Symantec™ Advanced Threat Protection 3.0 Administration Guide
Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

- **Asia-Pacific and Japan**: customercare_apac@symantec.com
- **Europe, Middle-East, and Africa**: semea@symantec.com
- **North America and Latin America**: supportsolutions@symantec.com
Technical Support ........................................................................................................... 4

Chapter 1  About Symantec Advanced Threat Protection Platform ................................................................. 12
  About Symantec Advanced Threat Protection (ATP) .................................................. 12
  ATP features per license entitlement ...................................................................... 14
  About endpoint detection and response (EDR) ....................................................... 15

Chapter 2  Performing initial Symantec Advanced Threat Protection setup configurations ......................... 17
  Accessing ATP Manager ............................................................................................ 17
  Configuring secure access to ATP Manager ............................................................ 18
  Completing setup tasks ............................................................................................. 19

Chapter 3  Configuring global settings .................................................................................. 22
  Changing the geographic location where you submit files for cloud-based sandboxing ........................................ 22
  Enabling data handling options .............................................................................. 23
  About Synapse correlation ......................................................................................... 24
  Enabling Synapse correlation with Email Security.cloud ........................................ 25
  Enabling Synapse correlation with Symantec ATP:Roaming .................................... 26
  About integrating ATP with Symantec Endpoint Protection ...................................... 27
  ATP / Symantec Endpoint Protection integration workflow ...................................... 29
  Symantec Endpoint Protection client versions and supported ATP features ...................... 31
  Creating an ATP read-only account for a Symantec Endpoint Protection Manager SQL database .................................................. 34
  Preparing a Symantec Endpoint Protection Manager embedded database for ATP log collection ...................................................... 36
  Configuring the connection to the Symantec Endpoint Protection Manager database ........................................................................ 38
  About configuring the connection to Symantec Endpoint Protection Manager .................................................. 39
Configuring endpoints in Symantec Endpoint Protection Manager to communicate with ATP .................................................. 42
Configuring EDR 2.0 and the endpoint data recorder .................. 43
Enabling and disabling EDR 2.0 ............................................. 46
Configuring the connection to Symantec Endpoint Protection Manager ................................................................. 47
Configuring communication with your Symantec Endpoint Protection clients ............................................................... 50
Configuring the endpoint data recorder .................................... 52
Configuring Symantec Endpoint Protection endpoint data recorder policy exceptions .................................................... 54
Configuring Symantec Endpoint Protection endpoint data recorder exclusions ............................................................... 56
Securing communication between endpoints and ATP ................. 56
About backing up and restoring ATP data .................................. 57
  Enabling backup for a management platform or all-in-one appliance ............................................................ 58
About licenses ........................................................................ 60
Viewing the license status and updating a license .................... 61
Viewing certificates ................................................................ 62
ATP actions against expiring certificates .................................. 63
Configuring the connection to an SMTP-compatible mail server ............................................................................. 63
Customizing and testing blocking pages .................................. 64
How ATP purges data from the ATP database ......................... 66

Chapter 4 Configuring default and appliance settings .................. 67
  About default and appliance settings ...................................... 68
  Appliances ........................................................................... 69
  Deleting a scanner from your configuration ............................ 72
  Rebooting and shutting down appliances ............................... 73
  Configuring network interface settings and enabling scanning .............................................................................. 74
  About configuring ATP with a virtual LAN (VLAN) ............... 77
  Defining internal networks to ATP ......................................... 77
  Configuring network proxy information ................................. 79
  Building an enterprise proxy list ........................................... 80
  Specifying the traffic that the proxy inspects .......................... 81
  Configuring connections to DNS servers ............................. 82
  Configuring the connection to a time server ......................... 83
  About syslog server connections ........................................ 84
  Configuring connections to syslog servers ........................... 88
    Editing a connection to a syslog server ............................... 89
    Deleting a connection to a syslog server ............................. 90
Appendix D Required Firewall Ports .................................................... 156
Required firewall ports ...................................................................... 156

Index ........................................................................................................ 162
About Symantec Advanced Threat Protection Platform

This chapter includes the following topics:

- About Symantec Advanced Threat Protection (ATP)
- ATP features per license entitlement
- About endpoint detection and response (EDR)

About Symantec Advanced Threat Protection (ATP)

Symantec Advanced Threat Protection (ATP) performs the critical security tasks that detect, protect, and respond to threats to your network. ATP Platform is comprised of the following control points:

ATP: Network
Processes the network stream in real-time across all Internet ports and protocols and passes it through various filters and detection engines. ATP can detect events on unmonitored endpoints as traffic passes through the scanner. Since ATP doesn't have Symantec Endpoint Protection agent's information, ATP is unable to provide all of the information about the endpoint, such as the user name, last check-in, or Symantec Endpoint Protection Manager group.

ATP: Endpoint
Gathers information by proxying communications between Symantec Endpoint Protection clients and Symantec and by leveraging Symantec Endpoint Protection’s Endpoint Detection and Response (EDR) functionality.

See “About endpoint detection and response (EDR)” on page 15.

ATP: Email
Integrates with Symantec Email Security.cloud to uncover the attacks that enter your organization through email.
ATP: Roaming Collects events from Symantec ATP:Roaming and correlates them with events from your other integrated control points.

ATP uses Synapse™ to correlate ATP network event data with Symantec Email Security.cloud email event data, Symantec Web Security.cloud web data, and Symantec Endpoint Protection endpoint event data, integrating detection and protection across your network, email system, roaming, and endpoints. The Synapse correlation engine automatically matches events with Symantec Endpoint Protection, Email Security.cloud, Web Security.cloud, and ATP to reduce the volume of security alerts. As incidents are detected, they are correlated with other incidents discovered on your network to show overall attack patterns and prioritize the most significant threats.

ATP employs the following detection technologies:

- **Vantage**
  Vantage is a signature-based detection engine that finds threats in the network stream.

- **Insight**
  Insight accesses the world's largest reputation database and has reputation intelligence on over 8 billion files. Insight is a Symantec-owned reputation request service for Insight reputation queries. This service gathers information about the Windows executable files that are observed on endpoints.

- **Mobile Insight**
  Mobile Insight performs similar analyses for Android applications as Insight does for Windows executable files. In addition to tackling malware detection, Mobile Insight also detects privacy and performance issues in mobile apps.

- **Antivirus engine**
  The Antivirus engine is a signature-based technology that detects malware.

- **Cynic**
  Cynic™ analysis and virtual execution detonates files in a cloud-based sandbox environment, analyzes, and reports each step of the observed behavior. Cynic uses machine-learning technology to compare the results to known, bad attributes. It then correlates your data with real-world data provided by the Symantec Global Intelligence Network to determine if the files are malicious.

- **Blacklists and Whitelists**
  Symantec global blacklist and whitelist feeds, which are updated on ATP appliances regularly, accelerate detection and optimize performance. You can also create custom Blacklists and Whitelists that you maintain through ATP.
Symantec Endpoint Protection includes Symantec Online Network for Advanced Response (SONAR) technology for process behavior detection and remediation. However, Symantec Endpoint Protection provides no insight into these details. When you integrate ATP and Symantec Endpoint Protection, ATP can provide insight into SONAR detections. SONAR detects the system changes that have occurred on your managed endpoints, the order that they occurred, and related file attributes. This information gives you greater visibility into the activity that occurs in your environment.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on Symantec Endpoint Protection endpoints to detect emerging threats. SONAR also detects changes or behavior on the endpoints that you should monitor. SONAR does not make detections on application type, but on how a process behaves.

ATP uses a file classifier to analyze files with unknown dispositions. The file classifier breakdowns files by their attributes to determine if the file is good or malicious. The classifier uses decision trees that are trained with millions of files. This technology uses machine-learning instead of signatures or sandbox detonation.

See “About licenses” on page 60.

### ATP features per license entitlement

Table 1-1 describes the features to which you’re entitled based on your Symantec Advanced Threat Protection (ATP) licenses.

<table>
<thead>
<tr>
<th>Feature</th>
<th>License Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td>Synapse</td>
<td>X</td>
</tr>
<tr>
<td>Endpoint Detection and Response (EDR)</td>
<td>X</td>
</tr>
<tr>
<td>Dashboard widgets (separately)</td>
<td>X</td>
</tr>
<tr>
<td>DAI</td>
<td>X</td>
</tr>
<tr>
<td>Data Handling</td>
<td>X</td>
</tr>
<tr>
<td>Backups</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 1-1  (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>License Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td>Reports</td>
<td>X</td>
</tr>
<tr>
<td>ATP notifications</td>
<td>X</td>
</tr>
<tr>
<td>Blocking page</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Based on operating mode</td>
</tr>
<tr>
<td>Search</td>
<td>Database</td>
</tr>
<tr>
<td>Event filtering</td>
<td>X</td>
</tr>
<tr>
<td>Policies</td>
<td>X</td>
</tr>
<tr>
<td>Splunk</td>
<td>X</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>X</td>
</tr>
<tr>
<td>API</td>
<td>X</td>
</tr>
</tbody>
</table>

### About endpoint detection and response (EDR)

With the implementation of Symantec Endpoint Protection 14.0 RU1 and later comes Endpoint Detection and Response (EDR) 2.0. Earlier versions of Symantec Endpoint Protection use EDR 1.0. EDR 1.0 requires that Symantec Advanced Threat Protection (ATP) and endpoint communications rely on the heartbeat between Symantec Endpoint Protection Manager and Symantec Endpoint Protection endpoints. EDR 2.0 refers to the enhanced EDR features that provide direct communication between ATP and Symantec Endpoint Protection endpoints for enhanced searching and management. EDR 2.0 also includes the verbose forensic activity information that the endpoint data recorder provides.

The following tasks can now be performed in near real-time using EDR 2.0:

- Delete file
- Endpoint search
- Endpoint data recorder search¹ and full and process dumps
- Ability for ATP to receive data from endpoints about the following events and activities:¹
  - Suspicious PowerShell executions
    Consists of suspicious PowerShell executions
- Load point changes
  Consists of suspicious modifications to load points
- Suspicious system activity
  Consists of the suspicious activity events that various rules detected
- Heuristic detections
  Consists of heuristically-detected events of a certain order of the system activity events that are known to occur when malware is executed
- Process launch activity
  Consists of most of the total process launch events that are generated

**Note:** Selecting this option can place a high demand on network resources.

- Process terminate activity
  Consists of most of the total of the process terminate events that are generated

**Note:** Selecting this option can place a high demand on network resources.

¹ You must enable the endpoint data recorder feature to perform data recorder searches, data dumps, and receive near-live responses from endpoints.

When ATP issues commands to endpoints that are offline, it periodically rechecks the status of the endpoint to determine if it has come back online. If the endpoint has come online, ATP issues the command. If a search or action is incomplete, queued, canceled, or timed-out, view the endpoint details page **LAST SEEN TIME**. This time indicates the last date and time of contact with the endpoint.

**Important:** See the *Symantec™ Advanced Threat Protection Upgrade Guide* for important information about upgrading ATP and enabling EDR and endpoint data recorder functionality.

To take advantage of the EDR 2.0 features, you must register your Symantec Endpoint Protection Manager(s) with ATP.

See “About the endpoint data recorder” on page 45.

**Note:** EDR data is not forwarded to syslog or Splunk. And EDR 2.0 functionality is not supported on the 8840 appliance.
Performing initial Symantec Advanced Threat Protection setup configurations

This chapter includes the following topics:

- Accessing ATP Manager
- Configuring secure access to ATP Manager
- Completing setup tasks

Accessing ATP Manager

You can access ATP Manager from a web browser on any client computer that can connect to the management port of your management platform or all-in-one appliance. You first access ATP Manager to run the setup wizard after you run bootstrap. Thereafter, you use ATP Manager to configure Symantec Advanced Threat Protection (ATP) and perform security operations.
To access ATP Manager

1. On the computer that can access the network that is connected to the management port, open a web browser.

2. In the web browser, type the following:
   
   https://<IP address>

   Where <IP address> is the address that you specified for the ATP appliance during the bootstrap process.

   For example, if the IP address that you specified for the appliance is 192.168.42.24, go to the following URL:

   https://192.168.42.24

   **Note:** Ensure that you use the HTTPS protocol to access ATP Manager.

3. For certain web browsers, you may need to configure a certificate security exception to access ATP Manager.

   Typically, this step is only required at the first logon per computer per session.

   See “Configuring secure access to ATP Manager” on page 18.

---

## Configuring secure access to ATP Manager

When you start the setup wizard from a browser, Symantec Advanced Threat Protection (ATP) generates a self-signed SSL certificate for ATP Manager. You can use this certificate to encrypt all ATP Manager sessions. For better security, however, Symantec recommends that you install a certificate that is created specifically for your ATP device and is signed by a trusted Certificate Authority.

The following procedure describes how to import a trusted Certificate Authority certificate. Each physical appliance or virtual appliance must have its own unique certificate.

Certificates may be CRT or CER format, with DER or PEM encoding. Only certificates with RSA keys are supported. Keys should not be pass phrase protected. They are encrypted within ATP.

Validation is done after the bundle is uploaded. To complete the validation, the following are required:

- Self-signed server certificate
- Server certificate signed by root CA. Bundle of (server cert + root CA)
Server certificate signed by intermediate CA – could be multiple intermediate CA. Bundle of (server cert + intermediate CAs + root CA)

To secure access to ATP Manager

1 Copy the certificate and key to a location that you can browse to from ATP Manager.
2 In ATP Manager, click **Settings > Global**.
3 In the **SSL Certificate** panel, click **+Add Certificate**.
4 In the **Certificate** field of the dialog box, click **Browse** and then navigate to and select your certificate.
5 In the **Unencrypted Private Key** field of the dialog box, click **Browse** and then navigate to and select your key.
6 Click **Upload**.
7 Repeat steps 3 through 6 on each browser that is used to access ATP Manager.

See “Accessing ATP Manager” on page 17.

### Completing setup tasks

After you complete the preliminary Symantec Advanced Threat Protection (ATP) installation in the setup wizard, complete the system configuration and enable scanning in ATP Manager.

Table 2-1 describes the tasks to complete installation.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new ATP Manager accounts.</td>
<td>Add additional <strong>Admin</strong>, <strong>Controller</strong>, and <strong>User</strong> accounts for accessing ATP Manager.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>As a best practice, you should set up at least one additional Admin user account immediately after installation in case there’s an issue accessing ATP Manager with the initial Admin account credentials.</td>
</tr>
<tr>
<td></td>
<td>See “Managing users” on page 97.</td>
</tr>
<tr>
<td></td>
<td>See “Adding local user accounts” on page 101.</td>
</tr>
<tr>
<td>Set up reports.</td>
<td>Set up the reports that can be generated on a daily, weekly, or monthly schedule.</td>
</tr>
<tr>
<td></td>
<td>See the Symantec™ Advanced Threat Protection Security Operations Manual for more information about reports.</td>
</tr>
</tbody>
</table>
Table 2-1  Tasks to complete Symantec Advanced Threat Protection installation (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload an SSL certificate for ATP Manager</td>
<td>ATP Manager is secured with a self-signed certificate. You can optionally upload a certificate from a certificate authority to protect ATP Manager. See “Configuring secure access to ATP Manager” on page 18.</td>
</tr>
</tbody>
</table>
### Table 2-1

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify proxy information.</td>
<td>ATP supports the following types of proxy configurations:</td>
</tr>
<tr>
<td></td>
<td>■ A network proxy. ATP uses a network proxy to access the external network.</td>
</tr>
<tr>
<td></td>
<td>■ An enterprise proxy within an enterprise environment. ATP treats the traffic that is routed to an enterprise proxy (which may have an</td>
</tr>
<tr>
<td></td>
<td>IP address within an internal network) differently than the traffic that is routed through a network proxy.</td>
</tr>
<tr>
<td></td>
<td>If you use proxies, each ATP appliance, whether in CIU, standalone, or scanner role, must have the IP addresses of existing proxies.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring network proxy information” on page 79.</td>
</tr>
<tr>
<td></td>
<td>See “Building an enterprise proxy list” on page 80.</td>
</tr>
</tbody>
</table>
Configuring global settings

This chapter includes the following topics:

- Changing the geographic location where you submit files for cloud-based sandboxing
- Enabling data handling options
- About Synapse correlation
- About integrating ATP with Symantec Endpoint Protection
- About backing up and restoring ATP data
- About licenses
- Viewing the license status and updating a license
- Viewing certificates
- ATP actions against expiring certificates
- Configuring the connection to an SMTP-compatible mail server
- Customizing and testing blocking pages
- How ATP purges data from the ATP database

Changing the geographic location where you submit files for cloud-based sandboxing

Your organization may have data privacy and residency requirements that restrict you from sending files outside of your region. ATP provides an option that ensures that your files are submitted to a Cynic data center within the United Kingdom (U.K.) for sandbox analysis.

When you enable this feature, all files that are submitted to Cynic for analysis are sent to the U.K. Cynic data center regardless of the sender's geographic location. This means that files
are sent to the U.K. Cynic data center no matter where the incident responder who submits the file is located or no matter where the ATP appliance resides when the network controller submits the file.

**Note:** If you submitted files to Cynic and those files are still being analyzed when you enable this option, you must resubmit those files. See the Logging > Actions page to determine which files need to be resubmitted. Any files that are submitted to Cynic by the network controller and are still being analyzed when you enable this option are not analyzed.

If this is a new installation of ATP or you are setting up a new scanner, Symantec recommends that you enable this option before you enable network scanning. This ensures that no files are inadvertently routed to a U.S. Cynic data center.

Click the following link to learn more about using the Symantec Malware Analysis appliance for on-premises sandboxing.

**To change the geographic location where you submit files for cloud-based sandboxing**

1. In ATP Manager, click **Settings > Global**.
2. Beside the **Cynic Sandboxing** label, check **Use United Kingdom regional instance only**.
3. Click **Ok** in the confirmation dialog box.

### Enabling data handling options

**Data Handling** options determine how Symantec Advanced Threat Protection (ATP) treats data that is not strictly required for evaluating network threats.

**Note:** Unchecking these options may not prevent all communication with Symantec. For example, if you enable correlation with Synapse, data is sent to Symantec for that feature. See “About Synapse correlation” on page 24.

**Table 3-1** describes each data handling option.
Table 3-1  Data handling options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send data to Symantec for statistical and diagnostic purposes</td>
<td>Your appliance (physical or virtual) collects the data that may indicate a hardware or a software issue. It also gathers information on customer interaction with the product and the product usage. When you enable this option, you give Symantec permission to periodically upload the data that helps improve the ATP product. Complete information on this option is available at <a href="http://www.symantec.com/about/profile/policies/eulas/">http://www.symantec.com/about/profile/policies/eulas/</a>.</td>
</tr>
<tr>
<td>Allow Symantec to use evaluated binaries for generating signatures</td>
<td>When you check this option, you give Symantec permission to develop antivirus signatures for any malware that is found on your system. Symantec can then distribute these signatures to all customers through LiveUpdate. If you uncheck this option, Symantec cannot develop and distribute antivirus signatures for the malware that is found exclusively on your system. If the same malware is found independently on another customer's system, however, Symantec may develop and distribute the antivirus signatures.</td>
</tr>
</tbody>
</table>

For additional information about these options, visit [www.symantec.com/about/profile/policies/eulas](http://www.symantec.com/about/profile/policies/eulas) and search for this product.

To enable data handling options

1. In ATP Manager, click **Settings > Global**.
2. Beside the **Data Handling** label, select the options you want to enable.

   **Data Handling** options are enabled by default.

   See “How ATP purges data from the ATP database” on page 66.

### About Synapse correlation

Synapse is a Symantec Advanced Threat Protection (ATP) technology that collects and correlates conviction events from the following Symantec control points: Network, Endpoint, Email, and Roaming. Conviction events are created on a control point when it detects malicious or suspicious activity using Symantec's threat detection technologies. When you enable correlation with a control point, ATP collects and correlates these events on a regular basis.
When correlating events across multiple control points, Synapse searches for common attack artifacts, such as the hash or signature of a malicious file, or the IP address or URL that delivered a threat. When it finds events with a common threat, Synapse creates a properly prioritized incident based on the status of the threat on each control point.

For example, suppose that Synapse finds an ATP: Network event and an ATP: Endpoint event with the same malware. If the malware was not blocked on the endpoint, Synapse creates a high-priority incident; if the malware was blocked, Synapse creates a low-priority incident. By providing this intelligence, Synapse significantly reduces the number of incidents that you need to investigate, letting you focus on the high-priority incidents that may require immediate attention.

