ForeScout® Extended Module for Symantec™
Endpoint Protection
Configuration Guide

Version 1.1
# Table of Contents

**About the Symantec Endpoint Protection Integration** ................................................. 4
Use Cases .................................................................................................................. 4
Additional Symantec Endpoint Protection Documentation ........................................ 5

**About This Module** .......................................................................................... 6

**Concepts, Components, Considerations** ............................................................. 7
Concepts ................................................................................................................... 7
Components ............................................................................................................. 8
Considerations ......................................................................................................... 9
What to Do .............................................................................................................. 9

**Requirements** .................................................................................................... 10
CounterACT Software Requirements ........................................................................ 10
ForeScout Extended Module License Requirements ............................................. 10
  Per-Appliance Licensing Mode ............................................................................. 11
  Centralized Licensing Mode ............................................................................... 12
  More License Information .................................................................................. 13
Symantec Endpoint Protection Requirements ........................................................ 13
About Support for Dual Stack Environments .......................................................... 13

**Install the Module** ............................................................................................. 13

**Set Up Web Services Client Application** ............................................................. 14
 Register an Application with Symantec Endpoint Protection Manager Web Services ........................................ 15
Authorize CounterACT to call Endpoint Protection Web Services .......................... 16
Get an OAuth Access Token from the Authorization Code ..................................... 17

**Configure the Module** ....................................................................................... 18
Test the Module ....................................................................................................... 21

**Run Symantec Endpoint Protection Policy Templates** ....................................... 21
Anti-Virus Compliance Policy Template .................................................................... 22
Host Infected Policy Template .................................................................................. 26
Host Integrity Compliance Policy Template ............................................................ 31
Intrusion Protection Compliance Template ............................................................ 35
Network Threat Protection Compliance Template .................................................. 38
Online Network for Advanced Response Compliance Template ......................... 43
Scan on IOC Alert Template .................................................................................... 47

**Create Custom Symantec Policies** ................................................................. 51
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
- Anti-spyware
- Intrusion Prevention
- Firewall
- Application white/black-listing
- Malware Behavioral Analysis

This ForeScout CounterACT® Extended Module integrates with 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 CounterACT administrator. Examples include information about operating system, logged on user, whether the endpoint has anti-virus installed, etc.

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 as 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.

Use Cases

This section describes use cases supported by this module. To understand how this module helps you achieve these goals, see About This Module.

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, any network-based remediation or quarantining is lacking from this arsenal. By integrating with CounterACT, the remediation actions available upon discovery of malware on an
Agent Presence Detection & Enrollment with Symantec Endpoint Protection

All endpoints in a Symantec Endpoint Protection environment should be running a valid Symantec Agent. CounterACT will be able to determine whether endpoints have the correct agent installed and running. An endpoint without the agent installed and running can be remediated by CounterACT either by automatically enrolling with Symantec Endpoint Protection Manager, or the user gets redirected to a portal which prompts to download and install the Agent before continuing. Refer to 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, but be configured with the desired features, such as anti-virus definitions up to date and network threat detection activated. CounterACT will be able to 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. Refer to Run Symantec Endpoint Protection Policy Templates.

Scan on Third Party Malware Detection

When there is suspicion of a virus or malware in the corporate network, it may be desirable to enact all available defenses on the corporate endpoints. Although the Symantec Endpoint Protection anti-virus 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 CounterACT is made 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. Refer to Scan on IOC Alert.

