the list are "Add", "Edit", and "Remove" buttons.
- Actions:**
  - Text: "Actions are applied to hosts matching the above condition."
  - Table with columns "Enable", "Action", and "Details". The table is currently empty, showing "No items to display". To the right of the table are "Add", "Edit", and "Remove" buttons.
- Advanced:**
  - Recheck match: "Every 8 hours, All admissions" with an "Edit" button.
  - Exceptions: "None."

At the bottom of the dialog are "Help", "OK", and "Cancel" buttons.

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The rules are predefined to detect if the endpoint has non-compliance with Network Threat Protection. Due to the Network Threat Protection Compliance policy scope, action is triggered on any endpoint that meets the default requirements.


The sub-rules of this policy check if an endpoint is still in compliance with Network Threat Protection; if a non-compliance is discovered, an alert is sent to the Forescout platform.

- 11.** Review the sub-rule conditions and actions.
- 12.** To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).

13. To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

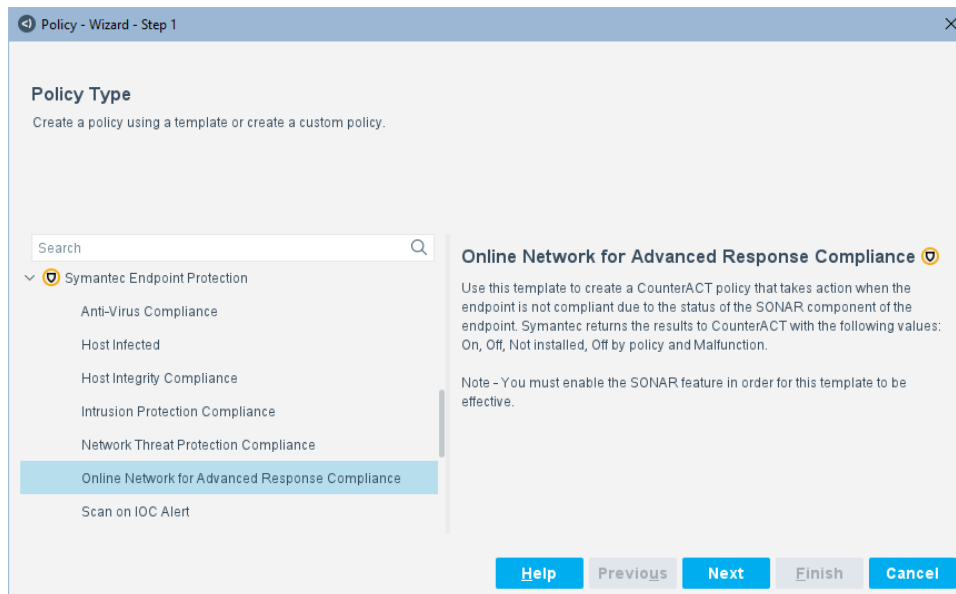
## Create an Online Network for Advanced Response Compliance Policy

Use this template to create a Forescout platform policy that takes action when the endpoint is not compliant due to the status of the Symantec Online Network for Advanced Response (SONAR) component of the endpoint. Symantec returns the results to the Forescout platform with the following values: On, Off, Not installed, Off by policy, and Malfunction.

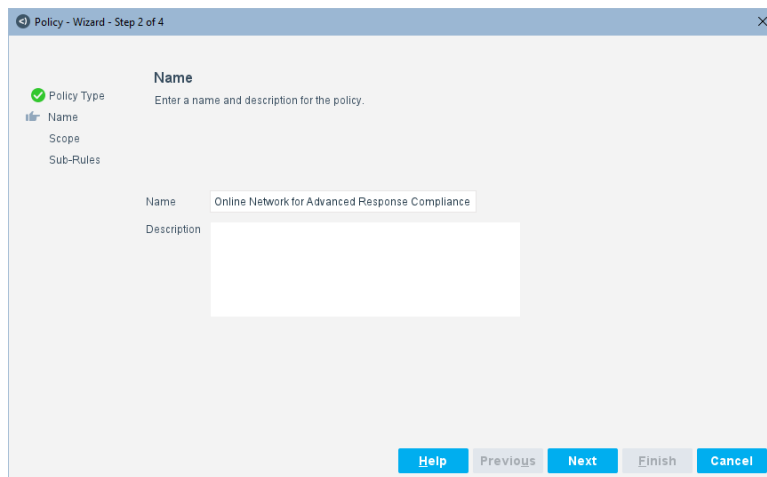
 *You must enable the SONAR feature in order for this template to be effective.*