Collecting events from multiple control points also lets you perform powerful searches across your entire environment, regardless of correlation. For example, suppose that one of your feeds warns you about a new threat that is unknown to Symantec. You can quickly query the events that were collected from your control points to see if this threat exists anywhere in your environment. If so, you can quickly take action to remediate the threat to ensure that no other devices are infected.

You can enable Synapse correlation for the control points you purchased. Once enabled, Synapse starts collecting and correlating events right away.

See “Enabling Synapse correlation with Email Security.cloud” on page 25.
See “About integrating ATP with Symantec Endpoint Protection” on page 27.

Enabling Synapse correlation with Email Security.cloud

Symantec Email Security.cloud provides detection methods and intelligence to protect your organization against zero day threats and targeted attacks. The detection methods include malware analysis and protection against malicious URL links within emails. In addition to blocking known threats, Email Security.cloud sends copies of files of interest to the Symantec Cynic cloud service for additional analysis.

Using Synapse, you can enable correlation between Symantec Advanced Threat Protection (ATP) and Email Security.cloud. When enabled, Synapse collects conviction events from Email Security.cloud and correlates them with events from your other control points (such as Network, Endpoint, and Roaming). When correlating these events, Synapse looks for relationships based on common threats and suspicious behavior. It then correlates common events into a single incident, helping you to identify and prioritize your work. After you enable Symantec Email Security.cloud Correlation, ATP starts collecting email events within the hour. You can view information about these events in ATP Manager.

See “About Synapse correlation” on page 24.
To enable correlation, your organization must subscribe to Email Security.cloud where the Email Advanced Threat Protection service is enabled. This subscription must have a Symantec Email Security.cloud user login account associated with it that has View Statistics permissions. The login account is used to enable correlation in ATP Manager.

Note: You can enable Symantec Email Security.cloud correlation on multiple ATP management platforms. However, you must use a different login account on each platform.

If the credentials for this account change (for example, you change your password), you can re-enter them by disabling and re-enabling Email Security.cloud Correlation in ATP Manager.

See “Required firewall ports” on page 156.

To enable Synapse correlation with Email Security.cloud

1. In ATP Manager, click Settings > Global.
2. In the Synapse section, check Enable Symantec Email Security.cloud Correlation.
3. In the dialog box, type the Symantec Email Security.cloud Login name and Symantec Email Security.cloud Password for your Email Security.cloud user login account, and then click Enable.

The format of the user name should be three letters followed by four numbers (e.g., ABC1234). Symantec provides this user name when you register for the service. Also, these credentials should be separate from the main admin account, have View Statistics permission, and be dedicated to ATP usage only.

Enabling Synapse correlation with Symantec ATP:Roaming

Symantec ATP:Roaming is a Symantec Web Security.cloud service that detects and blocks threats embedded in unencrypted (HTTP) and SSL-encrypted (HTTPS) web traffic. ATP: Roaming inspects web traffic from both your on-LAN and off-LAN (or "roaming") users. It also sends copies of files to Symantec Cynic for additional analysis.

Using Synapse, you can enable correlation between Symantec Advanced Threat Protection (ATP) and ATP:Roaming. When enabled, Synapse collects conviction events from ATP:Roaming and correlates them with events from your other control points (such as Network, Endpoint, and Email). When correlating these events, looks for relationships based on common threats and suspicious behavior. It then correlates common events into a single incident, helping you to identify and prioritize your work. After you enable ATP:Roaming Correlation, ATP starts collecting events within the hour. You can view information about these events in ATP Manager.

To enable correlation, your organization must have a licensed Symantec.cloud account for which ATP: Roaming is enabled. This account must have a Symantec Web Security.cloud user login account associated with it that has View Statistics permissions.

See “About Synapse correlation” on page 24.
To enable Synapse correlation with Symantec ATP:Roaming

1. In ATP Manager, click Settings > Global.
2. In the Synapse section, check Enable Symantec ATP:Roaming Correlation.
3. In the dialog box, type the Symantec Web Security.cloud Login and Symantec Web Security.cloud Password for your Web Security.cloud account, and then click Enable.

The format of the user name should be three letters followed by four numbers (e.g., ABC1234). Symantec provides this user name when you register for the service. Also, these credentials should be separate from the main admin account, have View Statistics permission, and be dedicated to ATP usage only.

See “Enabling Synapse correlation with Email Security.cloud” on page 25.

About integrating ATP with Symantec Endpoint Protection

Symantec Advanced Threat Protection (ATP) integrates with Symantec Endpoint Protection to let you detect and respond to potential threats at endpoints in your system. There are a number of configuration steps and procedures to fully integrate with Symantec Endpoint Protection, and you will most likely want to enable full integration. This section describes an overview of the configuration process with links to further details about each step. Integration with Symantec Endpoint Protection provides these capabilities:

- Correlation of event data from Symantec Endpoint Protection Manager to ATP through Synapse.
- Viewing files from endpoints and performing operations on those files, such as uploading the files to ATP for further analysis.
- Sending administrative commands to Symantec Endpoint Protection Manager and endpoints, such as adding files and domains to the whitelist or blacklist.
- Allowing ATP to act as a proxy for network requests for endpoints managed by Symantec Endpoint Protection. This lets ATP monitor and manage all network traffic from the endpoints and provide threat assessment for dangerous activity.
Note: If you enable integration with Symantec Endpoint Protection after you have already been scanning your network for some time, it is possible that duplicate records can be created in ATP after Symantec Endpoint Protection integration is enabled. This occurs in situations when network scanning is performed on endpoints and only the IP address of the endpoint is available (reverse DNS lookups are not enabled on the system). You can avoid this by either ensuring that reverse DNS lookups are available on your endpoints or by first enabling Symantec Endpoint Protection integration before enabling network scanning in ATP.

Before you integrate with Symantec Endpoint Protection, ensure that your Symantec Endpoint Protection installation meets the requirements for integration.

See “System requirements for ATP integration with Symantec Endpoint Protection management interfaces and embedded databases” on page 154.

See “Symantec Endpoint Protection client versions and supported ATP features” on page 31.

See “ATP / Symantec Endpoint Protection integration workflow” on page 29.

See “Required firewall ports” on page 156.
## ATP / Symantec Endpoint Protection integration workflow

### Table 3-2  ATP integration with Symantec Endpoint Protection workflow

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | On Symantec Endpoint Protection Manager, prepare the database for log collection. | Before ATP can collect incident logs, you must prepare each database so that ATP can log on to it remotely. The steps to prepare the Symantec Endpoint Protection Manager database depend on whether your system uses an external Microsoft SQL Server database or the embedded Symantec Endpoint Protection Manager database.  
  - Microsoft SQL natively supports remote access. Symantec strongly recommends that you create a read-only account on this database for ATP to access the data. Alternatively, you can let ATP access the database using DB administrator (sa) credentials.  
    See “Creating an ATP read-only account for a Symantec Endpoint Protection Manager SQL database” on page 34.  
  - The Symantec Endpoint Protection Manager embedded database format does not natively support remote access, so you must download a file from ATP Manager, install this software on Symantec Endpoint Protection Manager, and perform some configuration before ATP can collect incident logs.  
    See “Preparing a Symantec Endpoint Protection Manager embedded database for ATP log collection” on page 36. |
| 2    | Enable Synapse correlation of event data from Symantec Endpoint Protection. | Before connections to Symantec Endpoint Protection Manager databases can be configured, the Enable Symantec Endpoint Protection Correlation option must be checked in the Settings > Global > Synapse area of ATP Manager.  
    See “About Synapse correlation” on page 24. |
| 3    | In ATP Manager, configure the connection to the Symantec Endpoint Protection Manager database. | After you prepare the database for log collection, use the following procedure to enter the database information into ATP Manager.  
    See “Configuring the connection to the Symantec Endpoint Protection Manager database” on page 38. |
### Table 3-2  ATP integration with Symantec Endpoint Protection workflow (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4    | In ATP Manager, configure the connection to Symantec Endpoint Protection Manager instances. | For ATP to communicate with Symantec Endpoint Protection Manager, a connection must be configured to Symantec Endpoint Protection Manager. The connection serves these purposes:  
  - Administrative changes, such as changes to the whitelist or blacklist made through ATP, are sent to Symantec Endpoint Protection Manager through the SEPM controller connection.  
  - Information about the endpoints managed by Symantec Endpoint Protection Manager is retrieved through the SEPM controller connection so that it can be associated with event data. For example, computer names that are stored by Symantec Endpoint Protection Manager can be correlated to IP addresses in event messages.  
  See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39. |
| 5    | In Symantec Endpoint Protection Manager, configure Host Integrity and quarantine firewall policies, if not already enabled. | To isolate and rejoin endpoints from ATP Manager, you must have a Quarantine Firewall policy and Host Integrity policy set up in Symantec Endpoint Protection Manager. This requirement is necessary to ensure that the endpoint is put into/taken out of quarantine in the event that your Host Integrity policy FAILS, regardless of what the THEN clause states. If you run Symantec Endpoint Protection 14 RU1 or above, ATP automatically creates these policies when you configure your Symantec Endpoint Protection Manager integration. Otherwise, you must manually create these policies. Click the following link to learn more about how to create Symantec Endpoint Protection Manager Host Integrity policies: [http://www.symantec.com/docs/HOWTO101742](http://www.symantec.com/docs/HOWTO101742)  
  See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39. |
| 6    | In Symantec Endpoint Protection Manager, configure endpoints to send information to the ATP management node. | For ATP to act as a proxy for Symantec Endpoint Protection endpoint computers, the endpoints must be configured to send event data to ATP through the private cloud setting.  
  See “Configuring endpoints in Symantec Endpoint Protection Manager to communicate with ATP” on page 42. |
Table 3-2  ATP integration with Symantec Endpoint Protection workflow (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>In ATP Manager, add SSL certificates for secure communication between endpoints and ATP, if needed.</td>
<td>If secure communication between endpoints and ATP is needed when ATP acts as a proxy for endpoint network communication, you can upload the SSL certificates that may be required to secure the communication. See “Securing communication between endpoints and ATP” on page 56.</td>
</tr>
</tbody>
</table>

See “About integrating ATP with Symantec Endpoint Protection” on page 27. See “Required firewall ports” on page 156.

Symantec Endpoint Protection client versions and supported ATP features

Table 3-3  Supported Symantec Endpoint Protection 14.x versions by feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>14.1</th>
<th>14.0 RU1</th>
<th>14.0 MP1</th>
<th>14.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint search¹</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>Endpoint data recorder search</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>ATP database search</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>Event forwarding to ATP (live response)</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>SHA2 whitelisting/blacklisting</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>MD5 whitelisting/blacklisting</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
</tbody>
</table>
### Table 3-3

**Supported Symantec Endpoint Protection 14.x versions by feature (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>14.1</th>
<th>14.0 RU1</th>
<th>14.0 MP1</th>
<th>14.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a file</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Delete file (live response)</td>
<td>🟢</td>
<td>🟢</td>
<td></td>
<td>🟢</td>
</tr>
<tr>
<td>Delete file (thru Symantec Endpoint Protection Manager heartbeat)</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Cancel file delete and searches</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Isolate/rejoin endpoint</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Run Power Eraser</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Insight and submissions redirection from Symantec Endpoint Protection Manager</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Insight redirection from Symantec Endpoint Protection Manager</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Local Insight and submissions redirection</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
</tbody>
</table>

¹ ATP supports endpoint searches on endpoints running Symantec Endpoint Protection 14.0 and above. However, only endpoints that run Symantec Endpoint Protection 14.0 RU1 and later can take advantage of endpoint searches using EDR 2.0 functionality. Prior versions use EDR 1.0 functionality. See “About endpoint detection and response (EDR)” on page 15.
### Table 3-4  
**Supported SEP 12.x versions by feature**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported Symantec Endpoint Protection 12.x versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint search</td>
<td>ATP supports endpoint searches for the clients that use Symantec Endpoint Protection 12.1 RU5 and later. ATP manages the clients that use Symantec Endpoint Protection 12.1 RU 6 MP3 or later with full EDR 1.0 functionality. However, for the clients that use a version between Symantec Endpoint Protection 12.1 RU5 and 12.1 RU6 MP3, some functionality may be limited depending upon the version of the client.</td>
</tr>
<tr>
<td>Endpoint data recorder search</td>
<td>Unsupported</td>
</tr>
<tr>
<td>ATP database search</td>
<td>12.1 RU5 and later</td>
</tr>
<tr>
<td>Event forwarding to ATP (near live response)</td>
<td>Unsupported</td>
</tr>
<tr>
<td>SHA2 whitelisting/ blacklisting</td>
<td>12.1 RU6 MP7</td>
</tr>
<tr>
<td>MD5 whitelisting/ blacklisting</td>
<td>12.1 RU2 and later</td>
</tr>
<tr>
<td>Get a file</td>
<td>12.1 RU6 MP3</td>
</tr>
<tr>
<td>Delete file (live response)</td>
<td>Unsupported</td>
</tr>
<tr>
<td>Delete file (thru Symantec Endpoint Protection Manager heartbeat)</td>
<td>12.1 RU6 MP2 and later</td>
</tr>
<tr>
<td>Cancel file delete and searches</td>
<td>12.1 RU6 MP5 and later</td>
</tr>
<tr>
<td>Isolate/rejoin endpoint</td>
<td>12.1 RU6 MP3</td>
</tr>
<tr>
<td>Insight and submissions redirection from Symantec Endpoint Protection Manager</td>
<td>12.1 RU6 and later</td>
</tr>
<tr>
<td>Insight redirection from Symantec Endpoint Protection Manager</td>
<td>12.1 RU3 and later</td>
</tr>
<tr>
<td>Local Insight and submissions redirection</td>
<td>12.1 RU2 and later</td>
</tr>
</tbody>
</table>

### Table 3-5  
**Supported Symantec Endpoint Protection Manager versions by feature**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Symantec Endpoint Protection Manager version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud settings</td>
<td>SEPM 14.0 RU1 and later</td>
</tr>
</tbody>
</table>
Table 3-5  
Supported Symantec Endpoint Protection Manager versions by feature 
(continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Symantec Endpoint Protection Manager version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete blacklist/whitelist</td>
<td>SEPM 14.0 and later</td>
</tr>
<tr>
<td>API OAuth 2 authentication requirement</td>
<td>SEPM 12.1 RU6 and later</td>
</tr>
</tbody>
</table>

See "About integrating ATP with Symantec Endpoint Protection" on page 27.

Creating an ATP read-only account for a Symantec Endpoint Protection Manager SQL database

The following procedure describes how to create a read-only account that lets Symantec Advanced Threat Protection (ATP) log on to a Symantec Endpoint Protection Manager SQL database to collect incident logs for Synapse correlation. Once you create this account in Symantec Endpoint Protection Manager, you can configure ATP to connect to the SQL database.

To create a read-only account for a Symantec Endpoint Protection Manager SQL database

1 On the Symantec Endpoint Protection management server, open a PowerShell window.
2 Type the following command to open the sqlcmd utility.
   
   sqlcmd -S localhost -U sa -P<yourDBSAPassword>

   Replace <YourDBSAPassword> with your DB administrator password.
To create the read-only user satpn_ro, paste the following SQL commands directly into the utility.

Replace sem5 with the name of your DB and mypassword with the password that you want to assign to this account.

```
EXEC sp_addlogin 'satpn_ro', 'mypassword', 'sem5'
USE sem5
CREATE USER satpn_ro FOR LOGIN satpn_ro
EXEC sp_addrolemember 'db_datareader', 'satpn_ro'
GRANT SELECT ON SEM_COMPUTER to satpn_ro;
GRANT SELECT ON V_AGENT_BEHAVIOR_LOG to satpn_ro;
GRANT SELECT ON IDENTITY_MAP to satpn_ro;
GRANT SELECT ON V_AGENT_PACKET_LOG to satpn_ro;
GRANT SELECT ON V_AGENT_SECURITY_LOG to satpn_ro;
GRANT SELECT ON V_AGENT_TRAFFIC_LOG to satpn_ro;
GRANT SELECT ON V_AGENT_SYSTEM_LOG to satpn_ro;
GRANT SELECT ON V_ENFORCER_CLIENT_LOG to satpn_ro;
GRANT SELECT ON V_ENFORCER_SYSTEM_LOG to satpn_ro;
GRANT SELECT ON V_ENFORCER_TRAFFIC_LOG to satpn_ro;
GRANT SELECT ON V_SERVER_ADMIN_LOG to satpn_ro;
GRANT SELECT ON V_SERVER_SYSTEM_LOG to satpn_ro;
GRANT SELECT ON V_SERVER_CLIENT_LOG to satpn_ro;
GRANT SELECT ON V_SERVER_ENFORCER_LOG to satpn_ro;
GRANT SELECT ON V_SERVER_POLICY_LOG to satpn_ro;
GRANT SELECT ON V_LAN_DEVICE_DETECTED to satpn_ro;
GRANT SELECT ON V_ALERTS to satpn_ro;
GRANT SELECT ON VIRUS to satpn_ro;
GRANT SELECT ON V_SEM_COMPUTER to satpn_ro;
GRANT SELECT ON SEM_AGENT to satpn_ro;
GRANT SELECT ON PATTERN to satpn_ro;
GRANT SELECT ON HPP_ALERTS to satpn_ro;
```
GRANT SELECT ON SEM_APPLICATION to satpn_ro;
GRANT SELECT ON ACTUALACTION to satpn_ro;
GRANT SELECT ON ALERTMSG to satpn_ro;
GRANT SELECT ON HPP_APPLICATION to satpn_ro;
go

4 Type quit to exit.

5 In ATP Manager, add this database.
   See “Configuring the connection to the Symantec Endpoint Protection Manager database” on page 38.
   See “Configuring the connection to the Symantec Endpoint Protection Manager database” on page 38.

Preparing a Symantec Endpoint Protection Manager embedded database for ATP log collection

The log collector enables ATP to collect incident logs from a Symantec Endpoint Protection Manager database. To complete this procedure, you must be logged onto ATP Manager and the Symantec Endpoint Protection Manager server as an administrator. The Symantec Endpoint Protection Manager server must also meet certain system requirements.

See “System requirements for ATP integration with Symantec Endpoint Protection management interfaces and embedded databases” on page 154.

Note: The log collector utility installation is for MS Windows systems only.

The log collector uses port 8081 by default. If another process uses the same port, log collection fails. You can resolve any conflict by either moving the other process to a different port or you can edit the log collector port setting in step 5.

To prepare a Symantec Endpoint Protection Manager embedded database for ATP log collection

1 In ATP Manager, click Settings > Global.

2 In the Symantec Endpoint Protection Manager (SEPM) Databases group, click Download Synapse Log Collector for SEPM Embedded DB and save the file (SEPMLogCollector.msi) to your local disk.

3 Move the file onto the computer where the Symantec Endpoint Protection Manager database is located and run the file to install the log collector.
4 Proceed through the installation steps to specify the location for installation and continue until the installation is complete. Make sure to check **Launch Log Collector Configuration Utility** before clicking **Finish** to complete the installation.

5 The log collector configuration utility presents you with the following fields to complete:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service IP Address</strong></td>
<td>The IP address of the Symantec Endpoint Protection Manager computer. Make certain the ATP management node has access to this IP address. This is the address the log collector binds to for accepting new requests for logs.</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>The port number the log collector uses to listen for incoming requests. The default is 8081. <strong>Note:</strong> Make certain this port is enabled on your firewall to ensure that communication between your Symantec Endpoint Protection Manager database and the ATP management platform is allowed. See “Required firewall ports” on page 156.</td>
</tr>
<tr>
<td><strong>Log Collector Connection Password</strong></td>
<td>Specify the password that you would like to use for the log collector connection. This password is later used in the ATP configuration settings when creating a connection to the Symantec Endpoint Protection Manager database.</td>
</tr>
<tr>
<td><strong>Confirm Connection Password</strong></td>
<td>Re-enter the password from the previous field.</td>
</tr>
<tr>
<td><strong>Symantec Endpoint Protection Manager Embedded Database Configuration Password</strong></td>
<td>The password of the Symantec Endpoint Protection Manager database.</td>
</tr>
</tbody>
</table>

6 Click the **Test Database Connection** button to test that the connection works properly. If the connection fails, check the Symantec Endpoint Protection Manager database password that you supplied in the configuration fields to make certain it is correct.

7 Click **Confirm** to complete the log collector configuration.

8 In the ATP administration interface, add a Symantec Endpoint Protection Manager database connection that matches the configuration information you specified in step 5.

See “Configuring the connection to the Symantec Endpoint Protection Manager database” on page 38.
Configuring the connection to the Symantec Endpoint Protection Manager database

Before performing this procedure, make sure the Symantec Endpoint Protection Manager database is prepared for use with Symantec Advanced Threat Protection (ATP).