Scan non-Symantec Managed Endpoints upon Malware Discovery

CounterACT can be used to react to a problem that Symantec Endpoint Protection discovers on an endpoint. Symantec communicates with CounterACT about the threat, and via integration with the IOC Scanner, CounterACT 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. Refer to 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://www.symantec.com/content/elibrary/selibrary
About This Module

This module lets you integrate CounterACT 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 CounterACT.
  - **Anti-Virus Compliance** template - Detects which endpoints have the Symantec Agent installed and running with Auto-Protect enabled.
  - **Host Integrity Compliance** template - Based on compliance information, the CounterACT operator can attempt to remediate or quarantine non-compliant endpoints.
  - **Host Infected** template - Detects whether an endpoint is infected or not. If infected, the Host Infected policy instructs what actions to take.
  - **Intrusion Protection Compliance** template - Converts the Intrusion Prevention System configurations from Symantec into compliance information in CounterACT.
  - **Network Threat Protection Compliance** template - Offers the ability to enable Network Threat Protection on endpoints where it’s not enabled.
  - **Symantec Online Network for Advanced Response (SONAR) Compliance** template - When an endpoint is not compliant due to the status of the SONAR component, Symantec reports it to CounterACT.

- Create policies using other Symantec-related templates:
  - **Scan on Indication of Compromise (IOC) Alert** template - When other Advanced Threat Detection integrations within CounterACT 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 CounterACT properties and actions, to deal with issues not covered in other policy templates.

- View threats reported by Symantec and automatically add to the IOC repository. These IOCs are used by the IOC Scanner Plugin for Advanced Threat Detection (ATD) and recovery. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.

- Use CounterACT 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 CounterACT policies and other basic features work. Additionally, you should have a solid understanding of how to leverage threat intelligence distributed by IOCs.
Concepts, Components, Considerations

This section provides a basic overview of 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 about Symantec Endpoint Protection.

Logical Representation of Symantec Endpoint Protection Module

![Diagram of Symantec Endpoint Protection Module](image)

Base Integration and Extended Module Integration

There is a base integration of Symantec with CounterACT® 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 new Extended Module integrates with Symantec Endpoint Protection Manager. It provides a much tighter and more comprehensive integration covering more use cases and additional features of the Symantec Endpoint Protection Suite.
CounterACT 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 the 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 CounterACT as host properties, which can be included in CounterACT policy conditions. To evaluate these properties, CounterACT queries the Symantec server via database queries and their web service.

Regular Polling Intervals

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

Actions on Endpoints are performed 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 CounterACT by that CounterACT Appliance. In deploying, you should balance the following:

- Minimise bandwidth between CounterACT and Symantec by using a connecting CounterACT Appliance which is logically close to the Symantec Endpoint Protection Manager.
- Minimise CounterACT 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 additional components that help provide optimal integration of the Symantec Endpoint Protection Extended Module.

HPS Applications

HPS Applications is a valuable addition to the Symantec Endpoint Protection Module. It allows CounterACT to 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, CounterACT can detect the following:

- Whether the Symantec Agent is installed or not
- Whether the real-time detection component of the agent is running or not
- 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 achieves this by interacting directly with managed endpoints.

**Indications of Compromise (IOC) Scanner**

This module works with the Indications of Compromise (IOC) Scanner Module – CounterACT's action center for Advanced Threat Detection (ATD) and response. The IOC Scanner plugin provides:

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

**Considerations**

This section addresses additional considerations.

**Severity Levels**

The mapping of Symantec severity to CounterACT severity is listed here.

<table>
<thead>
<tr>
<th>Symantec Severity Category</th>
<th>CounterACT Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Critical</td>
</tr>
<tr>
<td>5</td>
<td>Critical</td>
</tr>
</tbody>
</table>

**What to Do**

You must perform the following to work with this module:

1. Verify that you have met system requirements. See Requirements.
2. Install the Module.
4. Configure the Module.
5. Run Symantec Policy Templates.
Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- Symantec Endpoint Protection Requirements

CounterACT Software Requirements

The module requires the following CounterACT releases and other CounterACT hard requirements:

- CounterACT version 8.0.
- Core Extensions Module version 1.0 or above with the IOC Scanner Plugin running.
- 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.

CounterACT continuously supports newly released Symantec Endpoint Protection Extended Modules versions. Refer to the Release Notes for the most updated list of requirements.

ForeScout Extended Module License Requirements

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

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

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

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

**Per-Appliance Licensing Mode**

When installing the module you are provided with a 90-day demo module license. If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

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

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

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

**Requesting a License**

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

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

1. Select the Home tab.

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

Centralized Licensing Mode

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

- No demo license is automatically installed during system installation.