### To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Online Network for Advanced Response Compliance**.



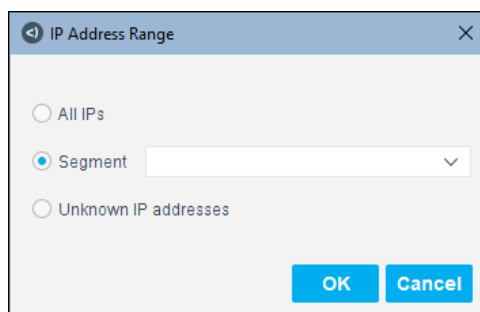
#### 4. Select **Next**.



5. Enter a name for the policy. Optionally, enter a description.

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

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



The following options are available:

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

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

The screenshot shows the 'Policy - Wizard - Step 3 of 4' dialog box with the 'Scope' tab selected. The left sidebar shows 'Policy Type', 'Name', 'Scope', and 'Sub-Rules' with 'Scope' being the active tab. The main area is titled 'Scope' and contains the instruction 'Define the range of Hosts to be inspected for this policy.' Below this, there is a section 'Hosts inspected by the policy' with a table. The table has two columns: 'Segment' and 'IP Addresses'. The first row shows 'No Name Assigned' and 'All IPv4, All IPv6'. To the right of the table are buttons for 'Add', 'Remove', and 'Segments'. At the bottom of the dialog are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

9. Select **Next**.

The screenshot shows the 'Policy - Wizard - Step 4 of 4' dialog box with the 'Sub-Rules' tab selected. The left sidebar shows 'Policy Type', 'Name', 'Scope', and 'Sub-Rules' with 'Sub-Rules' being the active tab. The main area is titled 'Sub-Rules' and contains the instruction 'Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.' Below this, there is a table with columns 'Name', 'Conditions', 'Actions', and 'Exceptions'. The table lists five sub-rules. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', and 'Down'. At the bottom of the dialog are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

	Name	Conditions	Actions	Exceptions
1	Symantec SONAR Enabled	Symantec - SONAR Status: On		
2	Symantec SONAR Disabled by Policy	Symantec - SONAR Status: Off by policy		
3	Symantec SONAR Not Running	Symantec - SONAR Status: Off, Malfunction		
4	Symantec SONAR Not Installed	Symantec - HostManaged:		
5	NotManaged by Symantec	No Conditions		

- 10.**Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Symantec SONAR Enabled**) to open a Sub-Rule dialog box.

The screenshot shows a dialog box titled "Policy: 'Online Network for Advanced Response Compliance'--> Sub-Rule: 'Symantec SONAR Enabled'". The dialog is divided into several sections:

- Name:** Displays "Name: Symantec SONAR Enabled" and "Description: Symantec SONAR Enabled". An "Edit" button is to the right.
- Condition:** States "A host matches this rule if it meets the following condition:". Below this is a dropdown menu set to "All criteria are True". A list of criteria contains one item: "Symantec - SONAR Status - On". To the right of the list are "Add", "Edit", and "Remove" buttons.
- Actions:** States "Actions are applied to hosts matching the above condition.". Below this is a table with columns "Enable Action" and "Details". The table is currently empty, showing "No items to display". To the right of the table are "Add", "Edit", and "Remove" buttons.
- Advanced:** Contains "Recheck match: Every 8 hours, All admissions" and "Exceptions: None.". An "Edit" button is to the right.

At the bottom of the dialog are "Help", "OK", and "Cancel" buttons.

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The rules are predefined to detect if the endpoint has non-compliance issues with Symantec Online Network for Advanced Response. Due to the SONAR Compliance policy scope, action is triggered on any endpoint that meets the default requirements.

The sub-rules of this policy check if an endpoint is still in compliance with SONAR; if a non-compliance is discovered, an alert is sent to the Forescout platform.

- 11.**Review the sub-rule conditions and actions.
- 12.**To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).