See "About integrating ATP with Symantec Endpoint Protection" on page 27.

---

**Note**: Up to ten connections to Symantec Endpoint Protection Manager databases have been tested and supported, but you can specify any number of connections in your configuration. If you have a complex Symantec Endpoint Protection installation that uses replication, you can configure only one database connection per replication group.

---

**Note**: For more information about the implications of replication groups and connections to the Symantec Endpoint Protection Manager instances, see the following topic.

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.

---

**To configure the connection to a Symantec Endpoint Protection Manager database**

1. In ATP Manager, click **Settings > Global**.
2. In the **Synapse** area, check **Enable Symantec Endpoint Protection Correlation**, if it is not already checked.

   When **Enable Symantec Endpoint Protection Correlation** is checked and the correlation is listed as **Healthy**, proceed to the next step.

3. In the **Symantec Endpoint Protection Manager (SEPM) Database** area, click **+Add SEPM**.
4. Enter the following information to configure a database:

   - **DB Type**: Select **MS SQL** from the list to collect logs from an external Microsoft SQL Server or select **Embedded DB** to collect logs from an embedded database.
   - **Entry Name**: Type the name of your Symantec Endpoint Protection Manager database server.
   - **DB Name**: Type the database name. This field requires a specific name for the database itself, not the host name. The name that you type here is case-sensitive and must exactly match the database name that is configured in Symantec Endpoint Protection Manager.
Type the listening IP address for the database server or database server named instance. This IP address must be static.

Type the listening TCP port that is configured for the database server or database server named instance. This port must be static.

If you are using an MS SQL database, do one of the following:

- Type the user name and password of the local Symantec Endpoint Protection Manager read-only account that you created to access the MS SQL database.
  See “Creating an ATP read-only account for a Symantec Endpoint Protection Manager SQL database” on page 34.
- Type the user name and password of a Symantec Endpoint Protection Manager account that you authenticated with a Microsoft Active Directory account. This account must have the appropriate login permissions.
  For details, see the Symantec™ Endpoint Protection Installation and Administration Guide.

If you are using an embedded database:

- Type the user name and password that you specified when you installed the log collector.
  See “Preparing a Symantec Endpoint Protection Manager embedded database for ATP log collection” on page 36.

Check this box to enable ATP to log on and gather logs from this database. (You can selectively enable and disable databases as needed without deleting the configuration information.)

5 Click Save.

About configuring the connection to Symantec Endpoint Protection Manager

For Symantec Advanced Threat Protection (ATP) to communicate with your endpoints, you must configure a connection to the Symantec Endpoint Protection Manager management server. The following is important information that you should know about setting up this connection.

Communication protocols, ports, and certificates
Communication protocols, ports, and certificates

Symantec recommends that all Symantec Endpoint Protection endpoint configuration settings use HTTPS and port 443 for communicating with ATP version 3.0 and later. For Symantec Endpoint Protection endpoints to communicate with ATP through this secure protocol, the endpoints must have a valid SSL certificate installed, allowing secure communication with ATP. The Symantec Endpoint Protection communication configuration dialog on ATP provides a mechanism to configure the Symantec Endpoint Protection port and protocol communication settings on Symantec Endpoint Protection Manager using Symantec Endpoint Protection’s private APIs. In addition, when the Symantec Endpoint Protection communication settings are saved on ATP, ATP’s SSL certificate is also pushed to the endpoints so that they can securely communicate with ATP over HTTPS. The certificate that is pushed down to endpoints through this mechanism uses a certificate that is configured on ATP at the time the settings are saved. This certificate is either the default built-in, self-signed ATP certificate or another trusted certificate that has been uploaded through ATP Manager. Only Symantec Endpoint Protection endpoints that run 14.0 RU 1 or later can take advantage of ATP’s private APIs to automatically receive ATP’s SSL certificate through this mechanism. If you have an environment with endpoints that run a previous version of Symantec Endpoint Protection, you must install ATP’s SSL certificate separately so that the endpoints securely communicate with ATP.

Important considerations about connections to multiple Symantec Endpoint Protection Manager instances

- Up to ten connections to Symantec Endpoint Protection Manager have been tested and are supported, but you can have any number of connections in your configuration.

- If you have multiple connected Symantec Endpoint Protection Manager instances at a site (that is, the Symantec Endpoint Protection Manager instances share a database), create a connection to only one Symantec Endpoint Protection Manager per site in ATP Manager. If multiple Symantec Endpoint Protection Managers from the same site attempt to connect to the same ATP management platform, they compete for authentication credentials and might not operate properly.

- With multiple connected Symantec Endpoint Protection Manager instances per site, commands from ATP are sent to the shared database by the instance that is connected to ATP. Therefore, all shared instances perform the command properly. But only the instance that executed the command may have the record of the command in the Symantec Endpoint Protection Manager console.

- When you use replication between Symantec Endpoint Protection Manager instances, the commands that ATP sends can take up to two replication cycles to propagate to all Symantec Endpoint Protection Manager instances in the environment. If you have enabled replication in your Symantec Endpoint Protection environment, then check the Replication is enabled between all SEPM’s box on the Settings > Global page for Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder settings in ATP Manager. When your entire network uses Symantec Endpoint Protection 14.0 RU1 or higher,
replication is no longer needed since ATP can communicate directly to the Symantec Endpoint Protection endpoints.

- Consider carefully your deployment strategy of ATP when working with a complex Symantec Endpoint Protection environment. You can reduce the amount of time to propagate commands by not using replication in Symantec Endpoint Protection and having ATP individually connect to each Symantec Endpoint Protection Manager instance. However, that may not be compatible with your current Symantec Endpoint Protection strategy.

**Important considerations about multiple domains in your Symantec Endpoint Protection management server**

- You must create a separate Symantec Endpoint Protection Manager connection for each configured domain. See the Symantec Endpoint Protection documentation for a complete description of the domains that Symantec Endpoint Protection defines.

- If you don't create a Symantec Endpoint Protection Manager connection for a defined domain in your environment, the commands that are sent to Symantec Endpoint Protection Manager are not forwarded to resources in the domain.

- You may see an error when sending a command to resources in domains without configured connections. Check the **Logging > Actions** page to determine which resources have not executed the command. Define a Symantec Endpoint Protection Manager connection for the domain that is associated with those resources to resolve the issue.

**Location of Symantec Endpoint Protection Manager and Symantec Endpoint Protection endpoints**

Symantec Endpoint Protection Manager and Symantec Endpoint Protection endpoints must be on separate computers for the EDR commands to function properly. Otherwise, when an endpoint is isolated (quarantined), there is no way to rejoin (unquarantine) it. The reason is that isolating the endpoint also isolates the Symantec Endpoint Protection Manager, so the connection between ATP and Symantec Endpoint Protection Manager is blocked.

**ATP auto-generated Symantec Endpoint Protection Manager policies**

Upon initial registration of the Symantec Endpoint Protection Manager, ATP installs Symantec Endpoint Protection Manager Host Integrity and Quarantine Firewall policies. Both policies are applied to each Symantec Endpoint Protection Manager non-inherited subgroup if none already exists. This is because if it is inherited, the parent's policy will apply to this group. Note that ATP unconditionally installs the ATP bundled policies but only applies them to the subgroups as necessary during registration. The policies appear as "ATP Host Integrity policy" and "ATP Quarantine Firewall policy" on your Symantec Endpoint Protection Manager. If you enable the endpoint data recorder, ATP also automatically adds an "ATP FDR Default" policy in Symantec Endpoint Protection Manager.

These policies are automatically created and applied to Symantec Endpoint Protection Manager without any interaction or notice in ATP Manager. As endpoints are added or moved between
subgroups, the endpoints inherit the group policy. ATP does not overwrite existing Quarantine Firewall policy or Host Integrity policy.

See “Configuring EDR 2.0 and the endpoint data recorder” on page 43.

See “About integrating ATP with Symantec Endpoint Protection” on page 27.

See “System requirements for ATP integration with Symantec Endpoint Protection management interfaces and embedded databases” on page 154.

See “Symantec Endpoint Protection client versions and supported ATP features” on page 31.

Configuring endpoints in Symantec Endpoint Protection Manager to communicate with ATP

You can configure your endpoints to communicate with Symantec Advanced Threat Protection (ATP) via the private cloud setting in Symantec Endpoint Protection Manager. Click the link below to learn more about how to configure endpoints to connect with ATP via ATP Manager.

See “Configuring the connection to Symantec Endpoint Protection Manager” on page 47.

If you upgrade to ATP 3.0 or later and want to preserve legacy behavior, your endpoints must be configured to connect through HTTP 8080 or HTTP 8443. If you use the Symantec Endpoint Protection proxy and want to take advantage of EDR 2.0 functionality, use HTTPS 443.

**Important:** Enrolled endpoints are disconnected when you re-configure these ports. However, the endpoint enrollment status does not appear changed in ATP Manager. If you reconfigure the Symantec Endpoint Protection Manager ports, you must re-enroll your Symantec Endpoint Protection endpoints with ATP.

---

**Note:** When you redeploy ATP without removing the Symantec Endpoint Protection Manager Controller, endpoints remain in an enrolled state. However, if you remove ATP from Symantec Endpoint Protection Manager's group settings, the endpoint are technically unenrolled. There is no longer a connection between endpoints and ATP.

---

**To configure endpoints in Symantec Endpoint Protection Manager to communicate with ATP**

1. Log into Symantec Endpoint Protection Manager.
2. Click **Clients**, then select the group that you want to configure.
   
   In Symantec Endpoint Protection, you can set policies on a per-computer or on a group basis. For more information about setting up groups, see the Symantec Endpoint Protection documentation.
3. For the desired computers or groups, go to the **Policies** tab and click **External Communications Settings**.
4. On the **External Communications Settings** dialog, click the **Private Cloud** tab.
5. Check **Enable private servers to manage my data**, and then click **Use ATP servers for Insight lookups and submissions**.

6. Check **Use Symantec servers when private servers are not available**.

7. Click **Add>>** and select **New server**.

8. In the **Add Server** dialog box, specify the URL and port number of ATP Manager.
   
The default protocol and port are HTTP and port 8080. Before selecting the HTTPS protocol, read the following topic:
   
   See “Securing communication between endpoints and ATP” on page 56.

9. Click **OK** in each dialog to complete the configuration.

### Configuring EDR 2.0 and the endpoint data recorder

EDR 2.0 is enabled by default upon new installations of ATP. It is disabled by default if you upgrade from a prior version of ATP. You can enable EDR 2.0 and not configure or use the endpoint data recorder. However, you cannot use the endpoint data recorder feature without enabling EDR 2.0. If you enable the endpoint data recorder, creating exclusions and exceptions are optional.

Table 3-6 provides the workflow for configuring EDR and the endpoint data recorder.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Enable EDR 2.0.  
Enable EDR 2.0 so that near real-time live responses and the endpoint data recorder function. EDR 2.0 is enabled by default upon new installations.  
See “Enabling and disabling EDR 2.0” on page 46. |
| Step 2 | Specify Symantec Endpoint Protection Manager information.  
Provide the necessary information to connect to your Symantec Endpoint Protection Manager, such as IP address, domain, user name, and password. Optionally, you can install an SSL certificate to secure communications between ATP and Symantec Endpoint Protection Manager.  
**Important**: Create a separate account on Symantec Endpoint Protection Manager for the sole purpose of connecting it with ATP.  
See “Configuring the connection to Symantec Endpoint Protection Manager” on page 47. |
### Table 3-6  
EDR and the endpoint data recorder configuration workflow (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3      | **Configure communication from Symantec Endpoint Protection to ATP Manager.**  
              The private cloud settings push out ATP's self-signed certificate to endpoints.  
              Confirm the address of the ATP Manager. Specify if you want to use ATP to perform Insight lookups or Symantec’s public servers.  
              **Important:** You must configure the protocol to HTTPS and the port to 443.  
              See “Configuring communication with your Symantec Endpoint Protection clients” on page 50.                                                                                     |
| Step 4      | **Enable and configure the endpoint data recorder.**  
              Create the global endpoint data recorder policies that are applied to all of your managed endpoints. Data is submitted to ATP from clients based on a minimal time interval and maximum batch size. You can specify these thresholds.  
              As endpoints are added to a group or moved to a different group, the endpoint inherits that group’s global policy, exclusions, and exceptions.  
              **Note:** Your endpoints must be running Symantec Endpoint Protection 14.0 RU1 or later to enable the endpoint data recorder.  
              See “Configuring the endpoint data recorder” on page 52.  
              See “About the endpoint data recorder” on page 45.                                                                                                                                     |
| Step 5      | **Specify endpoint data recorder exclusions.**  
              Specify file hash exclusions or file path exclusions. You can specify SHA256 file hashes.  
              See “Configuring Symantec Endpoint Protection endpoint data recorder policy exceptions” on page 54.                                                                                       |
| Step 6      | **Configure endpoint data recorder group exceptions.**  
              Specify endpoint data recorder exceptions for specific Symantec Endpoint Protection Manager groups.  
              See “Configuring Symantec Endpoint Protection endpoint data recorder exclusions” on page 56.                                                                                         |

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.  
See “About endpoint detection and response (EDR)” on page 15.
About the endpoint data recorder

If you run Symantec Endpoint Protection 14.0 RU1 and later, you can configure your endpoints to record the activities and events that occur on them. When you integrate Symantec Advanced Threat Protection (ATP) with Symantec Endpoint Protection, the endpoint data recorder offers ATP unrestricted insight into endpoint activity.

ATP can receive data from endpoints from the endpoint data recorder about the following events and activities:

- Suspicious PowerShell executions
  Consists of suspicious PowerShell executions
- Load point changes
  Consists of suspicious modifications to load points
- Suspicious system activity
  Consists of suspicious activity events that various rules detected
- Heuristic detections
  Consists of heuristically-detected events of a certain order of system activity events that are known to occur when malware is executed
- Process launch activity
  Consists of most of the total process launch events that are generated

  Note: Selecting this option can place a high demand on network resources.

- Process terminate activity
  Consists of most of the total of process terminate events that are generated

  Note: Selecting this option can place a high demand on network resources.

Register your Symantec Endpoint Protection Manager with ATP so that ATP can receive near-live response data from your endpoints about the events that occur on them. The endpoint data recorder events appear throughout ATP Manager along with other types of events (such as network events), in Dashboard widgets, on the Search > Database > Events page, and entity details pages. ATP uses the endpoint data recorder events along with other event types to create the incidents that appear on the Incident Manager.

You can also perform searches of the endpoint recorder data and retrieve full dumps or process dumps of data for forensic analysis and investigation.

You must register your Symantec Endpoint Protection Manager(s) with ATP to enable the endpoint data recorder. As part of that registration, you can specify whether you want ATP to receive near-live response event data or event data at scheduled intervals. You can also create
global policies for file exclusions and Symantec Endpoint Protection Manager subgroup exceptions.

See “About endpoint detection and response (EDR)” on page 15.

See also the Symantec™ Advanced Threat Protection Installation Guide for important information about the necessary sizing requirements that are needed to take advantage of endpoint data recorder features.

Note: Endpoint data recorder events are not forwarded to syslog.

Enabling and disabling EDR 2.0

EDR 2.0 refers to the enhanced Endpoint Detection and Response (EDR) features of Symantec Advanced Threat Protection (ATP) and Symantec Endpoint Protection. This enhanced functionality is available in ATP version 3.0 and later and SEP 14.1 and later. These features include direct communication between ATP and Symantec Endpoint Protection endpoints for enhanced searching and management. The feature also includes the verbose forensic activity information that the endpoint data recorder provides. EDR 2.0 is enabled by default in new installations of ATP version 3.0 and later. In this case, leave the option enabled. Then add Symantec Endpoint Protection Manager configuration details, Symantec Endpoint Protection Communication settings, and Endpoint Data Recorder configuration settings to start using EDR 2.0.

See “Configuring EDR 2.0 and the endpoint data recorder” on page 43.

Important: When you upgrade from ATP 2.3 or earlier, you must change the port and possibly the protocol that you use for SEP communication with ATP. This change in protocol and port is required to take advantage of Endpoint Detection and Response (EDR) 2.0 functionality, such as the endpoint data recorder. EDR 2.0 requires SEP endpoints to communicate with ATP on HTTPS and port 443. When EDR 2.0 is enabled, HTTP port 80 is no longer available for SEP clients to communicate to ATP as their Private Insight Server. The recommended protocol for all SEP communication with ATP (including Insight lookups) is HTTPS port 443. Alternate ports available for Private Insight Server settings are HTTP port 8080 or HTTPS port 8443. Note that using these alternative ports does not enable EDR 2.0.

Immediately upon upgrading to ATP 3.0, EDR 2.0 is disabled, and Private Insight Server settings are not affected. If you are running SEP 14.0 RU1 or later, when you enable EDR 2.0, ATP automatically pushes Private Insight Server settings to the SEPM. ATP also automatically pushes the appropriate ATP built-in SSL certificate (as well as third-party certificates that have already been installed and pushed to the endpoints) to the SEP endpoints running SEP 14.0 RU1 or later. The certificate ensures secure communication with ATP on HTTPS. If your SEPM is not on 14.0 RU1 or later, you must manually modify the Private Insight Server settings in the SEPM console. If you have endpoints that run versions before SEP 14.0 RU1, you must install the ATP certificate on those clients to ensure that they communicate with ATP.
See “Configuring endpoints in Symantec Endpoint Protection Manager to communicate with ATP” on page 42.

See the Symantec™ Advanced Threat Protection 3.0 Upgrade Guide for important information about upgrading ATP.

---

**Note:** EDR 2.0 and the endpoint data recorder functionality are not supported on the 8840 appliance, so the option to enable or disable are not operable.

Only users with the Admin role can enable or disable EDR 2.0 functionality.

**To enable or disable EDR 2.0**

1. In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.

2. Check **Enable EDR 2.0** to enable the option. Uncheck it to disable the option.

See “Configuring the endpoint data recorder” on page 52.

See “About endpoint detection and response (EDR)” on page 15.

---

**Configuring the connection to Symantec Endpoint Protection Manager**

Configure a connection to Symantec Endpoint Protection Manager so that Symantec Advanced Threat Protection (ATP) can communicate with Symantec Endpoint Protection Manager and in some instances, with your endpoints. This connection lets you take advantage of ATP EDR features. If you remove a Symantec Endpoint Protection Manager connection, EDR features are no longer available.

See “About endpoint detection and response (EDR)” on page 15.

**Important:** See the Symantec™ Advanced Threat Protection Upgrade Guide for important information about upgrading to ATP 3.0 and using EDR 2.0 functionality.

**To configure the connection to Symantec Endpoint Protection Manager**

1. In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.

2. If you want to configure a connection to a Symantec Endpoint Protection Manager instance that is part of a replication group, check the option **Replication is enabled between all SEPM's**. Then select the database connection to the Symantec Endpoint Protection Manager database for the replication group.

3. Do one of the following:
### Initially setting up Symantec Endpoint Protection Manager connection using the setup wizard

1. In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.

2. Click **Add server**.

### Modifying an existing Symantec Endpoint Protection Manager connection

1. In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.

2. Hover over the actions menu [three vertical dots] to the far right of the Symantec Endpoint Protection Manager connection that you want to update.

3. Click **SEPM Controller Connection**.
Specify the following information to configure a Symantec Endpoint Protection Manager connection:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entry Name</strong></td>
<td>Type a name that identifies the Symantec Endpoint Protection Manager connection. This field is for display purposes in the global settings list for ATP.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Type the IP address for the Symantec Endpoint Protection Manager server.</td>
</tr>
<tr>
<td><strong>Web Services Port</strong></td>
<td>Type the port number on which the Remote Management and Monitoring (RMM) service of Symantec Endpoint Protection Manager listens. The default port is 8446.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Type the administrator user name of the Symantec Endpoint Protection Manager server. This administrator can have a local Symantec Endpoint Protection Manager account, or a Symantec Endpoint Protection Manager account that you authenticated with a Microsoft Active Directory account. This account must have the appropriate logon permissions. Recommendation: Use a separate system administrator account that you create specifically for ATP access to Symantec Endpoint Protection Manager. Do not use the default administrator account.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Type the password that is associated with the user name to authenticate the user to the Symantec Endpoint Protection Manager server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Type the Symantec Endpoint Protection Manager domain name.</td>
</tr>
</tbody>
</table>
Add SEPM SSL Certificate

Optional

When you add a Symantec Endpoint Protection Manager SSL certificate, ATP checks the certificate every time that it communicates with Symantec Endpoint Protection Manager. The certificate ensures that ATP communicates with the correct server.