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

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

More License Information

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

Symantec Endpoint Protection Requirements

- Symantec Endpoint Protection Manager version 12.1.6 installed
- Configured to use a SQL Server Database (the embedded database option is not supported)
- CounterACT needs to be registered as a Symantec Endpoint Protection Web Services Client Application.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, IPv6 addresses are not yet supported by this component. The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

Install the Module

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

To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - Per-Appliance Licensing Mode
   - Customer Portal, Downloads Page - Centralized Licensing Mode
   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module .fpi file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select Options from the Tools menu.
5. Select **Modules**. The Modules pane opens.

6. Select **Install**. The Open dialog box opens.

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

8. Select **Install**. The Installation screen opens.

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

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

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

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

   - *Some components are not automatically started following installation.*

**Identifying Your Licensing Mode in the Console**

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

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

![License Table](image)

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

**Set Up Web Services Client Application**

This section addresses setting the Symantec Endpoint Protection Manager Web Services.
Register an Application with Symantec Endpoint Protection Manager Web Services

In order to work with Symantec Endpoint Protection Manager Web Services, a web services client application must first 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 a Symantec Endpoint Protection Manager Administrator account is required. Registration is performed only once for each instance of Symantec Endpoint Protection Manager.

To register an application with Symantec Endpoint Protection Manager:

1. The administrator needs to log in 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.

<table>
<thead>
<tr>
<th>Code</th>
<th>What To Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;hostname&gt;</td>
<td>Enter the IP address or hostname of the installed instance of Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>&lt;port_number&gt;</td>
<td>Enter the web services port of the installed instance of Symantec Endpoint Protection Manager. The default port number is 8446.</td>
</tr>
</tbody>
</table>

2. Press <Enter>. The Symantec Endpoint Protection Manager Web Service Application Registration page displays.

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

4. Provide a name for the application that will connect to Symantec Endpoint Protection – in the example below, the name CounterACT was used.
5. When the Web Service is registered, the Client ID and the Client Secret displays.

6. In the Web Service Application page, select **Enable access**.
7. Copy the Client ID and the Client Secret to a safe place for future reference.
8. Continue to the next section.

**Authorize CounterACT to call Endpoint Protection Web Services**

This section addresses authorizing the application just created to call the Symantec Web Services.

- The application must first be registered with Symantec Endpoint Protection Manager.

To authorize an application to call Symantec Endpoint Protection Web Services:

1. A browser window opens containing the following URL.

Using the same browser window as the one the Symantec web service application returned authorization, construct the URL by populating specific items with your information.

<table>
<thead>
<tr>
<th>Code</th>
<th>What To Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;hostname&gt;</td>
<td>Enter the IP address or hostname of the installed instance of Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>&lt;port_number&gt;</td>
<td>Enter the web services port of the installed instance of Symantec Endpoint Protection Manager. The default port number is 8446.</td>
</tr>
<tr>
<td>&lt;client_id&gt;</td>
<td>Enter the Client ID that was provided when the application was registered.</td>
</tr>
</tbody>
</table>

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


4. Select **Authorize**.

5. Continue to the next section.

**Get an OAuth Access Token from the Authorization Code**

You will need to get an 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.

1. The return page may display as an empty (blank) page. However, the code number can be seen in the page’s URL. In the example below, the URL contains a code number: RTa98F. **Take note of the code number.**

![Code Number](image1)

2. Using the same browser window you used for authorizing the Symantec Web Service access (step 9), open a new browser page and enter the below URL replacing the `<hostname>`, `<port>`, `<clientid>`, `<clientsecret>` and `<code>` with those that you have collected.

   ```
   ```

3. The return page is in JSON format. The access token is in the value field. The refresh token is in the `refreshToken` value field. See below for example:

   ![JSON Output](image2)

4. **Take note of these values** and enter them into the CounterACT device configuration. See [Configure the Module](#).