13. To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).
14. In the Sub-Rule dialog box, select **OK**.
15. In the Sub-Rules pane, select **Finish**.
16. In the Policy Manager, select **Apply**.

## Create a Scan on IOC Alert Policy

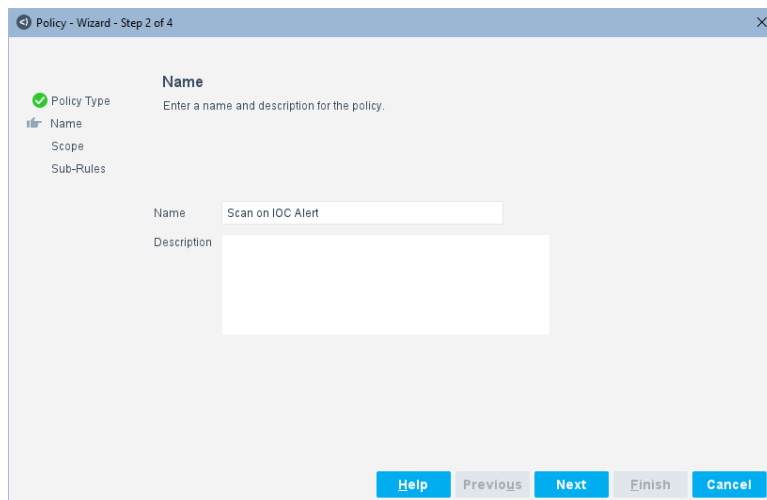
This policy waits for reports of IOCs/malware from other integrated engines via the Advanced Threat Detection integrations of the Forescout platform. That threat report is ingested and triggers a scan on Symantec-managed endpoints based on the severity of the recently-received IOC report. Depending upon the settings in the Scan on IOC Alert policy, a quick or full scan on the endpoint occurs.

### To create a policy:

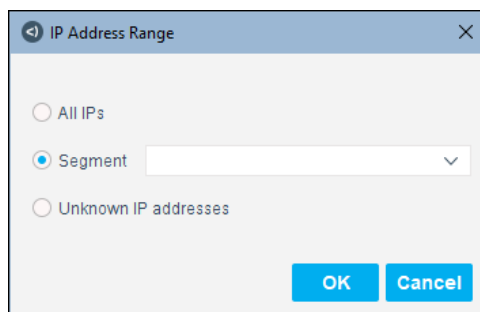
1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager and search for Symantec.
3. Expand the **Symantec Endpoint Protection** folder and select **Scan on IOC Alert**.



#### 4. Select **Next**.



5. Enter a name for the policy. Optionally, enter a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

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

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

Policy - Wizard - Step 3 of 4

**Scope**  
Define the range of Hosts to be inspected for this policy.

Policy Type  
Name  
Scope  
Sub-Rules

Hosts inspected by the policy

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

Add  
Remove  
Segments

Help Previous Next Finish Cancel

9. Select **Next**.

Policy - Wizard - Step 4 of 4

**Sub-Rules**  
Use this screen to review policy sub-rule definitions.  
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Policy Type  
Name  
Scope  
Sub-Rules

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Recent IOC Alert - High Severity	Last Reported IOC: High Severity NOT: Older than 1 hour ...		
2	Recent IOC Alert - Low Severity	Last Reported IOC: Medium Severity NOT: Older than 1 ho...		
3	No Recent IOC Alerts	No Conditions		

Add  
Edit  
Remove  
Duplicate  
Up  
Down

Help Previous Next Finish Cancel

- 10.** Predefined sub-rules for the policy are displayed in the Sub-Rules pane. Each sub-rule defines a level of non-compliance and may have one or more actions associated with it. Edit the sub-rule conditions and actions by double-clicking the sub-rule in the Sub-Rules pane (for example, **Recent IOC Alert – High Severity**) to open a Sub-Rule dialog box.