Check this option and then click **Browse** to locate and upload a certificate.

To obtain the Symantec Endpoint Protection Manager SSL certificate, go to the Symantec Endpoint Protection Manager administrative interface main page and select the option to download the SSL certificate. You can also download the certificate from the following URL:


**Note:** HTTPS is always used when ATP communicates with Symantec Endpoint Protection Manager. Therefore, communication is always secure.

5 Click **Next** to move to the next page in the wizard or click **Save**.

See “Configuring the endpoint data recorder” on page 52.

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.

Configuring communication with your Symantec Endpoint Protection clients

Configure the URL, protocol, and port that Symantec Endpoint Protection clients use to communicate with ATP on the Symantec Endpoint Protection Communication page. ATP uses private APIs to push the protocol and port configuration settings to the associated Symantec Endpoint Protection Manager along with ATP’s self-signed SSL certificate. ATP administrators can chose to send the configuration to only the top level Symantec Endpoint Protection client group or to all Symantec Endpoint Protection client groups.

When you configure communication with your Symantec Endpoint Protection clients, you can perform the following tasks through ATP:

- EDR 2.0 communication, which includes remediation commands, search commands, and live response events
  
  See “About endpoint detection and response (EDR)” on page 15.

  See “About the endpoint data recorder” on page 45.
Whitelisting and blacklisting by SHA256 hash or MD5 hash
SHA256 blacklist and whitelist are applied to ATP proxy reputation lookups. Only MD5 file hashes are blacklisted on Symantec Endpoint Protection Manager. Whitelisting on Symantec Endpoint Protection Manager through ATP is unsupported. See “About policies” on page 112.

Process Behavior event detection

PE file visibility

ATP database searches
If these communication settings are not configured, file search functionality is unavailable and domain searches are significantly degraded.

Note: These configuration settings apply to all of the clients that Symantec Endpoint Protection Manager manages. Configure these settings if you are installing ATP for the first time. If you performed an upgrade, you may have already configured private cloud settings in your Symantec Endpoint Protection Manager to take advantage of legacy features. If so, you do not need to make any changes on this page (click Next to proceed to the next dialog box). If you have configured private cloud settings on your Symantec Endpoint Protection Manager, making changes on this dialog box overrides those existing settings.

To configure communication with your Symantec Endpoint Protection clients

1. Do one of the following:

   Initially setting up Symantec Endpoint Protection Manager connection using the setup wizard
   Proceed to step 2.

   Modifying an existing Symantec Endpoint Protection Manager connection
   1. In ATP Manager, click Settings > Global and scroll down to Endpoint Detection and Response, Symantec Endpoint Protection Communication, and Endpoint Data Recorder.

   2. Hover over the actions menu [three vertical dots] to the far right of the Symantec Endpoint Protection Manager connection that you want to update.

   3. Click Symantec Endpoint Protection Communication.

2. Check Enable SEP endpoints to communicate with ATP, including performing Insight lookups.
3 Check **Use Symantec public domain look-up servers if ATP is unavailable** if you want ATP to use Symantec public servers if the private server is unavailable.

*Note:* This feature is unsupported for the endpoints that run Symantec Endpoint Protection 12.1.5 or earlier.

4 Check **Apply private cloud policies to all non-default SEPM groups** to ensure that private cloud policies for the top-level Symantec Endpoint Protection Manager group 'My Company' and its inherited groups are always overwritten regardless of whether you select this option.

5 Under the label **ATP Manager**, verify that the pre-populated protocol, URL, and port of the ATP Manager is accurate. If not, make changes as needed.

*Important:* Ensure that the protocol is HTTPS and that the port is configured to 443.

6 Click **Next** if you are in the wizard. Otherwise, click **Save**.

### Configuring the endpoint data recorder

When you configure the endpoint data recorder, you configure the global policies that apply to the all of the groups that this Symantec Endpoint Protection Manager manages. However, the policies do not apply to those groups that you exclude from the policy. As endpoints are added or moved between subgroups, the endpoints inherit the group policy.

See “Configuring Symantec Endpoint Protection endpoint data recorder exclusions” on page 56.

To enable the endpoint data recorder, you must be running Symantec Endpoint Protection 14.0 RU1 and later. An error message appears on the **Symantec Endpoint Protection Endpoint Data Recorder Configuration** page if endpoint data recorder is not supported for your version of Symantec Endpoint Protection Manager.

**To configure the Symantec Endpoint Protection endpoint data recorder**

1 Do one of the following:

   * Initially setting up Symantec Endpoint Protection Manager connection using the setup wizard
Modifying an existing Symantec Endpoint Protection Manager connection

1. In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.

2. Hover over the actions menu [three vertical dots] to the far right of the Symantec Endpoint Protection Manager connection that you want to update.

3. Click **Recorder Configuration**.

2 Check **Enable Endpoint Data Recorder** to enable endpoint data recorder on the clients that this Symantec Endpoint Protection Manager manages.

3. If you enable the endpoint data recorder, specify the maximum amount of disk space (in MB or GB) on the endpoint to store recorded data.

   The minimum size is 250 MB; the maximum is 20 GB. The default value is 1 GB.

4. Do one of the following:

   To send endpoint events to ATP in near real-time (approximately 15 events every 5 minutes)
   Check **Send events in near real time**.

   To limit when to send endpoint events to ATP
   Clients submit data to ATP based on a minimal time interval and maximum batch size.

   1. Check **Send data to ATP every** to configure the maximum frequency (in minutes or hours) that batches of events are sent to ATP.

      The maximum is 24 hours.

   2. Specify the maximum batch size.

      The minimum is 1 event; maximum is 100 events.

      Expect that an average client sends about 2 events per minute. Less than that (fewer than 10 events per 5 minutes) can back up the clients. More than that (greater than 15 events per 5 minutes) increases the load on your server during peak performance. Ensure that your system isn’t already fully loaded if you increase the batch size significantly.
Check the boxes for the types of events that you want submitted to ATP. By default, PowerShell executions are automatically submitted to ATP.

**Tip:** Limiting the events that are submitted to ATP can improve system performance. However, the trade-off is that you run the risk that a potential threat might go undetected.

Click **Next** if you are in the wizard. Otherwise, click **Save**.

See “Configuring Symantec Endpoint Protection endpoint data recorder policy exceptions” on page 54.

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.

See “About the endpoint data recorder” on page 45.

### Configuring Symantec Endpoint Protection endpoint data recorder policy exceptions

When you enable the endpoint data recorder, you create the global policies that apply to all of the groups in your Symantec Endpoint Protection Manager. However, you can create exceptions to those policies and apply them to specific groups. As endpoints are added or moved between subgroups, the endpoints inherit the group policy.

**To configure endpoint data recorder global policy exceptions**

1. Do one of the following:

   - **Initially setting up Symantec Endpoint Protection Manager connection using the setup wizard**
     - Proceed to step 2.
   - **Modifying an existing Symantec Endpoint Protection Manager connection**
     - In ATP Manager, click **Settings > Global** and scroll down to **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder**.
     - Hover over the actions menu [three vertical dots] to the far right of the Symantec Endpoint Protection Manager connection that you want to update.
     - Click **Recorder Exclusion**.

2. Under **SEPM Group Exceptions**, click **Add group exception**.

   **Tip:** If a group is excluded, when you perform an Endpoint search, ATP does not return the recorded events that belong to that group.
3 Specify the following information:

**SEPM Group**
Type the name of the SEPM group for which this exclusion applies.

**Exclude this SEPM Group from recording**
If the endpoint data recorder is enabled in the global policy, check this box to disable this feature for this group.

**Enable endpoint database size**
Specify the maximum amount of disk space (in MB or GB) on the endpoints in this group to store recorded data.

**Send events in near real time**
Check this box to submit endpoint events in this group to ATP in near real time (within 5 minutes).

**Send data to ATP every**¹
If you don't send events to ATP in near real time, specify the frequency (in minutes or hours) in which to send endpoint event data for this group.

- **Maximum batch size**¹
  If you do not send events to ATP in near real time, specify the maximum batch size of event data to send to ATP for this group.

- **Send the following types of events**
  Check the boxes for the types of events that you want submitted to ATP.

1 Data can be submitted to ATP based on a time interval or batch size. If you configure both settings, the first threshold that's met triggers the submission.

For example, assume that you specify the time interval to every 24 hours and the maximum batch size to 10 KB. At about 3 hours into the 24-hour period, the batch size reaches 10 KB. The event data is sent to ATP as soon as the 10-KB threshold is met.

4 Click **Save Exception**.

5 Repeat step 2 through step 4 to add another exception.

6 Click **Save**.

See “Enabling and disabling EDR 2.0” on page 46.

See “Configuring Symantec Endpoint Protection endpoint data recorder exclusions” on page 56.

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.
Configuring Symantec Endpoint Protection endpoint data recorder exclusions

Save disk space and improve event submission performance to ATP by excluding files hashes and files within the specific file paths that you know are safe.

To configure Symantec Endpoint Protection endpoint data recorder group exclusions

1. Do one of the following:

   - Initially setting up Symantec Endpoint Protection Manager connection using the setup wizard
     Proceed to step 2.
   - Modifying an existing Symantec Endpoint Protection Manager connection

2. Under Exclude Hash, click Add hash and description. Type the file hash and description in the dialog box and click Save.

   Repeat this step to add another file hash.

3. Under Exclude File Path, click Add file path and description. Type the file path and a description in the dialog box and click Save.

   Repeat this step to add another file path.

4. Click Next if you are in the wizard. Otherwise, click Save.

   See “Configuring Symantec Endpoint Protection endpoint data recorder policy exceptions” on page 54.

   See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.

   See “About the endpoint data recorder” on page 45.

Securing communication between endpoints and ATP

When you use Symantec Advanced Threat Protection (ATP) as a proxy for network traffic for Symantec Endpoint Protection Manager endpoints, you may want to ensure secure communication using trusted certificates. Each Symantec Endpoint Protection Manager instance
that is capable of secure communication is listed, and you can upload certificates to be used with each server.

Private key files must be password-protected and of PKCS8 (DER) type and certificates must be of X.509 (DER or PEM) type.

---

**Note:** For an example of creating certificates and uploading to ATP Manager, see the following Symantec knowledge base article:

---

To secure communication between endpoints and ATP

1. Copy the certificate(s) and key(s) to a location that you can browse to from ATP Manager.
2. In ATP Manager, click **Settings > Global**.
3. In the **Secure Endpoint Traffic** panel, click **+Add Certificate** to view the list of Symantec Endpoint Protection Manager servers.
4. For each server that you want to use certificates, perform the following:
   - In the **Certificate** field, click **Browse** to upload a certificate.
   - In the **Private Key** field, click **Browse** to upload the private key.
   - Type the password for the key in the **Key Encryption Password** field.
5. Click **Save** when you have completed uploading the certificates.

See “About integrating ATP with Symantec Endpoint Protection” on page 27.

---

### About backing up and restoring ATP data

You can back up the Symantec Advanced Threat Protection (ATP) data from an all-in-one or management platform appliance to a file on the appliance or on a remote computer. (Network scanners do not store data, therefore they do not require backups.) The backup can then be used to restore the events on the same appliance or on a different, but compatible appliance. For example, when you upgrade to a new ATP appliance, you can back up the old model and restore the events to the new model.

As a best practice, you should include backing up ATP as part of your network backup scheme. Another best practice is to back up appliance data before updating an all-in-one or management platform appliance.

You can back up ATP in the following ways:

- Schedule backups in ATP Manager in **Settings > Global**. You specify the backup file location on a remote computer.
Run the CLI `backup` command from the system console. You can specify a backup file location on a remote computer or on the local appliance.

You restore ATP data to an all-in-one appliance or a management platform by running the CLI `restore` command from the system console.

**Note:** Event data can be backed up and restored. However, configuration of the appliance is not restored using the restore command. A backup stores most of the configuration data for the management platform in text form. Symantec strongly recommends that you use the `--encrypt` keyword when using the `backup` command from the command line to secure your configuration data. You can view the text contents of a backup if you want to re-enter configuration data into ATP Manager.

See “Restoring data from a backup file using command-line” on page 152.

ATP saves the backup file with the current date and time in the following format:

```
satp_backup_product_version_yyyymmddHHmss.tar.gz
```

For example, ATP saves a backup on December 5, 2015 at 13:57:52 hours as:

```
satp_backup_2.0.0-1120_20151205135752.tar.gz
```

The product version consists of the major, minor, revision, and build numbers. The hour follows the 24-hour format.

You can rename the backup file without affecting the restore process. Do not attempt to edit the backup file.

When you perform a backup, ATP logs an event in the System Activity Log that lists the start and end time of the backup, its success or failure, the files it backed up, etc.

See “Enabling backup for a management platform or all-in-one appliance” on page 58.

See “backup command” on page 144.

See “Restoring data from a backup file using command-line” on page 152.

### Enabling backup for a management platform or all-in-one appliance

You should backup data on each management platform or all-in-one Symantec Advanced Threat Protection (ATP) appliance periodically in case of a critical problem with the software or hardware. Network scanner appliances do not store data, therefore they do not require backup.

Once a backup is scheduled, you can view the status and next run time of the backup in ATP Manager. The status of a backup can be scheduled (for future scheduled backups), running (for currently executing backups), successful (for successfully completed backups), or error (for backups that did not complete properly).
If a backup does not complete, check the debug logs on the appliance for further information on why the backup failed (for example, if the remote server was down and the logon failed).

**To enable backup for a management platform or all-in-one appliance**

1. In ATP Manager, click **Settings > Global**.

2. In the **Backup** panel, click **+Configure Backup** to configure a backup.

3. In the **Backup** dialog, check the box in the **Enable** field to enable the backup configuration. You can later disable the backup to prevent it from executing by unchecking this box.

4. In the **Method** field, select **FTP** or **Secure Copy (SCP)** to choose the file transfer method that the remote server on which you are sending the backup file supports.

5. In the **Schedule Type** field, choose one of the following:

   - **Interval**: Backs up the file more than once per day. After selecting this schedule type, enter the value (1 to 23) in the **Interval (Hours)** field to specify the number of hours between backups.

   - **Daily**: Backs up the file once per day. After selecting this schedule type, choose a **Start Time** from the menu.

   - **Weekly**: Backs up the file once per week. Also select the day of the week when you want the backup to occur. Then choose a **Start Time**.

   - **Monthly**: Backs up the file one or more days per month. After selecting this schedule type, type the day of the month when you want the backup to occur in the **Days of Month** field. To enter multiple days, type the days separated by commas (you can enter one or more days between day 1 and 28 for a backup). Then choose a **Start Time** from the menu.

   The time that is specified for the backups uses the current local time of the browser when the backup is configured. This time is converted to UTC time on the management platform so that the backup is performed at the correct corresponding time on the management server.

6. In the **Host** field, type the IP address or fully qualified domain name of the server where backups are sent.

7. In the **Path** field, type a path to the location of the folder or directory on the Host where backups are saved.

8. In the **Login** field and **Password** field², type the FTP or SCP logon credentials.

9. At the bottom of the page, click **Save**.
To perform a backup using the CLI

◆ On the management platform or all-in-one appliance, run the `backup` command with desired options. The backup is performed immediately, there is no scheduling when you use the command line.

For example, to backup data to a directory on a remote server using FTP, type:

```
backup --host=(IP address)¹ --protocol=ftp --port=(port number)
--user=(username)¹ --password=(password)² --path=<directory>¹
```

Click the following link for more information on the command options of the backup command.

See “backup command” on page 144.

¹ The Host, Path, Login fields do not support whitespace, non US-ASCII printable characters, or any of the following characters:

!%$&\'|*(){}[]<>;:'"

² The Password field does not support whitespace and non US-ASCII printable characters. It also does not support special characters, such as tilde, ligature, and umlaut. Examples of unsupported special characters are as follows:

Á Ñ È Ç È Æ

See “About backing up and restoring ATP data” on page 57.

See “restore command” on page 149.

---

### About licenses

Symantec Advanced Threat Protection (ATP) consists of the following control points: network, endpoint, and email. Your organization can purchase one, all, or any combination of these control points that meet your needs. Install the control points that your organization purchased to have access to that functionality. For more information about licensing or purchasing additional control points, see your Symantec sales representative.

When your organization purchased ATP, Symantec sent your organization an email with the license file attached in .slf format. Click **Browse** to locate and upload this license file. Each standalone appliance and CIU requires a license. A CIU distributes the license to each of the scanners it manages. You must install a valid license to proceed with installation.

**Note:** Only license files with the .slf extension are supported.

**Note:** Symantec Advanced Threat Protection: Network 1.0 licenses are not supported.

You can view the license status on the **Settings > Global Settings** page in ATP Manager.
See “Viewing the license status and updating a license” on page 61.

Viewing the license status and updating a license

You can monitor the status of your Symantec Advanced Threat Protection (ATP) license and upload new licenses in ATP Manager. When multiple licenses are installed, the license with the latest expiration date is the one that applied and that date appears (in UTC).

When a license expires, there is a 60-day grace period in which to upload a new license. During the grace period, all product functionality remains intact. After the grace period expires, packet scanning no longer occurs and Synapse correlation is discontinued. You are also unable to submit files to Cynic. However, you still have access to ATP Manager and all of your data.

Note: ATP does not monitor the license status of other products, including Symantec products that may provide data to Synapse for correlation.

See “About Synapse correlation” on page 24.

To view the license status

◆ In ATP Manager, click **Settings > Global** and scroll down to **Licensing**.
  
The license status appears.

To update a license

1 Save the license file to a location that is accessible from the computer where you are running ATP Manager.

2 In ATP Manager, click **Settings > Global**.

3 Scroll down to **Licensing**, and click **Upload License**.

4 In the **Upload License** dialog box, browse to and select the license file, and then click **Upload**.
  
The new license takes effect immediately, although it must be distributed to each of the scanners. If the previous license had expired, make sure that you enable scanning again on all scanner devices.

  See “Configuring network interface settings and enabling scanning” on page 74.

See “About licenses” on page 60.
Viewing certificates

Symantec Advanced Threat Protection (ATP) uses digital certificates to secure communication with your Symantec Endpoint Protection Manager web servers, and your Splunk server. It also uses a certificate to encrypt all ATP Manager sessions.

ATP monitors the status of each certificate, and provides both system health warnings and email notifications when those certificates approach or pass their expiration dates.

See “ATP actions against expiring certificates” on page 63.

As an administrator, you can navigate to the **Settings** pane in ATP Manager where each certificate is installed to view its status, name, issuing authority, recipient, and expiration date. From there, you can install a new certificate, if necessary.

---

**Note:** The SSL and Secure Endpoint Traffic panes display both the certificate's status and its additional information. The SEPM Controller Connection and Splunk panes display only the certificate's status. For these, you can hover over the status to display its additional information.

If there is no certificate installed, the Status is listed as None.

---

**To view certificate information for your SEPM Controller Connection**

1. In ATP Manager, click **Settings > Global Settings**.
   - In the **Endpoint Detection and Response, SEP Communication, and Endpoint Data Recorder** pane, the status appears in the **Certificate** column.

2. Hover over the status to view additional certificate information.

**To view SSL certificate information**

- In ATP Manager, click **Settings > Global Settings**.
  - In the **SSL Certificate** pane, the certificate information appears.

**To view certificate information for your Splunk server**

1. In ATP Manager, click **Settings > Data Sharing**.
   - In the **Splunk Event Forwarding** pane, the status appears in the **Certificate** column.

2. Hover over the status to view additional certificate information.

See “About configuring the connection to Symantec Endpoint Protection Manager” on page 39.

See “Securing communication between endpoints and ATP” on page 56.

See “Configuring secure access to ATP Manager” on page 18.
ATP actions against expiring certificates

Table 3-7 explains the actions that ATP takes when a certificate is within a certain number of days from its expiration date. When you install a new certificate, ATP immediately clears any system health warnings, stops sending email notifications, and updates the certificate's status.