   - **The hostname, port number, client ID, client secret, and code needs to be stored securely.**

**Configure the Module**

Configure the module to ensure that CounterACT can communicate with the Symantec Endpoint Protection suite.

**To configure the module:**

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.

2. Navigate to and select the **Modules** folder.

3. In the **Modules** pane, select **Symantec Endpoint Protection**, and select **Configure**. The Symantec Endpoint Protection pane opens.
4. Select **Add** to define a Symantec Endpoint Protection server to communicate with CounterACT. The Add Symantec Endpoint Protection Add Server Definition dialog box opens.

<table>
<thead>
<tr>
<th><strong>Server Address</strong></th>
<th>Enter the IP address of the Symantec server that sends notifications to CounterACT.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Port</strong></td>
<td>Enter the Symantec server port.</td>
</tr>
<tr>
<td><strong>Client ID</strong></td>
<td>Symantec web services port. Default value is 8446.</td>
</tr>
<tr>
<td><strong>Client Secret</strong></td>
<td>Enter the OAUTH client credentials.</td>
</tr>
<tr>
<td><strong>Access Token</strong></td>
<td>Enter the OAUTH access token to make web service API calls. You can generate the access key manually. See <a href="#">Get Access Token</a>.</td>
</tr>
<tr>
<td><strong>Refresh Token</strong></td>
<td>Enter the OAUTH refresh token that refreshes the access token when it gets expired. See <a href="#">Get Access Token</a>.</td>
</tr>
<tr>
<td><strong>Maximum Web Service Requests per Second (1-10000)</strong></td>
<td>Enter the number of web service requests per second (rate limiting). It is recommended to leave this as default and only adjust later if troubleshooting the integration is required.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Connecting CounterACT Device</strong></td>
<td>Select a CounterACT device to apply the server configurations to.</td>
</tr>
</tbody>
</table>

5. Select **Next**. The Database Server Definition pane opens.

**Database Server**

Enter the SQL server database (required) the Symantec Endpoint Protection module uses.

- **Server Instance** -- Enter a customized name of the SQL Instance. For example: ForeScout_SQL_Instance

**OR**

- **Port** - Select the SQL server database port number. The default is 1433.

**Database Name**

Enter the name of the SQL server database.

**Database Administrator username**

Enter the administrator username used to access the SQL server database. Windows authentication and SQL authentication are both supported.

- For Windows authentication, the database administrator username is user domain name followed by backslash and then username. For example, forescout\john.smith.
- For SQL authentication, the username is the SQL username, for example, sa.

**Database Administrator password**

Enter the administrator password used to access the SQL server database. When the administrator password is changed, the Refresh Token will expire. You will need to regenerate a new Access Token and Refresh Token.
Verify Database Administrator password

Re-enter the administrator password.

Polling Interval Minutes (0-60)

Database polling can be disabled by setting the number to 0. Disabling polling will stop the Symantec Endpoint Protection module 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.

6. Select Finish. An entry for the Symantec server is added to the list in the Symantec Endpoint Protection pane.

7. (Optional) Repeat these steps to define additional Symantec Endpoint Protection Managers.

Test the Module

1. To test communication with Symantec servers, select a server, and select Test. After viewing the test results, select Close.

2. In the Symantec Endpoint Protection pane, select Apply. A CounterACT Enterprise Manager Console dialog box opens.

3. Select Yes to save the module configuration, and then select Close.

Run Symantec Endpoint Protection Policy Templates

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

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

The following templates are available for detecting and managing endpoints:

- Anti-Virus Compliance
- Host Infected
- Host Integrity Compliance
- Intrusion Prevention Compliance
- Network Threat Protection Compliance
- Online Network for Advanced Response Feature Compliance
- Scan on IOC Alert
Anti-Virus Compliance Policy Template

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 CounterACT 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 CounterACT.
To use the Anti-Virus Compliance policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Anti-Virus Compliance. The Anti-Virus Compliance pane opens.
4. Select Next. The Name pane opens.