The screenshot shows a dialog box titled "Policy: 'Scan on IOC Alert'-->Sub-Rule: 'Recent IOC Alert - High Severity'". The dialog is divided into several sections:

- Name:** Displays "Recent IOC Alert - High Severity" with an "Edit" button. Below it, the description reads: "Initiate a pro-active full scan on Symantec Managed end...".
- Condition:** States "A host matches this rule if it meets the following condition:". It shows a dropdown menu set to "One criterion is True". Below this is a list of criteria:
 

Criteria	Buttons
Last Reported IOC - High Severity NOT: Older than 1 hour	Add, Edit, Remove
Last Reported IOC - Critical Severity NOT: Older than 1 hour	
- Actions:** States "Actions are applied to hosts matching the above condition.". It contains a table:
 

Enable	Action	Details	Buttons
<input type="checkbox"/>	Error	Error	Add, Edit, Remove
- Advanced:** Includes "Recheck match" set to "Every 1 hour, All admissions" and "Exceptions" set to "None". An "Edit" button is present.

At the bottom are "Help", "OK", and "Cancel" buttons.

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the integrity of the endpoint is checked. The Scan on IOC Alert sub-rules are predefined to send an alert if an Incident of Compromise is detected. Once detected, action is triggered on any endpoint that meets the default requirements.

The sub-rules of this policy scans and detects an Incident of Compromise on an endpoint and then sends an alert to the Forescout platform.

- 11.** Review the sub-rule conditions and actions.
- 12.** To add another condition, select **Add** in the Condition section. See [Symantec Endpoint Protection Policy Properties](#).
- 13.** To add another action, select **Add** in the Actions section. See [Symantec Endpoint Protection Policy Actions](#).

**14.**In the Sub-Rule dialog box, select **OK**.

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

**16.**In the Policy Manager, select **Apply**.

## Create Custom Symantec Policies

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

### Policies and Rules, Conditions and Actions

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

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

In addition to the bundled Forescout platform properties and actions available for detecting and handling endpoints, you can use properties to create custom policies that:

- Enable security components of the Symantec Agent on endpoints where they are not running.
- Trigger an update and synchronization of the Symantec Agent with the Symantec Endpoint Protection Manager.
- 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.

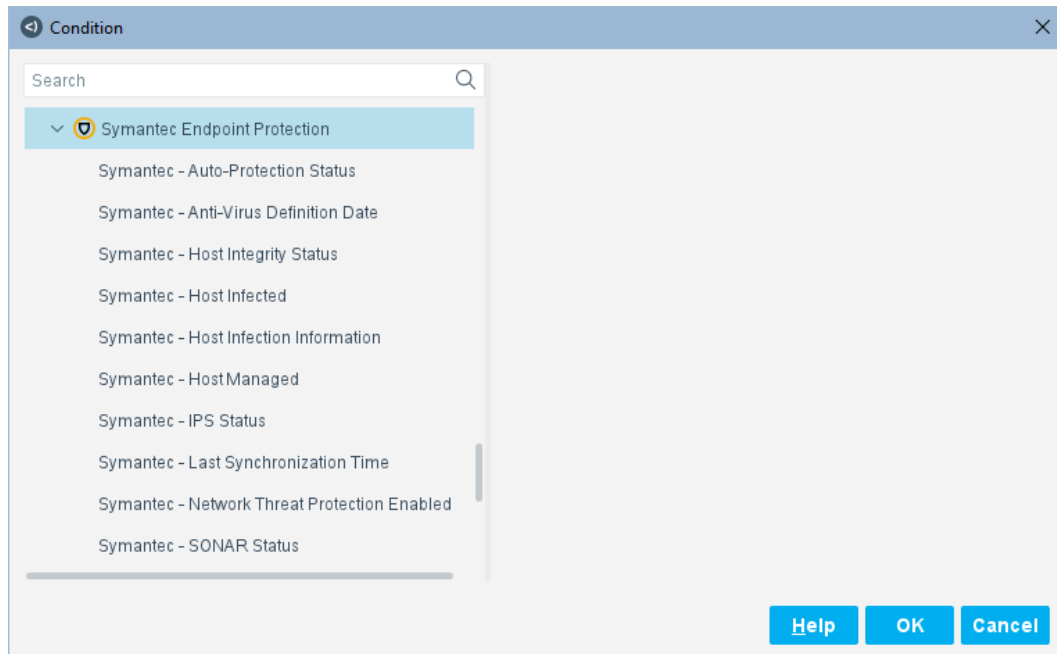
## Symantec Endpoint Protection Policy Properties

This topic describes the Symantec Endpoint Protection properties that are available when you install Forescout eyeExtend for Symantec Endpoint Protection.