Table 3-7 ATP actions against expiring certificates

<table>
<thead>
<tr>
<th>Days from expiration</th>
<th>System Health warning</th>
<th>Email notification</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than 60</td>
<td>System Is Healthy</td>
<td>None</td>
<td>Valid</td>
</tr>
<tr>
<td>60 and 30</td>
<td>System Needs Attention: Certificate is expiring in &quot;n&quot; day&lt;br&gt; This warning is generated only on the 60th and 30th day.</td>
<td>Sent to all administrators on the 60th and 30th day.</td>
<td>Expiring in &quot;n&quot; days</td>
</tr>
<tr>
<td>30-8</td>
<td>System Needs Attention: Certificate is expiring in &quot;n&quot; day</td>
<td>Sent to all administrators once a week during this period.</td>
<td>Expiring in &quot;n&quot; days</td>
</tr>
<tr>
<td>7-1</td>
<td>System Is Critical: Certificate is expiring in &quot;n&quot; days</td>
<td>Sent to all administrators every day during this period.</td>
<td>Expiring in &quot;n&quot; days</td>
</tr>
<tr>
<td>Day of expiration</td>
<td>System Is Critical: Certificate is expiring today</td>
<td>Sent to all administrators on this day.</td>
<td>Expiring today</td>
</tr>
<tr>
<td>Less than 1</td>
<td>System Is Critical: Certificate expired</td>
<td>Sent to all administrators every day during this duration.</td>
<td>Expired</td>
</tr>
</tbody>
</table>

See “Viewing certificates” on page 62.

Configuring the connection to an SMTP-compatible mail server

For Symantec Advanced Threat Protection (ATP) to email notifications, you must configure the connection to a mail server. ATP is compatible with any mail server that supports Simple Mail Transport Protocol (SMTP).

If your mail server requires authentication to send messages, you must set up an account for the appliance on your mail server.
To configure the connection to an SMTP-compatible mail server

1. In ATP Manager, click Settings > Global.
2. In the SMTP Server panel, click Edit SMTP Server.
3. In the SMTP Server field, type the name of your mail server.
4. In the Port field, type the port that your mail server uses.
5. In the Appliance email field, type the email address where alerts are sent from.
6. If your mail server requires authentication to send messages, check Authentication Required and then type the User name and Password assigned to the ATP appliance.
7. Click Save.

See “Adding local user accounts” on page 101.

Customizing and testing blocking pages

Blocking pages are used only when you operate in Inline Block mode and scanning is turned on. When Symantec Advanced Threat Protection (ATP) blocks access to a website or prevents the download of a potentially malicious file, a blocking page displays in the browser to inform the user.

Blocking pages have the following messages, which cannot be modified:

- For a site that is blocked by the Symantec blacklist: "The site you are attempting to visit has been blocked. Click here for more information."
- For a site that is blocked by a Blacklist policy: "The site you are attempting to visit has been blocked by your administrator. Click here for more information."
- For a blocked file that is blocked by a Blacklist policy: "The file you are attempting to access has been blocked. Click here for more information."

If you do not customize the blocking page, the user sees the Symantec logo at the top of the page. Also, each message has a URL link in the text "Click Here". The URL points to:


To customize the blocking page, you can replace the Symantec logo with a custom image. You can also replace the URL with a different one, which the user can click to get more information (such as a statement of your company policies). Both the image and the URL are required to customize the blocking page.

To customize blocking pages

1. In ATP Manager, click Settings > Global.
2. In the Blocking Page area, click Edit Blocking Page.
To replace the Symantec logo with a custom image, click **Browse** next to the **Logo Image** field, locate the image, and then click **Open**.

The file size of the image must be less than 900 KB, and the recommended image size is 300 pixels wide by 79 pixels high. Only .jpg format images are supported.

To replace **www.symantec.com** with a custom URL, type the URL in the **More Info URL** field.

Symantec recommends that you type the URL of a local resource that explains your organization's Internet policies. ATP performs some validation, but you must independently verify that the page does not link to a malicious site.

Click **Save**.

**Note:** Once customized settings are saved, they are no longer viewable in the **Blocking Page Settings** dialog. Revisiting that dialog does not show your current customization options. You can click the **View Blocking Page** option to see a sample of the currently defined blocking page (scanning must be enabled and your device must be in an Inline mode). If you want to change the customizations, you must upload a new image and specify a new URL for more information.

**Note:** If you are operating in Inline Monitor or Inline Block mode, you must configure your gateway to be on the LAN side of ATP for blocking pages to appear on your endpoints.

See “**Configuring network interface settings and enabling scanning**” on page 74.

**To test the appearance of custom blocking pages**

The appliance must operate in Inline Block or Inline Monitor mode and scanning must be turned on to test blocking pages.

1. Open a browser on a protected endpoint.

2. Type the following web addresses to test different messages:
   - For a site that is blocked by the Symantec blacklist:
     http://<IP address of inline LAN/WAN pair>:8080/BlockSite.html
   - For a site that is blocked by an ATP Blacklist:
     http://<IP address of inline LAN/WAN pair>:8080/BlockSiteAdmin.html
   - For a blocked file that is blocked by an ATP Blacklist:
     http://<IP address of inline LAN/WAN pair>:8080/BlockFile.html

See “**Completing setup tasks**” on page 19.
How ATP purges data from the ATP database

Symantec Advanced Threat Protection (ATP) regularly monitors the amount of data that you have in your internal databases to ensure that it does not grow uncontrollably and consume too much disk storage space. When your database reaches a certain threshold, ATP automatically purges it.

ATP automatically performs 2 types of database purges based on the following:

- **Retention period**
  ATP performs a daily purge of your databases on data that is over 6 months old, regardless of whether your storage space threshold is exceeded.

- **Storage space usage**
  ATP performs a check every 15 minutes on the size of your databases to ensure that your data does not exceed 85 percent of your storage space. If your data exceeds this threshold, ATP purges roughly 10 percent of your data beginning with the oldest records.
  If your data exceeds the threshold, ATP logs a system activity event when this type of purge occurs. This event lists the types of database records that were deleted.

ATP only performs one type of purge at a time. ATP also only purges one type of data at a time until the storage space threshold is met. Database records are purged in the following order:

- **RRS (Reputation Request Score) events**
  ATP only retains RRS events for 30 days, regardless of whether your storage space threshold is exceeded.

- **Endpoint Data Recorder dumps**
  ATP only retains your 5 most recently completed Endpoint Data Recorder dumps

- **Completed, terminated, and in-progress commands (for example, saved searches and their results, or searches that are currently running)**
  ATP only retains your most recent 1000 commands, regardless of their age or whether your storage space threshold is exceeded. These include your most recent 900 non-search commands (for example, when you delete a file or quarantine an endpoint), and your most recent 100 search commands (for example, when you search for a suspicious file).

- **Security events, incidents, and system activity events**

- **Entity tracking events**

See “About backing up and restoring ATP data” on page 57.
Configuring default and appliance settings

This chapter includes the following topics:

- About default and appliance settings
- Appliances
- Deleting a scanner from your configuration
- Rebooting and shutting down appliances
- Configuring network interface settings and enabling scanning
- About configuring ATP with a virtual LAN (VLAN)
- Defining internal networks to ATP
- Configuring network proxy information
- Building an enterprise proxy list
- Specifying the traffic that the proxy inspects
- Configuring connections to DNS servers
- Configuring the connection to a time server
- About syslog server connections
- Configuring connections to syslog servers
- About configuring a connection to an SNMP manager or trap receiver
- Configuring ATP to use cloud sandboxing or on-premises sandboxing
About default and appliance settings

In a Symantec Advanced Threat Protection (ATP) management platform-network scanner configuration, default settings provide a way to configure groups of settings that can quickly be applied to the network platform and network scanners. Each appliance can accept the default setting or choose to have its own setting for configuration items.

Default settings

- Lets you configure settings that apply to all of your appliances.

To access default settings

1. In ATP Manager, click Settings > Appliance.
2. Click the Edit Default Appliance Settings icon.

Appliance settings

- Lets you configure settings that apply to a specific appliance. Appliance settings override Default settings. Also lets you delete an appliance that has the role of Scanner.

To access appliance settings

1. In ATP Manager, click Settings > Appliance.
2. Click on the appliance that you want to configure in the Appliances list.

See “Appliances” on page 69.

See “Deleting a scanner from your configuration” on page 72.

Table 4-1 lists the configuration options that you can set as default for all appliances or individually customize for each appliance.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default settings</th>
<th>Appliance settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network Configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Defining internal networks to ATP” on page 77.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Proxy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring network proxy information” on page 79.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Proxy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Building an enterprise proxy list” on page 80.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-1  Configuration options on ATP appliances (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default settings</th>
<th>Appliance settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Relationship</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Specifying the traffic that the proxy inspects” on page 81.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring connections to DNS servers” on page 82.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring the connection to a time server” on page 83.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring connections to syslog servers” on page 88.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring a connection to an SNMP v3 manager or trap receiver” on page 91.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sandboxing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>See “Configuring ATP to use cloud sandboxing or on-premises sandboxing” on page 93.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See “Rebooting and shutting down appliances” on page 73.

### Appliances

The **Appliances** page in the ATP Manager provides you with detailed information about the appliance. The graphic that appears under the appliance name indicates the health of the appliance.

**Table 4-2** provides information about the details that appear beside the appliance health graphic.
Table 4-2  Appliance details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| EVENT STORAGE USAGE    | The amount of disk storage space that your appliance has allocated to store events. You can hover over the bar to display the actual amount of used space. The color of the bar indicates the state of the actual usage based on the following:  
  ■ Green  
  Actual usage is below 70 percent.  
  ■ Orange  
  Actual usage is between 70 and 85 percent.  
  ■ Red  
  Actual usage is about 85 percent.  
When the amount of storage space exceeds one of these thresholds, ATP logs a notification in the System Activity log. |
| APPLIANCE ID           | ATP automatically generates this number when you install the physical appliance or virtual appliance.                                                                                                                                                                                                                                     |
| SERIAL NUMBER          |  
  ■ Physical appliance  
  The serial number of the physical appliance.  
  ■ Virtual appliance  
  The appliance ID preceded by "VMware-".  
ATP automatically populates this field when you install the physical appliance or virtual appliance.                                                                                                                                                                  |
| APPLIANCE TYPE         |  
  ■ Physical appliance  
  The model of the hardware appliance (i.e., 8880 or 8840).  
  ■ Virtual appliance  
  VMware Virtual Platform  
ATP automatically populates this field when you install the physical appliance or virtual appliance.                                                                                                                                                                                                                  |
| Product                |                                                                                                                                                                                                                                                                                                                                              |
| ATP                    | The version of ATP that the appliance is running.                                                                                                                                                                                                                                                                                          |
| AV ENGINE              | The antivirus definition ID that the appliance is using.                                                                                                                                                                                                                                                                                   |
| VANTAGE                | The Vantage definition ID that the appliance is using.                                                                                                                                                                                                                                                                                     |
| INSIGHT                | The Insight definition ID that the appliance is using.                                                                                                                                                                                                                                                                                      |
### Table 4-2 Appliance details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEEPSIGHT INTELLIGENCE</td>
<td>The DeepSight Intelligence definition ID that the appliance is using.</td>
</tr>
<tr>
<td>LAST UPDATE</td>
<td>The date and time (in UTC) that the most recent content updated (e.g., definition IDs) regardless of the outcome (successful or unsuccessful). Update errors are reported in the system health.</td>
</tr>
<tr>
<td>DYNAMIC ADVERSARY INTELLIGENCE</td>
<td>The Dynamic Adversary Intelligence definition ID that the appliance is using.</td>
</tr>
<tr>
<td>Scanning</td>
<td></td>
</tr>
<tr>
<td>SCANNING</td>
<td>Whether the scanner is enabled or disabled.</td>
</tr>
<tr>
<td>MODE</td>
<td>The operating mode that is assigned to the appliance.</td>
</tr>
<tr>
<td></td>
<td>See the Symantec™ Advanced Threat Protection Installation Guide for more information about operating modes.</td>
</tr>
<tr>
<td>MANAGEMENT IP</td>
<td>The IP address of the management platform (i.e., ATP Manager).</td>
</tr>
</tbody>
</table>

The Action bar contains options that let you shut off the appliance or restart it.

See “Rebooting and shutting down appliances” on page 73.

Beneath the Action bar are options that you can configure that apply specifically for this appliance.

- **Network Interface Settings**
  
  See “Configuring network interface settings and enabling scanning” on page 74.

- **Internal Network Configuration**
  
  See “Defining internal networks to ATP” on page 77.

- **Network Proxy**
  
  See “Configuring network proxy information” on page 79.

- **Enterprise Proxy**
  
  See “Building an enterprise proxy list” on page 80.

- **Proxy Relationship**
  
  See “Specifying the traffic that the proxy inspects” on page 81.

- **DNS Settings**
  
  See “Configuring connections to DNS servers” on page 82.

- **Time Server**
  
  See “Configuring the connection to a time server” on page 83.
Deleting a scanner from your configuration

As an administrator, you can delete a physical or virtual network scanner from Symantec Advanced Threat Protection (ATP) as long as that scanner is not part of an all-on-one appliance. When you delete a scanner, it is removed from the Appliances list in ATP Manager; however, none of the events (or other data) associated with that scanner are deleted. This deletion also prevents the management platform from displaying a System Health error message when the network scanner fails to report its status.

Before you delete a scanner, you must first shut it down. Failure to do so may result in that scanner re-appearing on the Appliances list after you delete it.

You can re-add the scanner (for example, to another management platform) by re-imaging the physical appliance or re-installing the virtual appliance.

To delete a network scanner

1. In ATP Manager, select Settings > Appliances.
2. From the Appliances list, click the Shutdown Appliance icon for the scanner you want to delete.
   
   Wait a few minutes to ensure that the appliance is completely shut down.

3. Click the Delete Appliance icon for the scanner that you want to delete.

   **Note:** The Delete Appliance icon only appears for appliances that have the role of Scanner.

4. On the Warning dialog box, click OK.

See “Adding a scanner in your configuration” on page 136.

See “Re-imaging a physical appliance” on page 136.

See “Reinstalling a virtual appliance” on page 137.
Rebooting and shutting down appliances

Shutting down an appliance

You may want to manually shut down an appliance to re-image it, physically move it, or delete the appliance from ATP Manager. When you manually shut down an appliance, the appliance turns off. Scanning stops, and Symantec Advanced Threat Protection (ATP) is no longer able to detect potential threats.

See the *Symantec™ Advanced Threat Protection Installation Guide* for more information about how to restart the appliance.

Rebooting an appliance

When you manually reboot or restart the appliance, the appliance turns off and then restarts itself. As the appliance is turning off and restarting, no scanning occurs and ATP cannot detect potential threats. After the appliance has restarted, all of the configurations that existed before the reboot are retained. Scanning recommences if a scanner was configured and enabled before the reboot.

**Warning:** Software updates require ATP to be taken offline. Never reboot or shutdown the appliance during an update. The appliance reboots itself after the update.

To reboot or shut down an appliance from the Default Appliance page

1. In ATP Manager, click **Settings > Appliances**.
2. In the **Appliances** list for the appliance you want to reboot or restart, select the appropriate option in the far right column.

To reboot or shut down an appliance from the Appliance page

1. In ATP Manager, click **Settings > Appliances**, and then click on the appliance in the **Appliances** list.
   
   **Tip:** Hover over the appliance and click when the mouse pointer changes to a finger icon.
2. In the Action bar, select the option to either reboot the appliance or restart it.

See “About default and appliance settings” on page 68.

See “Appliances” on page 69.

See “Re-imaging a physical appliance” on page 136.

See “Reinstalling a virtual appliance” on page 137.
Configuring network interface settings and enabling scanning

Perform the following operations on the Network Interface Settings area of the Appliances settings page:

- Enable or disable Symantec Advanced Threat Protection (ATP) scanning for all-in-one or network scanner appliances (management platform devices do not scan).
- Set the operating mode to tap, inline monitor, or inline block.
- Specify the network port settings when operating in inline monitor or inline block mode. See “About configuring ATP with a virtual LAN (VLAN)” on page 77.

Your organization may have data privacy and residency requirements that restrict you from sending files outside of the region. ATP provides an option that ensures that your files are submitted to a data center in the United Kingdom for sandbox analysis. Symantec recommends that you enable this option before you enable network scanning to ensure that no files are improperly routed.

The Edit Interface option lets you change the operating mode and network specification. Before you can edit the network interface settings, you must turn scanning off.

**Note:** Configuring inline mode (either initially or when switching from tap to inline) can result in a brief network disruption. During initial configuration of a device in inline mode, network traffic is blocked until scanning is turned on. If you switch an existing device from tap mode to inline mode, network traffic is disrupted once the physical or virtual configuration changes to the device are made (that is, re-cabling or changing the virtual switches). Network traffic resumes once scanning has been turned on in ATP Manager. If you plan to enable inline mode, you may need to plan a scheduled network interruption for your system.

To turn scanning on or off

1. In ATP Manager, click Settings > Appliances, and then select the all-in-one device or network scanner from the list.
2. In the Network Interface Settings panel, click the toggle switch in the Scanning field. Scanning is switched to the opposite of its previous status.
3. In the Confirmation dialog box, click OK.

If you operate in one of the inline modes, a warning message may appear. The warning indicates there is a brief network disruption when scanning is turned on or off. If you turn scanning off when operating in tap mode, the warning asks if you are sure that you want to proceed.
To change the operating mode

1. In ATP Manager, click Settings > Appliances, and then select the all-in-one or network scanner from the list.

2. If scanning is on, disable scanning.
   
   See “To turn scanning on or off” on page 74.

3. Click the Edit Interface option.

4. Select the desired operating mode from the choices in the Scan Mode field.

5. For inline monitor and inline block modes, configure the network interface settings. For tap mode, no network information is required.

   See “To configure the network settings for inline monitor or inline block mode” on page 75.

6. Click Save.

7. Make certain the cables on your physical appliance or the virtual switches on your virtual appliance are configured properly for the mode you want to choose.

   See Symantec Advanced Threat Protection Installation Guide for information on properly configuring your physical and virtual appliances.

8. Turn on scanning after completing the configuration.

   See “To turn scanning on or off” on page 74.

To configure the network settings for inline monitor or inline block mode

1. In ATP Manager, click Settings > Appliances, and then select the all-in-one or network scanner from the list.

2. If scanning is on, disable scanning.

   See “To turn scanning on or off” on page 74.

3. Click the Edit Interface option.
4 Specify the network interface information. You must specify the IPV4 network settings, but if you have IPV6 addresses, you can specify the configuration in the IPV6 fields.

<table>
<thead>
<tr>
<th>IPV4 Fields</th>
<th>IPV6 Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPV4 Address</strong></td>
<td><strong>IPV6 Address</strong></td>
</tr>
<tr>
<td>The address of the WAN interface in IPV4 format.</td>
<td>The address of the WAN interface in IPV4 format.</td>
</tr>
<tr>
<td>For VLAN trunking deployments, use the address of the Native VLAN subnet.</td>
<td>For VLAN trunking deployments, use the address of the Native VLAN subnet.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td><strong>Prefix Length</strong></td>
</tr>
<tr>
<td>The subnet mask of the WAN interface.</td>
<td>The prefix length of the IPV6 address for the WAN interface.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td><strong>Gateway</strong></td>
</tr>
<tr>
<td>The address of the router or switch that corresponds to the WAN interface IPV4 address.</td>
<td>The address of the router or switch that corresponds to the WAN interface IPV6 address.</td>
</tr>
<tr>
<td>For VLAN trunking deployments, use the address of the VLAN router (or firewall).</td>
<td>For VLAN trunking deployments, use the address of the VLAN router (or firewall).</td>
</tr>
</tbody>
</table>

**Note:** If you type data in any of the IPV6 fields, all IPV6 fields become required. If you mistakenly type data into the IPV6 fields, clear all IPV6 fields of any data and the IPV6 fields become optional again.

5 If you have a device with more than one inline interface, you can optionally click **+ Add Inline 2** to configure the second interface. Specify the information as described in Step 4 for the second inline interface. If your device does not have a second inline interface, this option does not appear.

If you have a device with more than one inline interface, you can optionally click **+ Add Inline 2** to configure the second interface. Specify the information as described in Step 4 for the second inline interface. If your device does not have a second inline interface, this option does not appear.

You can also remove a previously specified second inline interface by clicking **- Remove Inline 2**.

6 Click **Save**.

**Note:** The **Save** option is only enabled if all required fields are properly completed. If there is an error in the data of any field, you must fix the error before saving the configuration.
About configuring ATP with a virtual LAN (VLAN)

If you use a virtual LAN (VLAN), you can configure your Symantec Advanced Threat Protection (ATP) appliance to inspect the network traffic that includes VLAN tags.

To configure your appliance in an environment that uses VLAN trunking, you must position your appliance between your VLAN router (or firewall) and your VLAN subnets.

When configuring your scanner for inline monitor or inline block mode, you must configure your network interface settings so that the Gateway points to your VLAN router (or firewall), and the IP address points to the subnet that is associated with your native VLAN. (You must have a VLAN subnet to implement this solution.)

See “Configuring network interface settings and enabling scanning” on page 74.