**Name the Policy**

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

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


**Define Which Endpoints Will Be Inspected - Policy Scope**

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

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

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

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

**How Endpoints Are Detected and Handled**

Sub-rules allow you to 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 CounterACT 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.

**Sub-Rules**

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.
10. Double-click the **Symantec - Auto-Protect running and up-to-date** sub-rule to open it. The Policy: [Name of Anti-Virus Compliance policy] Sub-Rule: Symantec Auto-Protect running and up-to-date dialog box opens.
11.In this page, you can Add conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

12.Select OK. In the Policy: [Name of Anti-Virus Compliance policy] Sub-Rule: Symantec Auto-Protect running and up-to-date dialog box, select OK.

13.Repeat steps 10 - 12 to make changes in other sub-rules.


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

**Host Infected Policy Template**

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. An example action would be to quarantine the infected endpoint from the network.
To use the Host Infected policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Host Infected. The Host Infected pane opens.
4. Select Next. The Name pane opens.

**Name the Policy**

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


**Define Which Endpoints Will Be Inspected - Policy Scope**

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

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

− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

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

### How Endpoints Are Detected and Handled

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

The Sub-Rules instruct CounterACT 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.

### Sub-Rules

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

10. Double-click the **Not Infected, and No Recent Infections** sub-rule to open it. The Policy: [Name of Host Infected policy] Sub-Rule: Not Infected, and No Recent Infections dialog box opens.
11. In this page, you can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** and **Policy Actions** sections.

12. Select **OK**. In the Policy: [Name of Host Infected policy] Sub-Rule: Not Infected, and No Recent Infections dialog box, select **OK**.

13. Repeat steps 10 - 12 to make changes in other sub-rules.

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

15. On the CounterACT Console, select **Apply** to save the policy.
Host Integrity Compliance Policy Template

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

To use the Host Integrity Compliance policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Host Integrity Compliance. The Host Integrity Compliance pane opens.
4. Select Next. The Name pane opens.
Name the Policy

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

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


Define Which Endpoints Will Be Inspected - Policy Scope

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

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

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


**How Endpoints Are Detected and Handled**

Sub-rules allow you to 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 CounterACT 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.

**Sub-Rules**

The sub-rules of this policy detects the non-compliance of an endpoint's integrity.

10. Double-click the **Symantec Host Integrity Status: SUCCESS** sub-rule to open it. The Policy: [Name of Host Integrity Compliance policy] Sub-Rule: Symantec Host Integrity Status: SUCCESS dialog box opens.
11. In this page, you can Add conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

12. Select OK. In the Policy: [Name of Host Integrity Compliance policy] Sub-Rule: Symantec Host Integrity Status: SUCCESS dialog box, select OK.

13. Repeat steps 10 - 12 to make changes in other sub-rules.


15. On the CounterACT Console, select Apply to save the policy.
Intrusion Protection Compliance Template

Use the Intrusion Protection Compliance policy to take the status of the IPS configuration from Symantec and transforms it into Compliance information in CounterACT. The CounterACT 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 use the Intrusion Protection Compliance policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Intrusion Protection Compliance. The Intrusion Protection Compliance pane opens.
4. Select Next. The Name pane opens.
**Name the Policy**

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

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

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

**Define Which Endpoints Will Be Inspected - Policy Scope**

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

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

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

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

### How Endpoints Are Detected and Handled

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

The Sub-Rules instruct CounterACT 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.

### Sub-Rules

The sub-rules of this policy checks if an endpoint is still in compliance with Intrusion Protection; if a non-compliance is discovered, an alert is sent to CounterACT.

10. Double-click the **Symantec Intrusion Protection Enabled** sub-rule to open it. The Policy: [Name of Intrusion Protection Compliance policy] Sub-Rule: Symantec Intrusion Protection Enabled dialog box opens.
In this page, you can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** and **Policy Actions** sections.

12. Select **OK**. In the Policy: [Name of Intrusion Protection Compliance policy] Sub-Rule: Symantec Intrusion Protection Enabled dialog box, select **OK**.