#### To access Symantec Endpoint Protection properties:

- 1.** Go to the Properties tree from the Policy Conditions dialog box.

2. Expand the **Symantec Endpoint Protection** folder in the Properties tree.



The following properties are available.

<b>Symantec - Auto-Protection Status</b>	Indicates a change to the Auto-Protection status.
<b>Symantec - Anti-Virus Definition Date</b>	Indicates the date the Anti-Virus was last updated on the endpoint.
<b>Symantec - Host Integrity Status</b>	Indicates the Symantec integrity status detected on the endpoint.
<b>Symantec - Host Infected</b>	Indicates whether an endpoint is infected.
<b>Symantec - Host Infection Information</b>	Indicates information about the infection(s) detected on the endpoint by Symantec.
<b>Symantec - Host Managed</b>	Indicates whether the endpoint is managed by a Symantec Endpoint Protection Manager.
<b>Symantec - IPS Status</b>	Indicates the status of the Intrusion Prevention System (IPS) on the endpoint.
<b>Symantec - Last Synchronization Time</b>	Indicates the last time the Symantec Agent communicated with the Symantec Endpoint Protection Manager.
<b>Symantec - Network Threat Protection Enabled</b>	Indicates whether the Symantec Network Threat Protection is enabled.
<b>Symantec - SONAR Status</b>	Indicates the status of the Symantec Online Network for Advanced Response (SONAR).

## Track Changes

This section describes how to track changes on the Symantec Endpoint Protection properties.

Tracking any changes to any properties associated to an endpoint is a vital step to detection and quick action. There are default settings for each of the properties. You can also customize the Track Changes settings.

### To access Symantec Endpoint Protection Track Changes:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the **Track Changes** folder in the Properties tree.

The following Track Changes properties are available.

<b>Symantec Auto-Protection Status Change</b>	Indicates a change to the Auto-Protection status.
<b>Symantec Host Integrity Status Change</b>	Indicates a change to the host integrity status on the endpoint.
<b>Symantec Host Infected Status Change</b>	Indicates a change to the infection state of an endpoint.
<b>Symantec Intrusion Prevention System Status Change</b>	Indicates a change to the status of the Symantec IPS on the endpoint.
<b>Symantec Network Threat Protection Status Change</b>	Indicates a change to the endpoint's Symantec Threat Protection status.
<b>Symantec SONAR Status Change</b>	Indicates a change to the Symantec Online Network for Advanced Response's (SONAR) status on the endpoint.

## Symantec Endpoint Protection Policy Actions

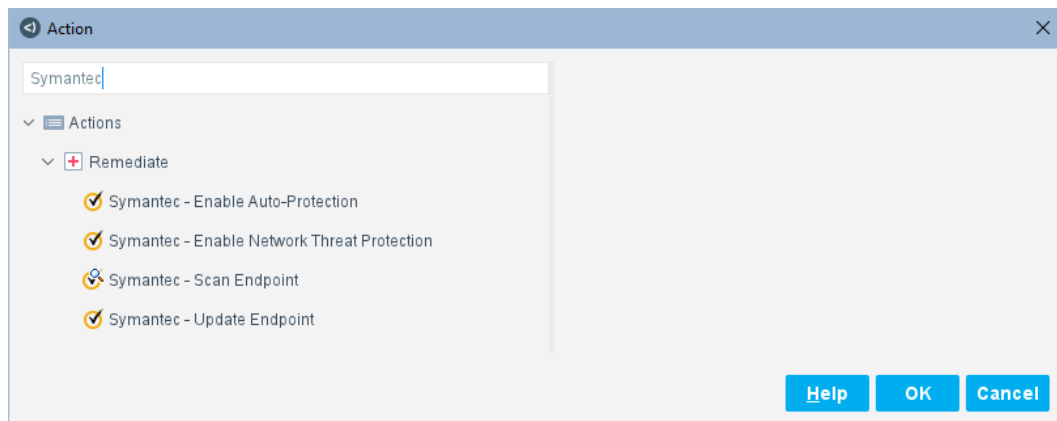
Forescout platform policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a device infected with a virus to an isolated VLAN or send the device user or IT team an email.

In addition to the bundled Forescout properties and actions available for detecting and handling endpoints, you can work with Symantec-related properties and actions to create the custom policies. These items are available when you install the module.