To test this configuration, make sure that you can ping your ATP appliance from with the VLAN subnets.

Note: The VLAN ID of the VLAN that detects an event appears on the Event Details page. If you have stacked VLANs, only the outer VLAN ID appears.

Defining internal networks to ATP

Define your internal networks to specify which computers are part of your network. Any traffic that originates from somewhere other than these internal networks is considered “outside the network.” With this information, Symantec Advanced Threat Protection (ATP) can determine the difference between the malware infections that affect internal computers and the attacks that originate from outside the network.
To define the default internal network

1. In ATP Manager, click **Settings > Appliances**, and then click **Edit Default Appliance**.
2. In the **Internal Network Configuration** panel, click **+Add Internal Network**.
3. In the **Subnet** field, type the IP address of your internal subnet.
   
   For example, if your internal computers are in the range 10.42.24.0 to 10.42.24.255, type 10.42.24.0.
4. In the **Netmask** field, type the netmask for the subnet.
   
   For example, if your internal computers are in the range 10.42.24.0 to 10.42.24.255, type 255.255.255.0.

   ATP supports the wide subnets that are also known as supernets. If portions of your network are in a contiguous wide range, it is not necessary to list separate internal network entries for each range. A single wide range is sufficient.
   
   For example, if you have a list of internal subnets as follows:
   
   - 10.42.1.0/255.255.255.0
   - 10.42.2.0/255.255.255.0
   - ...
   - 10.42.20.0/255.255.255.0
   - 10.42.30.0/255.255.255.0

   You can combine the subnets into one internal network of 10.42.0.0/255.255.0.0.
5. Optionally, in the **Description** field, type a description of the internal network.
6. If your internal network has computers in separate network ranges, specify additional networks.
7. Click **Save**.

To define a custom internal network configuration for an individual device

1. In ATP Manager, click **Settings > Appliances**, and then select the appliance name in the **Appliances** list.
2. In the **Internal Network Configuration** panel, uncheck **Use Default** if it is checked.
3. Follow steps 2 through 7 of the previous procedure.
To apply the default internal network configuration to a device

1. In ATP Manager, click **Settings > Appliances**, then select the appliance name in the **Appliances** list.

2. In the **Internal Network Configuration** panel, check **Use Default**.

---

**Note:** **Use Default** is not available until you configure the default internal network configuration.

See “Completing setup tasks” on page 19.

---

### Configuring network proxy information

The Symantec Advanced Threat Protection (ATP) appliance uses the network proxy during communications outside of the network, such as when the appliance downloads virus definitions from LiveUpdate or contacts Synapse for analyses.

You can configure access to a network proxy that requires Basic Access Authentication (BA) or no authentication at all.

---

**Note:** There are some required domains and URLs that ATP must be able to access. Your proxy server must be configured to allow access to the same required domains that your firewall must be able to access. See *Symantec Advanced Threat Protection Installation Guide* for more information about required domains for your firewall server.

---

To configure the default network proxy

1. In ATP Manager, click **Settings > Appliances**.

2. Click **Edit Default Appliance**.

3. In the **Network Proxy** panel, check **Use Network Proxy**, and then click **+Edit Proxy**.

4. On the **Edit Network Proxy Configuration** dialog box, in the **IP Address** field, type the IP address of the network proxy.

5. In the **Port Number** field, type the port number that the network proxy uses.

6. If the network proxy requires authentication, enter the credentials in the **User Name** and **Password** fields.
   
   Leave these fields blank if the proxy doesn’t require authentication.

7. Click **Save**.
To apply the default network proxy settings to a device
1. In ATP Manager, click **Settings > Appliances**, and click the device in the **Appliances** list.
2. In the **Network Proxy** panel, check **Use Default**.

**Note:** **Use Default** is not available until you enable and configure a default network proxy.

To configure a custom network proxy connection for a single device
1. In ATP Manager, click **Settings > Appliances**, and then click the device in the **Appliances** list.
2. In the **Network Proxy** panel, uncheck **Use Default** if it is checked.
3. Check **Use Network Proxy**, then click **+Edit Proxy**.
4. In the **IP Address** field, type the IP address of the network proxy that you want this device to use.
5. In the **Port Number** field, type the port number that the network proxy uses.
6. If the network proxy requires authentication, type the credentials in the **User Name** and **Password** fields.
   Leave these fields blank if the proxy doesn’t require authentication.
7. Click **Save**.

See “Building an enterprise proxy list” on page 80.

See “Required firewall ports” on page 156.

### Building an enterprise proxy list

Symantec Advanced Threat Protection (ATP) does not normally inspect traffic between internal computers. A proxy server usually has an IP address in the internal range, so if the proxy sits between ATP and the Internet, all traffic between protected endpoints and the Internet appears as internal traffic. When you add the proxy server IP address to the **Enterprise Proxy** list, however, ATP treats all traffic to the proxy as outbound network traffic and inspects it.

Configure an enterprise proxy only if ATP is on the LAN side of the proxy. Otherwise, the appliance does not inspect traffic between the proxy and the Internet. If you use a single-leg proxy, Symantec recommends that you configure the ATP enterprise proxy so that it only inspects traffic between the proxy and the internal networks.
To build the default enterprise proxy list

1. In ATP Manager, click **Settings > Appliances**, and then click the **Edit Default Appliance** icon.

2. In the **Enterprise Proxy** panel, click **+Add Enterprise Proxy**.

3. In the **Add Enterprise Proxy** dialog box, in the **IP Address** field, enter the IP address of the enterprise proxy server.

4. Click **Save**.

5. Repeat steps 2 to 4 for each additional enterprise proxy in your network.

To apply the default enterprise proxy settings to a device

1. In ATP Manager, click **Settings > Appliances**, then click the appliance name in the **Appliances** list.

2. In the **Enterprise Proxy** panel, check **Use Default**.

**Note:** **Use Default** is not available until you configure the default enterprise proxy.

---

To build a custom enterprise proxy connection for a single device

1. In ATP Manager, click **Settings > Appliances**, then click the appliance name in the **Appliances** list.

2. In the **Enterprise Proxy** panel, uncheck **Use Default**, if it is checked.

3. Click **+Add Enterprise Proxy**.

4. In the **Add Enterprise Proxy** dialog box, in the **IP Address** field, enter the IP address of the enterprise proxy server.

5. Click **Save**.

6. Repeat steps 2 to 5 for each additional enterprise proxy in the network that is scanned by this device.

See “**Configuring network proxy information**” on page 79.

### Specifying the traffic that the proxy inspects

By default, Symantec Advanced Threat Protection (ATP) inspects the network traffic that flows from your monitored endpoints to your enterprise proxy. As such, a conviction event reports the endpoint IP as the local IP and the proxy IP as a remote IP.

However, you can configure ATP so that the scanner processes the data stream between the enterprise proxy and the Internet. When ATP scans traffic between the enterprise proxy and the Internet, ATP can include original TCP source address information from the Internet traffic.
X-Forwarded-For: header field. This lets ATP still report conviction events with the endpoint IP instead of the Internet IP. However, external IP addresses are not detectable, so geolocations may not be discoverable. Symantec recommends that you scan the traffic from the enterprise proxy and the Internet because it lets ATP identify which internal computers are associated with traffic.

**Note:** ATP cannot scan the traffic that the proxy caches. So it may not see all targeted computers.

**To specify the traffic that the proxy inspects**

1. In ATP Manager, click **Settings > Appliances**.
2. Do any of the following:
   - To modify the default appliance
     1. On the Action bar, click **Edit Default Appliance**.
     2. Scroll down the page to **Proxy Relationship**.
     3. Click **Edit Deployment Location**.
     4. The scanner inspects traffic between:
        - monitored endpoints and the enterprise proxy
        - the enterprise proxy and the Internet
        This setting is the default option.
     5. Click **Save Deployment Location**.
   - To modify an appliance
     1. In the **Appliances** list, click on an appliance to modify its settings.
     2. Scroll down the page to **Proxy Relationship**.
     3. Do one of the following:
        - To change the default setting, uncheck **Use default**, click **Edit Deployment Location**, and select the enterprise proxy and the Internet, and click **Save Deployment Location**.

See “Building an enterprise proxy list” on page 80.
See “Configuring network proxy information” on page 79.

## Configuring connections to DNS servers

A Domain Name Server (DNS) is primarily needed to access Internet resources by name (for example, liveupdate.symantec.com). If you provide the fully qualified domain name for SMTP or NTP servers, DNS must be enabled before the Symantec Advanced Threat Protection (ATP) appliance can connect to these servers.
To change the DNS settings for an individual appliance
1. In ATP Manager, click **Settings > Appliances**, and then click on the appliance in the **Appliances** list.

   **Tip:** Hover over the appliance and click when the mouse pointer changes to a finger.
2. In the **DNS** panel, uncheck **Use Default**, if it is checked.
3. In the **DNS** panel, click **Edit DNS**.
4. Edit the **Primary DNS** or **Secondary DNS** IP address.
   
   You must specify an IPv4 address for the primary DNS server. You can specify either an IPv4 or IPv6 address for the secondary DNS server.
5. Click **Save DNS**.

To configure default DNS server settings
1. In ATP Manager, click **Settings > Appliances**, then click the **Edit Default Appliance** icon.
2. In the **DNS** panel, click **Edit DNS**.
3. In the **DNS** panel, type or change the **Primary DNS** or **Secondary DNS** IP address.
   
   You must specify an IPv4 address for the primary DNS server. You can type either an IPv4 or IPv6 address for the secondary DNS server.
4. Click **Save DNS**.

To apply default DNS server settings to a device
1. In ATP Manager, click **Settings > Appliances**, then click the appliance name in the **Appliances** list.
2. In the **DNS** panel, check **Use Default**.

**Note:** **Use Default** is not available until you configure the default DNS server settings.

---

**Configuring the connection to a time server**

To accurately timestamp incidents, Symantec Advanced Threat Protection (ATP) must synchronize its internal clock to a Network Time Protocol (NTP) time server.
A management platform and its network scanners can point to different time servers, as long as all time servers are accurate. Synapse relies on the time that is recorded for each incident to do proper correlation. In addition, SSL requires the correct time for proper operation.

**Important:** For incidents and events to have correct times in ATP Manager, ensure that your local computer and browser have the current time.

You configure the IP address of an NTP time server when you run bootstrap on the appliance. You can change this IP address in ATP Manager, or you can configure a default time server and apply that setting to individual appliances.

**To configure the connection to a time server**

1. Do either of the following:
   - **To configure the default time server**
     - In ATP Manager, click **Settings > Appliances**, and then click **Edit Default Appliance** icon.
   - **To configure a custom time server address for a single appliance**
     1. In ATP Manager, click **Settings > Appliances**, and then double-click on the appliance in the **Appliances** list.
     2. Uncheck **Use Default** in the **Time Server** panel, if it is checked.

2. In the **Time Server** panel, click **Edit Time Server**.
3. In the **Current Host** field, type the IP address or host name of the time server.
4. Click **Save Time Server**.

**To apply the default time server setting to a device**

1. In ATP Manager, click **Settings > Appliances**, and then double-click on the appliance in the **Appliances** list.
2. In the **Time Server** panel, check **Use Default**.

---

**Note:** **Use Default** is not available until you configure the default time server IP address.

---

**About syslog server connections**

Symantec Advanced Threat Protection (ATP) can send conviction incidents and notification messages to remote syslog servers using standard syslog forwarding. Using a remote syslog server lets you work with logs on a separate server, and it lets multiple devices send logs to a centralized location. Syslog output is sent over UDP. To set up the connection, you configure the network connection to each syslog server in ATP Manager. You must also configure each
syslog server to accept the logs from ATP. ATP always uses the syslog facility of "user" and severity of "INFO".

See “Configuring connections to syslog servers” on page 88.

---

**Note:** EDR, FDR, and search data are not forwarded to syslog.

ATP uses Common Event Format (CEF) for all syslog output. CEF defines a text-based syntax for pushing events to security information and event management (SIEM) systems. The syntax consists of a header and a set of key-value pairs. The CEF definition provides many SIEM-related, predefined fields, and ATP uses them where applicable.

Where no applicable predefined fields exists, ATP provides the key as “json” and a JSON object as value, which in turn contains all of the ATP-specific fields and their values. See the following example:

```
json={"actual_action":"Quarantined","actual_action_idx":1,"agent_infected":0,"agent_version":"14.0.1904.0000","alert":"Security risk found","data_source_url_domain":
","device_ip":"194.164.1.245","device_name":"140116-012018","device_time":
"2017-01-25T09:18:16.914Z","device_uid":"1fdfd164-e54b-446f-b803-218d939da4c4","disposition":1,"domain_name":"WORKGROUP","external_ip":"","file":
{"app_name":"cloudcar.exe","company_name":"null","confidence":119,"detection_type":"Heuristic","disposition":1,"folder":"C:\Users\Admin\Downloads","name":"cloudcar.exe","sha2":"3559378c933cdd434af2083f7535460843d2462033de74ec7c70dbef70124f5"},"host_name":
"170446-012018","internal_ip":"194.164.1.245","local_host_mac":"00-0c-29-cc-3e-17","no_of_viruses":1,"sep_mid":"de2508a9b62b26b4132029a46dd80","source":"Real Time Scan","threat":{"name":"WS.Reputation.1"},"type_id":4123,"user_name":"Admin","virus_def":
"2017-01-23 rev. 022","virus_name":"WS.Reputation.1","sep_installed":true}
```

CEF log format consists of a syslog prefix, a CEF header, and the extension. The syslog prefix contains a date, host name, log level, and component identifier. **Table 4-3** describes the CEF header fields that ATP sends.

<table>
<thead>
<tr>
<th>CEF header field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The CEF format version number</td>
</tr>
<tr>
<td>Device Vendor</td>
<td>Symantec</td>
</tr>
<tr>
<td>Device Product</td>
<td>The ATP appliance</td>
</tr>
<tr>
<td>Device Version</td>
<td>The ATP version number</td>
</tr>
<tr>
<td>CEF header field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Signature ID</td>
<td>The ID of a Symantec AntiVirus Engine or Vantage conviction. For other types of convictions, the ID is 0.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the event. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- atp_incident</td>
</tr>
<tr>
<td></td>
<td>- lcp_sep_alert_event</td>
</tr>
<tr>
<td></td>
<td>- lcp_sep_risk_event</td>
</tr>
<tr>
<td></td>
<td>- email_conviction_event</td>
</tr>
<tr>
<td></td>
<td>- sep_proxy_insight_event</td>
</tr>
<tr>
<td></td>
<td>- sep_proxy_ips_event</td>
</tr>
<tr>
<td></td>
<td>- sep_proxy_sonar_event</td>
</tr>
<tr>
<td></td>
<td>- sep_proxy_av_event</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the incident. From lowest to highest severity, the number can be 1, 3, 5, 8, or 10. If the value is 5, the CEF contains a non-conviction incident.</td>
</tr>
<tr>
<td>[Extension]</td>
<td>(Optional) Additional information, such as source IP address or file hash. The information is contained in sets of key-value fields. Where no applicable predefined fields exists, ATP provides the key as “json” and a JSON object as value, which will in turn contain all the ATP-specific fields and their values.</td>
</tr>
</tbody>
</table>

An example of a conviction incident log is as follows:

Jan 25 09:59:01 localhost lcp_sep_alert_event: INFO - ATP-Appliance
CEF:0|Symantec|ATPU|3.0.0|4123|
lcp_sep_alert_event|0|device_time=2017-01-25T09:18:16.914Z
device_uid=1fdfd144-e54b-476f-b803-218d939da4c4 internalIP=194.164.4.245
internalHost=170116-012018 filePath=C:\Users\Admin\Downloads fname=cloudcar.exe
sha2=3559378c933cdd434af2083f7535460843d2462033de74ec7c70d6e5f70124f5 md5=
AVEVirusName=WS.Reputation.1 actual_action=Quarantined user_name=Admin
domain_name=WORKGROUP json="actual_action": "Quarantined","actual_action_idx":1,"agent_infected":0,"agent_version":"14.0.1904.0000","alert":"Security risk found","data_source_url_domain":"
","device_ip":"194.1448.4.245","device_name":"170116-042018","device_time":"2017-01-25T09:18:16.914Z","device_uid":"1fdfe168-e54b-444g-b803-218d939da4c4","disposition":1,"domain_name":"WORKGROUP",
"external_ip":","file":{"app_name":"cloudcar.exe","company_name":"null","confidence":119,"detection_type":"Heuristic","disposition":1,"folder":

Configuring default and appliance settings
About syslog server connections
"C:\Users\Admin\Downloads", "name": "cloudcar.exe", "sha2": "3559378c933cdd434af2083f7535460843d2462033de74ec7c70debe5f70124f5", "host_name": "170446-012018", "internal_ip": "194.144.1.245", "local_host_mac": "44-0c-29-bb-3e-19", "no_of_viruses": 1, "sep_mid": "de2508a9b66bccc264132029a46dd680", "source": "Real Time Scan", "threat": {"name": "WS.Reputation.1"}, "type_id": 4123, "user_name": "Admin", "virus_def": "2017-01-23 rev. 022", "virus_name": "WS.Reputation.1", "sep_installed": true

Feb 1 11:07:06 localhost atp_incident: INFO - ATP-Appliance
CEF:0|Symantec|ATPU|3.0.0|16|atp_incident|0|device_time=2017-02-01T11:00:47.697Z
incident_uuid=eaf03410-e86d-11e6-e42a-000000000000c rule_name=incident_update
description=incident_update message=incident_update
json={"device_ip": "144.0.0.1", "device_name": "localhost.
localdomain", "type_id": 16, "composite": 1, "id": 1, "device_end_time": "2017-02-01T11:00:47.697Z", "uuid": "eaf03410-e44d-11e6-e42a-000000000000c", "events": 
"notavailable", "device_end_time": "2017-02-01T11:00:43.962Z", "device_ip": "194.144.1.245", 
"device_name": "194.144.1.245", "device_time": "2017-02-01T11:00:43.229Z", "device_uid": 
"1fde68e-e54b-476f-bb03-218d939a4c4", "disposition": 1, "external_ip": "213.211.198.62", 
"external_port": 80, "id": 1, "infected": false, "internal_hostname": "
192.144.1.445", "internal_ip": "194.144.1.445", "internal_port": 
56642, "ping_submit": true, "product_name": "SGS-ATP", 
"product_ver": "2.0", "scanner_name": "ATP-Appliance", "scanner_uid": 
{564d59c9-1df3-9ec8-84fc-3dc3a08dadcf}, 
"severity_id": 4, "signature_id": "24461", "signature_name": "Diagnostic: EICAR Standard Anti-Virus Test File", 
"silent": false, "threshold": 1, "type_id": 4113, 
"vlan_id": 0, "user_name": "Admin", "sep_installed": 
true, "timezone": 0, "time": "2017-02-01T11:00:43.229Z", 
"end_time": "2017-02-01T11:00:43.962Z", "log_time": "2017-02-01T11:07:06.882Z", 
"uuid": "ac6f70d-e44d-11e6-e769-0000000025c0", "log_name": "epmp_events-2017-02-01T11:00:43.962Z", "incident_priority_level": "LOW"}, "device_time": "2017-02-01T11:00:47.697Z", "atp_incident_id": 100011, "event_count": 10, "priority_level": 1, "scanners": 
["ATP-Appliance"], "filehash": ["b4e7c4260f2f0b0942244bcb0c0b389e705903487586ad3914d3914d9f8f1648868b30", 
"3559378c933cdd434af2083f7535460843d2462033de74ec7c70debe5f70124f5", "2546dcfc65ad85d4ddcc64fb056871cd5a00f2471cb7a5bf6d4ac23b6e9edad", 
"86263727095009b1363c82bb51b3d9b329352d60a1ecc251d4a309d44a07c3b", 
"275a021bbf6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"]
Configuring connections to syslog servers

Symantec Advanced Threat Protection (ATP) sends syslog communications over UDP. If you set up an all-in-one device, you only need to configure default syslog server connections. If you installed a management platform with one or more network scanners, you can apply the default syslog server connection settings to each appliance, or you can configure custom settings for individual appliances.

See “About syslog server connections” on page 84.
To configure a connection to a syslog server

1 Do either of the following:

- To configure the syslog server connection for the default appliance
  Do the following:
  1 In ATP Manager, click **Settings > Appliances**.
  2 Click **Edit Default Appliance**.

- To configure a custom syslog server connection for a single device
  Do the following:
  1 In ATP Manager, click **Settings > Appliances**, and double-click on the device in the **Appliances** list.
  2 In the **Syslog** section, uncheck **Use default**, if it is checked.