13. Repeat steps 10 - 12 to make changes in other sub-rules.

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

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

---

**Network Threat Protection Compliance Template**

Use the Network Threat Protection (NTP) Compliance policy to categorize endpoints based on whether the CounterACT operators have this Symantec feature enabled. It offers the ability to enable the feature on those endpoints where it's 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 CounterACT.
Use this template to create a CounterACT policy that takes action when an endpoint is not compliant due to a NTP-related issue.

To use the **Network Threat Protection Compliance** policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Symantec Endpoint Protection** folder and select **Network Threat Protection Compliance**. The **Network Threat Protection Compliance** pane opens.
4. Select **Next**. The Name pane opens.

**Name the Policy**

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

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

**Define Which Endpoints Will Be Inspected - Policy Scope**

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

The following options are available:

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

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

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

### How Endpoints Are Detected and Handled

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

The Sub-Rules instruct CounterACT 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.

**Sub-Rules**

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

11. In this page, you can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

12. Select **OK**. In the Policy: [Name of Network Threat Protection Compliance policy] Sub-Rule: Symantec Network Threat Protection Enabled dialog box, select **OK**.

13. Repeat steps 10 - 12 to make changes in other sub-rules.

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

15. On the CounterACT Console, select **Apply** to save the policy.
Online Network for Advanced Response Compliance Template

Use this template to create a CounterACT 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 CounterACT 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 use the SONAR policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Online Network for Advanced Response Compliance. The Online Network for Advanced Response Compliance pane opens.
4. Select Next. The Name pane opens.

Name the Policy

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


**Define Which Endpoints Will Be Inspected - Policy Scope**

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

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

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

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

### How Endpoints Are Detected and Handled

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

The Sub-Rules instruct CounterACT 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.

### Sub-Rules

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

10. Double-click the **Symantec SONAR Enabled** sub-rule to open it. The Policy: [Name of Online Network for Advanced Response Compliance policy] Sub-Rule: Symantec SONAR Enabled dialog box opens.
11. In this page, you can Add conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

12. Select OK. In the Policy: [Name of Online Network for Advanced Response Compliance policy] Sub-Rule: Symantec SONAR Enabled dialog box, select OK.

13. Repeat steps 10 - 12 to make changes in other sub-rules.


15. On the CounterACT Console, select Apply to save the policy.
Scan on IOC Alert Template

This policy waits for reports of IOCs/malware from other integrated engines via the Advanced Threat Detection integrations of CounterACT. 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 use the Scan on IOC Alert policy template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Symantec Endpoint Protection folder and select Scan on IOC Alert. The Scan on IOC Alert pane opens.
4. Select Next. The Name pane opens.
Name the Policy

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

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


Define Which Endpoints Will Be Inspected - Policy Scope

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

The following options are available:

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

− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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


### How Endpoints Are Detected and Handled

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

The Sub-Rules instruct CounterACT 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.

**Sub-Rules**

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

10. Double-click the **Recent IOC Alert – High Severity** sub-rule to open it. The Policy: [Name of Scan on IOC Alert policy] Sub-Rule: Recent IOC Alert – High Severity dialog box opens.
11. In this page, you can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** and **Policy Actions** sections.

12. Select **OK**. In the Policy: [Name of Scan on IOC Alert policy] Sub-Rule: Recent IOC Alert – High Severity dialog box, select **OK**.

13. Repeat steps 10 - 12 to make changes in other sub-rules.

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

15. On the CounterACT Console, select **Apply** to save the policy.
Create Custom Symantec Policies

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

Policies and Rules, Conditions and Actions

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

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

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can use 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 CounterACT Console, select the Policy tab. The Policy Manager opens.
2. Select Add to create a policy, or select Help for more information about working with policies.
Policy Properties

This section describes the Symantec Endpoint Protection properties that are available when you install the Symantec Endpoint Protection Module.