### To access Symantec Endpoint Protection actions:

1. Go to the Action tree from the Policy Conditions dialog box.

## 2. Expand the Remediate folder in the Actions tree.



The following actions are available.

<b>Symantec - Enable Auto-Protection</b>	Enables Symantec Auto-Protection on the endpoint.
<b>Symantec - Enable Network Threat Protection</b>	Enables Symantec Network Threat Protection on the endpoint.
<b>Symantec - Scan Endpoint</b>	Triggers an anti-virus scan on the endpoint. You can configure the scan to be a full hard disk scan or a quick scan.
<b>Symantec - Update Endpoint</b>	Triggers a synchronization of Symantec policies and definition files from Symantec Endpoint Protection Manager to the endpoint.

### Related IOC Scanner Plugin Properties

In addition to the properties provided by Forescout eyeExtend for Symantec Endpoint Protection, the IOC Scanner Plugin provides the **IOCs Detected by CounterACT** property, which contains data from threats detected by this module. Refer to the [IOC Scanner Plugin Configuration Guide](#) for details.

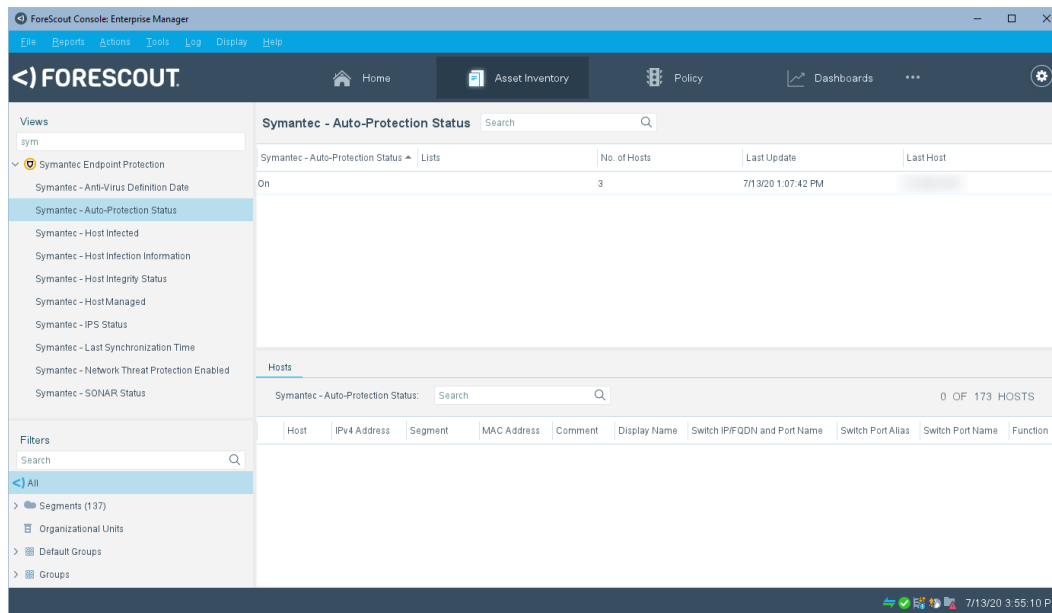
## Display Symantec Endpoint-Related Data

Use the Asset Inventory to view the real-time configuration status of the various security components of Symantec on your endpoints. The inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoint information reported by the Symantec Agent.
- View endpoints that have been detected with specific threats.
- Easily track which endpoints of each of the different Symantec Agent security components running.
- Incorporate inventory detections into policies.

**To access the inventory:**

1. In the Console, select **Asset Inventory**.
2. In the Views pane, expand the **Symantec Endpoint Protection** folder.



Based on the Symantec Endpoint Protection properties, the following information is available:

- Symantec - Anti-Virus Definition Date
- Symantec - Auto-Protection Status
- Symantec - Host Infected
- Symantec - Host Infection Information
- Symantec - Host Integrity Status
- Symantec - Host Managed
- Symantec - IPS Status
- Symantec - Last Synchronization Time
- Symantec - Network Threat Protection Enabled
- Symantec - SONAR Status

Refer to [Working with Asset Inventory Detections](#) in the *ForeScout Administration Guide* or the Console Online Help for information about working with the Asset Inventory.