2 Click **+Add Syslog Server**.

3 In the **Add Syslog Server** dialog box, in the **Host** field, type the IP address of the syslog server.

4 In the **Protocol** field, select the appropriate protocol.

5 In the **Port** field, type the port on the syslog server that accepts syslog messages.
   Syslog usually uses port 514.

6 Click **Save**.

Refer to the manufacturer's instructions if you need assistance.

Editing a connection to a syslog server

You can modify the Symantec Advanced Threat Protection (ATP) connection IP address or port number to the syslog server connection.

To edit a connection to a syslog server

1 Do either of the following:

- To edit the syslog server connection for the default appliance
  Do the following:
  1 In ATP Manager, click **Settings > Appliances**.
  2 Click **Edit Default Appliance**.
To edit a custom syslog server connection for a single device

Do the following:

◆ In ATP Manager, click Settings > Appliances, and double-click on the device in the Appliances list.

2 In the Syslog group, hover over the server that you want to edit (option icons appear). Click the Edit option.

3 In the Edit Syslog Server dialog box, edit the settings as needed and then click Save.

See “Configuring connections to syslog servers” on page 88.

See “Deleting a connection to a syslog server” on page 90.

Deleting a connection to a syslog server

You can delete that default syslog server connections to Symantec Advanced Threat Protection (ATP) that can be applied to all devices, or you can delete the custom connections that you created for an individual device. When you delete a default syslog server connection, that connection is deleted for all devices that use the defaults. If you configured custom syslog server connections for a device, you can delete each connection individually. You can also disable all default syslog server connections on a particular device to prevent that device from connecting to any syslog server.

To delete a connection to a syslog server

1 Do either of the following:

To edit the syslog server connection for the default appliance

Do the following:

1 In ATP Manager, click Settings > Appliances.

2 Click Edit Default Appliance.

To edit a custom syslog server connection for a single device

Do the following:

◆ In ATP Manager, click Settings > Appliances, and double-click on the device in the Appliances list.

2 In the Syslog panel, hover over the server that you want to delete (option icons appear). Click the Delete option.

3 In the Confirmation dialog box, click Yes.

To disable default syslog server connections on an individual device

1 In ATP Manager, click Settings > Appliances, double click the appliances in the Appliances list.

2 In the Syslog panel, uncheck Use default.
See “Configuring connections to syslog servers” on page 88.

See “Editing a connection to a syslog server” on page 89.

About configuring a connection to an SNMP manager or trap receiver

Symantec Advanced Threat Protection (ATP) can be monitored using Simple Network Management Protocol (SNMP). Each management platform or all-in-one appliance must be configured to connect to and authenticate with the monitoring system. Network scanner and management platform appliances send SNMP notifications individually. A network scanner does not depend on the management platform to send notifications.

ATP supports only **SNMPv3** because of this standard's greater security. **SNMPv1** and **SNMPv2c** are not supported.

Before you configure the connection in ATP Manager:

1. Create an account on the SNMP system for each all-in-one or management platform ATP device.
   
   Each ATP device needs a user name and password to authenticate with the SNMP manager/trap receiver.

2. Configure the encryption type (DES or AES) and the secret key on your SNMP server.

3. In ATP Manager, navigate to **Settings > Appliances**, then click **Edit Default Appliance**. In the **SNMP** section, use the links to download the following ATP SNMP MIBs.
   
   - Download and import **ATP-SNMP-MIB.txt** into the SNMP manager.
   - Download and import **ATP-TRAPS-MIB.txt** and **ATP-NOTIFICATIONS-MIB.txt** into the SNMP Trap Receiver.

4. On your Network Management System, set the query timeout for polling to ATP to five seconds or more.

   ATP does not support management by SNMP. You cannot use a Network Management System to make changes to a ATP appliance. Instead, you can use ATP Manager to make changes to one or more ATP appliances.

See “Configuring a connection to an SNMP v3 manager or trap receiver” on page 91.

Configuring a connection to an SNMP v3 manager or trap receiver

The following procedures describe how to configure a default or device-specific Symantec Advanced Threat Protection (ATP) connection to an SNMP v3 manager or trap receiver.
If you use the same server for both management and traps, configure the connection for the Manager role, and then repeat the procedure for the Trap role. Enter the same IP address for both.

**To configure a connection to the default SNMP v3 manager**

1. In ATP Manager, click **Settings > Appliances**, and then click **Edit Default Appliance**.
2. In the **SNMP** panel, click **+Add SNMP v3**.
3. Specify the following information:

   - **Type**: From the menu, choose **Manager** if you want the SNMP management server to poll ATP. Choose **Trap** if you want the SNMP trap receiver to accept SNMP notifications from ATP.
   - **Trap IP Address**: Type the IP address of the SNMP trap receiver.
   - **User**: Type the user name that you assigned to this ATP device on the SNMP manager/ trap receiver.
   - **Password**: Type the password that you assigned to the SNMP manager and trap receivers respectively.
   - **Auth Type**: From the menu, select the authentication hash type that matches the authentication hash type on the SNMP manager/ trap receiver: **MD5** or **SHA**.
   - **Encrypt Type**: From the menu, select the encryption type that matches the encryption type on the SNMP manager/ trap receiver: **DES** or **AES**. ATP supports AES128.
   - **Secret Key**: Type the secret key that matches the secret key on the SNMP manager/ trap receiver.
   - **Engine ID**: The engine ID is a unique identifier (usually in hexadecimal form) for the SNMP v3 trap server. This ID is created when the SNMP service is created. The administrator of the SNMP server should be able to provide the engine ID value to type in this field.

4. Click **Save**.
5 Repeat steps 2 through 4 for each additional SNMP v3 server connection that you need to configure.

6 Check Enable SNMP.

This setting lets you enable and disable SNMP communications without deleting the connection settings.

See “About configuring a connection to an SNMP manager or trap receiver” on page 91.

To apply the default SNMP v3 server settings to a device

1 In ATP Manager, click Settings > Appliances, and then click the device in the Appliances list.

2 In the SNMP panel, check Use Default.

---

Note: Use Default is not available until you configure default SNMP settings.

---

To configure an SNMP v3 server connection for a single device

1 In ATP Manager, click Settings > Appliances, and then click the device in the Appliances list.

2 In the SNMP panel, uncheck Use Default, if it is checked.

3 Follow steps 2 through 4 of To configure a connection to the default SNMP v3 manager.

---

Configuring ATP to use cloud sandboxing or on-premises sandboxing

Symantec Advanced Threat Protection (ATP) can send files to a sandboxing service to “detonate” potential malware in a virtual environment to observe its behavior.

The default sandboxing option is Symantec’s Cynic cloud-based malware detonation system. ATP 3.0 introduces a preview feature that lets ATP submit files to your own on-premises Symantec Malware Analysis 4.2 or later and Content Analysis 2.2 or later. This feature lets you keep file analysis local.

---

Note: A preview feature is a fully implemented feature that hasn’t yet completed Symantec’s rigorous testing and review process. As a result, preview features are not fully supported. Preview features provide a glimpse into the functionality that ATP is developing and gives you an opportunity to help shape the feature through your feedback.
You can configure sandboxing on an ATP appliance-by-appliance basis. And each ATP appliance can use different sandboxing settings. So some ATP appliances can use Cynic; others can use an on-premises Malware Analysis appliance.

This option is also useful if you have multiple ATP appliances in different locations. Each can use a different malware analysis technology for on-premises appliances to keep files local. For example, assume that you have an ATP appliance in Los Angeles and another in London. You can configure each to submit files only to your local Malware Analysis appliance in Los Angeles and London, respectively.

Configure Cynic cloud-based sandboxing | Configure on-premises Symantec Malware Analysis appliance sandboxing

**Configure Cynic cloud-based sandboxing**

Cynic cloud service is the default option. You only need to configure this setting if you want to change the setting back to Cynic cloud service from Malware Analysis on premises appliance.

To configure ATP to use Cynic for sandboxing

1. In ATP Manager, click **Settings > Appliances**.
2. Do one of the following:
   - Click **Edit Default Appliance** to edit the defaults for the ATP appliance.
   - In the **Appliances** list, click on the appliance that you want to edit.
3. Scroll down to **Sandboxing**, and click **Edit Sandboxing Settings**.
4. Click the **Service** drop-down menu, and select **Cynic cloud service**.
5. Click **Save**.

See “Changing the geographic location where you submit files for cloud-based sandboxing” on page 22.

**Configure on-premises Symantec Malware Analysis appliance sandboxing**

To configure ATP to use an Symantec Malware Analysis appliance for sandboxing

1. In ATP Manager, click **Settings > Appliances**.
2. Do one of the following:
   - Click **Edit Default Appliance** to edit the defaults for the ATP appliance.
   - In the **Appliances** list, click on the appliance that you want to edit.
3. Scroll down to **Sandboxing**, and uncheck **Use default**.
4. Click **Edit Sandboxing Settings**.
5. Click the **Service** drop-down menu, and select **Malware Analysis on premises appliance**.
6 Configure the following Malware Analysis appliance server settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Analysis Server</td>
<td>Type the host name or IP address of your malware analysis server.</td>
</tr>
<tr>
<td>Malware Analysis User</td>
<td>Type the user name for a user who has access rights to the malware analysis server.</td>
</tr>
<tr>
<td>Malware Analysis Token</td>
<td>A token is generated on the Malware Analysis appliance. This token proves to the Malware Analysis appliance that ATP has your permission to analyze files.</td>
</tr>
</tbody>
</table>

To generate the Malware Analysis token:

1. Log on to the Malware Analysis appliance.
2. Click **System Settings > Users**.
3. On the **List Users** tab, select a user.
4. Under **Add New API Key**, type an API key label.
   
   For example: ATP Key.
5. Click the **API Key Access Level** drop-down list and select **analyst**.
6. Select **Add New Key**.
7. In the **API Key Created** window, copy the API key.
   
   You cannot access this key again once you close this window.
8. Click **close window**.
9. In ATP Manager, copy the generated key into the **Malware Analysis Token** field.

7 Optionally, check **Use Network Proxy** to access the Malware Analysis appliance through the ATP network proxy.

   See “Configuring network proxy information” on page 79.

8 Optionally, you can secure communications between ATP and the Malware Analysis appliance by doing all of the following:

   - Obtain a certificate from your Malware Analysis appliance and save it in a location that you can access from ATP Manager.
In ATP Manager on the **Edit Sandboxing Settings** dialog box, check **Validate Server Certificate**.

- Browse to and select the Malware Analysis appliance certificate.

  Using a server certificate prevents spying or malicious interference.

9. Click **Save**.

---

### About static routes

A static route is a path to an internal subnet through an intermediate switch. You can specify up to three static routes when you run bootstrap on an all-in-one device or network scanner. Configure a static route to the user's subnet if a user wants to access ATP Manager from a part of the network that is normally inaccessible from the Symantec Advanced Threat Protection (ATP) appliance.
Creating and managing user accounts

This chapter includes the following topics:

- Managing users
- Adding local user accounts
- Editing a local user account
- Disabling and enabling a local user account
- Requesting a new logon password
- Preparing for Active Directory integration
- Adding an Active Directory domain
- Adding an Active Directory group
- Adding the initial administrator account

Managing users

A Symantec Advanced Threat Protection (ATP) user is a user who can log into ATP Manager and then access features and perform functions based on the user's role. Each ATP user requires a user account.

As an administrator, you can add and manage user accounts in the following ways:
Add local user accounts

You can manually add user accounts in ATP Manager. When you add a local user account, you specify the user's login credentials, email address, and role. The user’s role authorizes which ATP Manager pages the user can access and which functions the user can perform.

You manage local user accounts manually. For example, if you hire a new employee, you must add a user account for that individual. You must then make any future password and email address changes as required. If the employee leaves your organization, you disable the employee’s user account.

See “Adding local user accounts” on page 101.

See “Editing a local user account” on page 103.

See “Disabling and enabling a local user account” on page 104.

Integrate ATP with Microsoft Active Directory

If you use Microsoft Active Directory (AD) to manage your organization's users, you can add AD groups to ATP. Users from those groups use their AD credentials to log into ATP Manager.

Additionally, you can assign an ATP user role to each group that you add. The group’s role authorizes which pages its users can access and which functions they can perform.

Note: For information on how to import your AD groups into Symantec Endpoint Protection Manager, see the following article: http://www.symantec.com/docs/HOWTO80777.

AD integration facilitates the management of your ATP users by dynamically using the most current AD account information when users log into ATP Manager. If a user's information or employment status changes in AD, ATP automatically recognizes those changes.

See “Preparing for Active Directory integration” on page 105.

See “Adding an Active Directory domain” on page 106.

See “Adding an Active Directory group” on page 109.

Note: You can add local user accounts and integrate with AD concurrently. If you do both, you should not add local user accounts that exist on your AD server. Additionally, you should have at least one local administrator account who can log into ATP Manager if ATP cannot access your AD server. This account may be your initial administrator account, or another account that you create.

See “Adding the initial administrator account” on page 111.

See “ATP user roles” on page 99.
ATP user roles

Symantec Advanced Threat Protection (ATP) provides the following user roles for ATP Manager:

- **Admin**: An administrator has the highest access level, with full read/write access to all ATP Manager functions.
- **Controller**: A controller has full read/write access to all ATP Manager functions except to the Settings options.
- **User**: A user has limited access throughout ATP Manager, with no access to the Settings options. A user can view events and incidents, but cannot perform actions against them.

### Table 5-1: ATP Manager user role access rights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Admin</th>
<th>Controller</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform IoC (Indicators of Compromise) searches</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Perform endpoint searches</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td><strong>Dashboard</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network, endpoint, and email traffic from dashboard widgets</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td><strong>Incidents</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View incidents and related details pages</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Add a file to Whitelist or Blacklist policies</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Quarantine and un-quarantine an endpoint</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Clean a file from an endpoint</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
</tbody>
</table>
### Table 5-1  ATP Manager user role access rights (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Admin</th>
<th>Controller</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download a file from an endpoint</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Submit a file to Cynic or VirusTotal</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Add comments to an incident</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>View events</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View policies</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Create policies</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Modify policies</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Delete policies</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View logs</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View existing reports</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
<tr>
<td>Schedule and run reports</td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
<td><img src="access_icon.png" alt="Access" /></td>
</tr>
</tbody>
</table>
### Table 5-1 ATP Manager user role access rights (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Admin</th>
<th>Controller</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download reports</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete reports</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global settings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Appliance settings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>User settings</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Note:</strong> All users have the rights to reset their passwords from the ATP Manager logon page.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>See “Requesting a new logon password” on page 104.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Sharing settings</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

See “Managing users” on page 97.
See “Adding local user accounts” on page 101.
See “Editing a local user account” on page 103.
See “Disabling and enabling a local user account” on page 104.

### Adding local user accounts

As an administrator, you can add a local user account for any user who needs to log into ATP Manager. When you add a local user account, you specify the user's login credentials, email address, and role. The user's role determines which pages the user can access and which functions the user can perform.

See “ATP user roles” on page 99.
Note: If you use Microsoft Active Directory (AD) to manage your organization's users, you can add an AD domain and AD groups in ATP Manager. Users from these groups use their AD credentials to log into ATP Manager. The group’s role determines which pages its users can access and which functions they can perform.

See “Adding an Active Directory domain” on page 106.
See “Adding an Active Directory group” on page 109.

You can also specify whether the user should receive an email notification when an incident occurs. This notification includes information about the incident, and may be helpful for incident responders who need to react to potential threats. It also includes an attached report that contains additional information about the incident, such as related incidents.

After you add a local user account, an email is sent to the user with the login credentials that you specified. When the user logs into ATP Manager for the first time, the user is required to change the password.

You cannot delete a local user account after you add it. You can disable a user account, which prevents that user from logging into ATP Manager.

See “Disabling and enabling a local user account” on page 104.

To add a local user account

1. In ATP Manager, click **Settings > Users > Local Accounts > + Add Account**.
2. In the **Add New Account** dialog box:
   - Type the user’s **Login** name.
   - Type the user’s **Password** and confirm it.
   - Type the **Display Name**.
     The display name appears in the upper right corner of ATP Manager when the user is logged on.
   - From the **Role** drop-down menu, select the user’s role.
     See “ATP user roles” on page 99.
   - Type the **User Email** address.
     The user's email address is used to receive email notifications regarding the user's account; for example, password resets.
3. Check **Receive email notifications when incidents occur** if you want the user to receive an email notification and report when an incident is created.
4. Click **Save**.

See “Managing users” on page 97.
See “Editing a local user account” on page 103.
See “Disabling and enabling a local user account” on page 104.
See “Requesting a new logon password” on page 104.

Editing a local user account

As an administrator, you can edit the following local user account information in ATP Manager:

- **Password**
  If you edit the user's password, the password you provide is temporary. The user receives an email with the temporary password, which the user is required to change the next time the user logs into ATP Manager.

- **Display Name**
  Appears in the upper right corner of ATP Manager when the user logs in.

- **Role**
  Determines which ATP Manager pages the user can access and which functions the user can perform.

- **User Email**
  Used to receive email notifications regarding the user's account; for example, password resets.

- **Receive email notification when incidents occur**
  Used to receive an email notification and report when an incident is created.

**Note:** Changes that you make to a user's account take effect the next time the user logs into ATP Manager.

**Note:** You cannot edit the user's Login name.

You can also enable and disable a user account.

See “Disabling and enabling a local user account” on page 104.

To edit a local user account

1. In ATP Manager, click **Settings > Users > Local Accounts**.
2. Hover over the actions menu [three vertical dots] to the far right of the account that you want to edit, and then click **Edit User Account**.
3. In the **Edit User Account** dialog box, edit the settings as needed.
4. Click **Save**.

See “Adding local user accounts” on page 101.
Disabling and enabling a local user account

When you add a local Symantec Advanced Threat Protection (ATP) user account, the account is enabled by default. As an administrator, you can disable a local user account (for example, if the user is no longer employed by your organization). Disabling an account does not delete it; the account still appears on the Local Accounts page. However, a disabled user cannot log into ATP Manager. Additionally, the user no longer receives email notifications.

You can re-enable a user account that is disabled.

To disable or enable a user account

1. In ATP Manager, click **Settings > Users > Local Accounts**.
2. On the row with the account that you want to change, move the slider to the left to disable the account, and to the right to enable it.

Requesting a new logon password

As a Symantec Advanced Threat Protection (ATP) user, you may need to request a new ATP Manager logon password for the following reasons:

- You feel your current password is not secure.
- You forgot your existing password.
- You are locked out of ATP Manager because you typed your current password incorrectly five consecutive times. In this event, you receive an email notification informing you that you are temporarily locked out of your account for ten minutes.
- Your administrator assigned you a new, temporary password.

To request a new logon password

1. On the ATP Manager Log On page, click **Forgot password?**.
2. On the **Forgot Password** page, in the **User name** field, type your login name and click **Retrieve**.
A temporary password is sent to the email address that is associated with the login name you entered. When you log into ATP Manager with this password, you are prompted to change it. When you change your temporary password, you receive another email notifying you of the change.

If you do not receive the email notification, it may be because there is no email address associated with your user account. Contact your ATP administrator.

See “Managing users” on page 97.

Preparing for Active Directory integration

If you use Microsoft Active Directory (AD) to manage your organization’s users, you can integrate ATP with AD to facilitate user management. ATP Manager.

See “Managing users” on page 97.

Before you integrate ATP with AD, you must perform the tasks listed in Table 5-2.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create AD groups based on ATP user roles</td>
<td>Create an AD group on your AD server that contains ATP users for any of the desired ATP user roles: administrator, controller (also known as an incident responder), and user. ATP uses the user’s AD credentials to log into ATP Manager. The user’s role then authorizes which pages the user can access and which functions the user can perform. You add these groups to ATP after you add your AD domain. See “Adding an Active Directory group” on page 109.</td>
</tr>
<tr>
<td>Create email distribution lists (DLs) for email notifications (Optional)</td>
<td>Create a DL for each group of users that you want ATP to send an email notification to when an incident occurs. This notification includes information about the incident, and may be helpful for incident responders who need to react to potential threats. You can specify this DL when you add an AD group in ATP Manager. See “Adding an Active Directory group” on page 109.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create an ATP user on your AD server</td>
<td>Create an ATP user on your AD server that has the <strong>Read all user information</strong> common task assigned to it. This task allows ATP to query your AD server for user and group information. You specify the credentials for this user when you configure your AD domain in ATP Manager. <strong>Note:</strong> You only need to create this account if you configured your AD server to prevent anonymous queries. Symantec recommends that you create this user, as allowing anonymous access to your AD server may be a security risk. See “Adding an Active Directory domain” on page 106.</td>
</tr>
<tr>
<td>Prepare your network environment</td>
<td>Provide ATP access to your AD server over port 636.</td>
</tr>
<tr>
<td>Prepare your AD server</td>
<td>Ensure that your AD server is using Windows Server 2012 R2 (or later).</td>
</tr>
<tr>
<td>Issue a certificate</td>
<td>Issue a certificate to your primary and backup AD servers. You provide this certificate to ATP later to enable secure communications. While this step is optional, Symantec recommends that you secure your environment.</td>
</tr>
</tbody>
</table>

See “Managing users” on page 97.