To access Symantec Endpoint Protection properties:

1. Navigate 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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec - Anti-Virus Definition Date</td>
<td>Indicates the date the Anti-Virus was last updated on the endpoint.</td>
</tr>
<tr>
<td>Symantec - Auto-Protection Status Change</td>
<td>Indicates whether there's a change to the Auto-Protection status.</td>
</tr>
<tr>
<td>Symantec - Host Infected</td>
<td>Indicates whether an endpoint is infected.</td>
</tr>
<tr>
<td>Symantec - IPS Status</td>
<td>Indicates the status of the Intrusion Prevention System (IPS) on the endpoint.</td>
</tr>
<tr>
<td>Symantec - Last Synchronization Time</td>
<td>Indicates the last time the Symantec Agent communicated with the Symantec Endpoint Protection Manager.</td>
</tr>
</tbody>
</table>
### Track Changes

This section describes how you can 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 to each of the properties listed below. You can also customize the Track Changes settings.

**To access Symantec Endpoint Protection Track Changes:**

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the Track Changes folder in the Properties tree.
3. The following Track Changes properties are available.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Threat Protection Enabled</td>
<td>Indicates whether the Symantec Network Threat Protection is enabled.</td>
</tr>
<tr>
<td>Symantec - SONAR Status</td>
<td>Indicates the status of the Symantec Online Network for Advanced Response (SONAR).</td>
</tr>
<tr>
<td>Symantec Auto-Protection Status Change</td>
<td>Indicates whether there's been a change to the Auto-Protection status.</td>
</tr>
<tr>
<td>Symantec Host Infected Status Change</td>
<td>Indicates a change to the infection state of an endpoint.</td>
</tr>
<tr>
<td>Symantec Host Integrity Status Change</td>
<td>Indicates a change to the host integrity status on the endpoint.</td>
</tr>
<tr>
<td>Symantec Intrusion Prevention System Status Change</td>
<td>Indicates whether there has been a change to the status of the Symantec IPS on the endpoint.</td>
</tr>
<tr>
<td>Symantec Network Threat Protection Status Change</td>
<td>Indicates whether there has been a change to the endpoint's Symantec Threat Protection status.</td>
</tr>
<tr>
<td>Symantec SONAR Status Change</td>
<td>Indicates whether there has been a change to the Symantec Online Network for Advanced Response's (SONAR) status on the endpoint.</td>
</tr>
</tbody>
</table>

### Policy Actions

CounterACT policy actions let you instruct CounterACT 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 CounterACT 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. Navigate to the Action tree from the Policy Conditions dialog box.
2. Expand the Remediate folder in the Actions tree.
The following actions are available.

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

**Related IOC Scanner Plugin Properties**

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

**Display Symantec Endpoint-Related Data**

Use the CounterACT Inventory to view in real-time the 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. Select the **Inventory** icon from the Console toolbar.
2. Navigate to **Symantec Endpoint Protection** folder.
The following information, based on the Symantec Endpoint Protection properties, is available:

- Symantec - Anti-Virus Definition Date
- Symantec - Auto-Protection Status
- Symantec - Host Infected
- Symantec - Host Infected 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 Inventory Detections* in the *CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT Inventory.

**Additional CounterACT Documentation**

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

- [Documentation Downloads](#)
Documentation Downloads

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

- **Per-Appliance Licensing Mode** - [Product Updates Portal](https://updates.forescout.com/support/index.php?url=counteract)
- **Centralized Licensing Mode** - [Customer Portal](https://forescout.force.com/support/)

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

2. Select the CounterACT version you want to discover.

Customer Portal

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

To access documentation on the ForeScout Customer Portal:

2. Select Downloads or Documentation.

Documentation Portal

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

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

To access the Documentation Portal:

2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

**CounterACT Help Tools**

Access information directly from the CounterACT Console.

**Console Help Buttons**

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

**CounterACT Administration Guide**

Select CounterACT Help from the Help menu.

**Plugin Help Files**

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

2. Select the plugin and then select Help.

**Documentation Portal**

Select Documentation Portal from the Help menu.

**Identifying Your Licensing Mode in the Console**

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

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

![Options and Licenses](image)

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

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

2018-04-10 09:21