### Adding an Active Directory domain

To integrate Symantec Advanced Threat Protection (ATP) with your Microsoft Active Directory (AD) server, you must add your AD domain in ATP Manager. You can only specify one domain, which can include a primary and backup server.

There are a number of preliminary tasks that you should perform before you add your domain. For a list of these tasks:

See “Preparing for Active Directory integration” on page 105.

Once you add your AD domain, you can add the AD groups that are part of that domain.
See “Adding an Active Directory group” on page 109.

To add an Active Directory domain

1. In ATP Manager, click **Settings > Users > Active Directory**.
2. Click **+Add Domain**.

**Note:** You can only add one domain. After you add your domain, you no longer see the **Add Domain** option (unless you delete the domain).
3. On the **Domains** page, add the following:

<table>
<thead>
<tr>
<th><strong>Primary IP or Hostname</strong></th>
<th>The IP address or hostname of your AD server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Port</strong></td>
<td>The port over which you want ATP to communicate with your AD server. The recommended port is 636.</td>
</tr>
<tr>
<td><strong>Backup IP or Hostname (optional)</strong></td>
<td>The IP address or hostname of your backup AD server. ATP uses this server if your Primary server is unavailable.</td>
</tr>
<tr>
<td><strong>Backup Port (optional)</strong></td>
<td>The port over which you want ATP to communicate with your Backup AD server.</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>The Fully Qualified Domain Name (FQDN) with which users log into ATP Manager. For example, if users log in using <a href="mailto:name@yourcompany.com">name@yourcompany.com</a>, the FQDN is the portion of the login that follows that @ symbol.</td>
</tr>
<tr>
<td><strong>NetBIOS Name</strong></td>
<td>The NetBIOS name of your AD server.</td>
</tr>
<tr>
<td><strong>Allow anonymous authentication</strong></td>
<td>To authenticate ATP users, ATP needs to log into your AD server to query your AD groups.</td>
</tr>
<tr>
<td></td>
<td>Check this box to allow ATP to log into your AD server anonymously (without a username and password). If you do not check this box, ATP prompts you to enter a username and password (see below).</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The username and password of the user who can log into your AD server to query your AD groups.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>This account must exist on your AD server with the Read all user information common task assigned to it. It must also have any other permissions that it needs to access AD services. For information on how to create this account, see the following KB article: <a href="http://www.symantec.com/docs/TECH104726">http://www.symantec.com/docs/TECH104726</a>.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This user is only required if you do not allow for anonymous authentication (see above).</td>
</tr>
</tbody>
</table>
Validate Certificate

Check this box to add the certificate that you issued to your ATP server. This certificate should match the certificate of your primary and backup AD servers.

When you check this box, you can browse your local machine to find, add, and validate the certificate.

4 Click OK.

Deleting an Active Directory domain

You can delete your Active Directory domain. When you do, the groups associated with that domain are also deleted. If a user from one of these groups is logged into ATP Manager at the time you delete the domain, the user remains logged in and is able to perform group-related functions.

To delete an Active Directory domain

1 In ATP Manager, click **Settings > Users > Active Directory**.

2 For the domain that you want to delete, hover over the **Actions** icon (three vertical dots), and then click the **Delete** icon.

Updating the certificate

If you issue a new certificate to your AD server, you must also supply it to your ATP server. When you do, you can add it to ATP and then validate it.

You can view the status of the current certificate in the **Certificate Status** column in the **Domain** section of the **Settings > Users > Active Directory** page.

To update the certificate

1 In ATP Manager, click **Settings > Users > Active Directory**.

2 Hover over the **Actions** icon (three vertical dots) for the domain, and then click the **Edit** icon.

3 On the **Domain** page, click **Validate Certificate**, and then click **Browse** to find and add the certificate.

4 Click **Save**.

Adding an Active Directory group

If you want to use Microsoft Active Directory (AD) to authenticate users who log into ATP Manager, you need to add AD groups to Symantec Advanced Threat Protection (ATP). Users from these groups use their AD credentials to log into ATP Manager.
Before you can add groups, you must add your AD domain. See “Adding an Active Directory domain” on page 106.

The groups that you add must belong to the AD domain, and be comprised of users that you authorize to act in the roles that are listed below. The group’s role authorizes which pages its users can access and which functions its users can perform. See “ATP user roles” on page 99.

**Admin**
Administrators can access all pages and perform all functions in ATP Manager.

**Controller (or “incident responder”)**
Controllers (or "incident responders") can access all pages in ATP Manager, except the **Settings** page.

**User**
Users can access all pages in ATP Manager, except the **Settings** page. Users can view events and incidents, but cannot perform actions against them (such as isolating machines or deleting files on endpoints).

You can add more than one group per role. For example, you may have multiple AD groups for Controllers based on their location.

If a user belongs to multiple groups that have different roles, the group with the highest role takes precedence. For example, if a user belongs to both the Controller and User groups, the user is granted the permissions of the Controller group.

**To add an Active Directory group**

1. In ATP Manager, click **Settings > Users > Active Directory**.
2. Click **+ Add Group**.
3. On the **Group** page, enter the **Group Name** and then click **Check Name**.
   
   A list appears if there is more than one group containing all or part of the name that you specified.
4. From the list, select the group that you want to add.
5. From the **ATP Role** drop-down list, select the role that applies to this group.
6. (Optional) Check **Receive email notifications when incidents occur** if you want users in this group to receive an email notification when ATP creates an incident.
7. Enter the Email address(es) of the users that you want to receive the email notification.
   
   This email address can be a distributed list, or multiple email addresses separated by commas. ATP does not use the email addresses that are associated with your AD users.
8. Click **Save**.

See “Managing users” on page 97.

See “Preparing for Active Directory integration” on page 105.

See “Adding an Active Directory domain” on page 106.
Adding the initial administrator account

You add the initial administrator account in the Symantec Advanced Threat Protection (ATP) setup wizard. After you complete the wizard, you can log into ATP Manager with the credentials of this account to add other users and complete your setup tasks.

See “Managing users” on page 97.

See “Completing setup tasks” on page 19.

After you add the initial administrator account, the account you used to run the setup wizard is disabled. Additionally, you cannot edit the login name of the initial administrator account.

Tip: Consider creating a backup administrator account. This backup administrator account can be helpful if the initial administrator account is lost or becomes corrupted or the initial admin account is inaccessible. See “Adding local user accounts” on page 101.

To set up the initial administrator account

1. In the Create an Administrator Account dialog box:
   - Type the login name.
   - Type a password and confirm it.
   - Type the display name. The display name appears in the upper right corner of ATP Manager when the user is logged in.
   - Type the administrator’s email address.

2. Click Submit.
Creating Blacklist and Whitelist policies

This chapter includes the following topics:

■ About policies
■ Creating a Blacklist policy
■ Creating a Whitelist policy
■ Supported policy match values for IP addresses, domains, and URLs
■ Managing policies

About policies

The Policies page lets you create Blacklist policies and Whitelist policies for files and external computers. This page is also where you can manage the policies that you created or that Symantec Advanced Threat Protection (ATP) creates when you take the Add to Blacklist or Add to Whitelist action when remediating incidents.

Only users with the Admin or Controller role can create Blacklist policies and Whitelist policies.
Table 6-1  Policy types

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklist</td>
<td>These are the files and external computers that ATP has not identified as a threat, but that you deem untrustworthy. If you run ATP in inline block mode, ATP blocks users from accessing the external computers or files that you specify in your Blacklist policies. If you run ATP in tap mode or inline monitor mode, users can access items in your Blacklist. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.</td>
</tr>
<tr>
<td>Whitelist</td>
<td>These are the files and external computers that you know are safe. ATP considers these items trustworthy and takes no action when endpoints access them.</td>
</tr>
</tbody>
</table>

Creating a Blacklist policy

Symantec maintains a worldwide blacklist of external computers and files that is updated regularly and integrated with Symantec Advanced Threat Protection (ATP). You can supplement this list by creating Blacklist policies for external computers or the files that you deem untrustworthy. For example, you may want to create a Blacklist policy for a file that recently appeared in your cybersecurity intelligence that Symantec has yet to identify as a threat.

Create a Blacklist policy to do any of the following:

Block or detect access to an external computer

You can create a Blacklist policy for an external computer based on its IP address or subnet, domain, or URL.

If you run ATP in inline block mode, ATP blocks access to external computers. When a user attempts to access a blacklisted external computer, a blocking page appears indicating why access is denied. If you run ATP in any other mode, ATP does not block access. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.
You can create a Blacklist policy for a file based on its hash value as follows:

- **MD5**
  If ATP is integrated with Symantec Endpoint Protection, Symantec Endpoint Protection prevents blacklisted MD5 files (Windows executable files and MSI installers) that are on your endpoints from running.
  When you create a Blacklist policy for a file using its MD5 hash value, the hash value is added to the ATP blacklisted file on Symantec Endpoint Protection Manager. This file is added to the File Fingerprint Lists policy for all domains and all groups within those domains. If you add a new group to Symantec Endpoint Protection, the ATP blacklisted file is subsequently synchronized with that group as well. Additionally, if you edit the ATP blacklisted file on Symantec Endpoint Protection (for example, by removing an entry), Symantec Endpoint Protection overwrites your edits the next time that the file is synchronized. The ATP blacklisted file does not affect other fingerprint files that you create in Symantec Endpoint Protection.

- **SHA256**
  If Symantec Endpoint Protection is configured to use your ATP proxy, Symantec Endpoint Protection immediately quarantines blacklisted SHA256 files when it detects them on your endpoints.

  If you run ATP in inline block mode, ATP blocks access to blacklisted files. When a user attempts to access a blacklisted file, a blocking page appears. If you run ATP in any other mode, ATP does not block access. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.

You must have the Admin role or Controller role to create Blacklist policies.

**To create a Blacklist policy**

1. In ATP Manager, click **Policies**.
   - The **Blacklist** tab appears.
2. Click the plus sign and select **Add to Blacklist**.
3. In the **Add to Blacklist** dialog box, click the **Type** drop-down list and select one of the following:
   - **IP**
   - **Domain**
   - **URL**
   - **SHA256**
     The SHA256 hash value must be 64 characters with values ranging between 0 - 9 and a - f.
   - **MD5**
Note: You cannot edit the Type or Match Value of a blacklisted item after you add it. However, you can delete it or edit the comment. See “Managing policies” on page 120.

4 In the Match Value field, type the value of the blacklisted item based on the type that you selected.

ATP validates the value based on its type. The Match Value appears in the Blacklist policy list as the Rule Value.

See “Supported policy match values for IP addresses, domains, and URLs” on page 117.

5 Optionally, type a comment in the Comments field.

For example, you may want to specify the file name for SHA256 hash.

Note: Extended ASCII characters do not render properly in .csv format.

6 Click Save.

Creating a Whitelist policy

You can create Whitelist policies for files and external computers so that Symantec Advanced Threat Protection (ATP) explicitly allows access to them regardless of their reputation. When you whitelist an item, ATP considers it "trusted" and takes no action on it. For example, if you whitelist a file, ATP does not inspect that file nor does it request a reputation score for it. Whitelisting trusted files and external computers can conserve scanning resources and reduce the number of events that ATP creates. It can also eliminate false negatives.

Create a Whitelist policy to do any of the following:
When you whitelist an external computer, ATP considers it trustworthy and does not inspect traffic to or from it from your endpoints (even if it's blacklisted). You can whitelist an external computer based on its IP address or subnet, domain, or URL.

ATP permits access to whitelisted computers in the following ways:

- **IP address and IP subnet**
  - If you whitelist an IP address, ATP bypasses all traffic inspection to and from that IP address. However, it continues to inspect the traffic that is associated with other IP addresses on the same subnet of that IP address.

- **Domain**
  - If you whitelist a domain, ATP allows access to any sub-domains and URLs associated with that domain.

- **URL**
  - If you whitelist a URL, ATP allows access to any sub-pages (including files) associated with that URL.

**Allow explicit access to a file**

You create a Whitelist policy for a file based on its SHA256 hash value or URL. If you whitelist a file based on its SHA256 hash value, ATP allows access to it on any external computer. If you whitelist a file based on its URL, ATP allows explicit access to it on that site only.

When you whitelist a file, ATP considers it trustworthy regardless of its identity as a known threat or its reputation. When an endpoint accesses a whitelisted file, ATP takes no action against it. For example, if Symantec Endpoint Protection is configured to use your ATP proxy, ATP does not block the file (even if it's blacklisted). If Symantec Endpoint Protection is not configured to use your ATP proxy, ATP does not generate a detection event.

You must have the Admin role or Controller role to create Whitelist policies.

**To create a Whitelist policy**

1. In ATP Manager, click Policies > Whitelist > + Add to Whitelist.
2. Click the plus sign and select Add to Whitelist.
3. In the Add to Whitelist dialog box, click the Type drop-down list and select one of the following:
   - IP
   - Domain
   - URL
   - SHA256
The SHA256 hash value must be 64 characters with values ranging between 0 - 9 and a - f.

Note: You cannot edit the Type or Match Value of a whitelisted item after you add it. However, you can delete it or edit the comment. See “Managing policies” on page 120.

4 In the Match Value field, type the value of the whitelisted item based on the type that you selected.

ATP validates the value based on its type. The Match Value appears in the Whitelist policy list as the Rule Value.

See “Supported policy match values for IP addresses, domains, and URLs” on page 117.

5 Optionally, type a comment in the Comments field.

For example, you may want to specify the file name for SHA256 hash.

Note: Extended ASCII characters do not render properly in .csv format.

6 Click Save.

**Supported policy match values for IP addresses, domains, and URLs**

The following table provides the supported whitelist and blacklist policy match values for IP addresses, domains, and URLs for Symantec Advanced Threat Protection (ATP).
### Supported policy match values for IP addresses, domains, and URLs

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain or URL</td>
<td>You can use special characters, such as international characters</td>
<td><a href="http://go%C5%9B%C4%87.pl/a">http://gość.pl/a</a></td>
</tr>
<tr>
<td></td>
<td>You can use full or partial domain names.</td>
<td>gov.ca/dmv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.gov.ca</td>
</tr>
<tr>
<td><strong>Note:</strong> ATP looks for the most specific match when you have both Blacklist and Whitelist policies with similar domain names. For example, you can blacklist news.google.com and whitelist google.com.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 6-2  (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>You can use both the IPv4 and IPv6 protocols</td>
<td>10.10.10.0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fe80::250:56ff:fe99:3903</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> ATP looks for the most specific match when you have both Blacklist and White-list policies with similar IP addresses. For example, you can blacklist an IP address that falls within a whitelisted IP subnet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Unspecified addresses, zero subnet masks, and zero CIDR bit length/prefixes are not allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ d.d.d.d/0.0.0.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ d.d.d.d/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use dot-decimal notation for IPv4</td>
<td>010.010.010.010</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can eliminate leading zeros. For example, you can represent 010.010.010.010 as 10.10.10.10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use IPv4-compatible addresses for IPv6</td>
<td>::w.x.y.z</td>
</tr>
<tr>
<td></td>
<td>You can use colon-eliminated hex notation for IPv6</td>
<td>For example, you can represent FF01:0:0:0:0:0:101 as FF01::101.</td>
</tr>
</tbody>
</table>

See “Creating a Whitelist policy” on page 115.
See “Creating a Blacklist policy” on page 113.
See “Managing policies” on page 120.
Managing policies

Symantec Advanced Threat Protection (ATP) helps you manage the policies that you create either manually or that are created when you take the Add to Blacklist or Add to Whitelist action on the files and endpoints that you analyze.

You must have the Admin role or Controller role to add and remove Blacklist policies or Whitelist policies. Actions that are not permitted based on your role appear in ATP Manager as inactive.

Table 6-3  Manage policies

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>To view existing policies</td>
<td>In ATP Manager, click <strong>Policies</strong>. The <strong>Blacklist</strong> tab appears by default. Click the <strong>Whitelist</strong> tab to view Whitelist policies.</td>
</tr>
<tr>
<td>To modify a comment</td>
<td>1. Click on the comment that you want to modify.</td>
</tr>
<tr>
<td></td>
<td>2. Revised the existing comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click the check mark to save your changes.</td>
</tr>
<tr>
<td>To move a policy to the other list</td>
<td>1. Click on the actions menu (three vertical dots) to the far right of the row for the policy that you want to move. Options appear.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Move to Whitelist</strong> or <strong>Move to Blacklist</strong>, as appropriate.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Ok</strong> to confirm your action.</td>
</tr>
<tr>
<td>To filter policies</td>
<td>Click <strong>Show Filters</strong> and select one or more types that you want to filter on.</td>
</tr>
<tr>
<td>To search policies</td>
<td>Type the search value into the <strong>Filtered Search</strong> field. Matching values appear as soon as you start populating this field.</td>
</tr>
<tr>
<td>To delete a policy</td>
<td>1. Click on the actions menu (three vertical dots) to the far right of the row for the policy that you want to move. Options appear.</td>
</tr>
<tr>
<td></td>
<td>2. Click the &quot;x&quot; mark.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Ok</strong> in the confirmation dialog box.</td>
</tr>
</tbody>
</table>
### Table 6-3
Manage policies *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **To export policies to a .csv text file** | **1** On the Blacklist or Whitelist tab, click the drop-down arrow on the right side of the header row.  
**2** Click **Export Grid**.  
**3** On the **Export** dialog box, under **Report Name**, type a name for the export file.  
**4** Click **OK**.  
You can view and download the exported file from the **Reports > Exports Report** page.  
**Note:** Extended ASCII characters do not render properly in .csv format. |

See “Creating a Blacklist policy” on page 113.

See “Creating a Whitelist policy” on page 115.
Monitoring system health

This chapter includes the following topics:

- ATP system messages and recommended actions

ATP system messages and recommended actions

Symantec Advanced Threat Protection (ATP) provides the following system messages:

Table 7-1 - System Is Critical | Table 7-2 - System Needs Attention

Table 7-1 lists the Critical state messages and recommended actions to correct the cause.

### Table 7-1 System Is Critical messages

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>License failure</td>
<td>Contact Symantec Support.</td>
<td>Report</td>
</tr>
<tr>
<td>License is invalid</td>
<td>Install a new license. If the license still fails, contact</td>
<td>ATP Manager</td>
</tr>
<tr>
<td></td>
<td>Symantec Support.</td>
<td></td>
</tr>
<tr>
<td>Unable to get license info</td>
<td>Contact Symantec Support.</td>
<td>ATP Manager</td>
</tr>
</tbody>
</table>
### Table 7-1  System Is Critical messages (continued)

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synapse error</strong></td>
<td>Either a Synapse connectivity error or a Symantec Endpoint Protection Manager database error occurred. Use the following remedies. This failure indicates that the system cannot connect to Symantec Synapse service. The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the <code>status_check</code> command to validate if there is connectivity with the Symantec servers. Verify the Symantec Endpoint Protection Manager database configuration, including the IP address, user name, password, and database name.</td>
<td>Report</td>
</tr>
<tr>
<td><strong>The system is unable to communicate with Synapse</strong></td>
<td>This failure indicates that the system cannot connect to Symantec Synapse service. The most likely cause is either that the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the <code>status_check</code> command to validate if there is connectivity with the Symantec servers.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td><strong>System is unable to communicate with Symantec Endpoint Protection Manager Database</strong></td>
<td>Verify the Symantec Endpoint Protection Manager database configuration, including the IP address, user name, password, and database name.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td><strong>Time server not configured on CIU, Synapse correlation will not work</strong></td>
<td>Configure a time server in ATP Manager.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td><strong>Update failure</strong></td>
<td>Restart the appliance and reapply the update. If the condition persists, contact Symantec Support.</td>
<td>Report</td>
</tr>
<tr>
<td>Message/Cause</td>
<td>Recommended action</td>
<td>Message location</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Device encountered an error during software update</td>
<td>Restart the appliance and reapply the update.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td></td>
<td>If the condition persists, contact Symantec Support.</td>
<td></td>
</tr>
<tr>
<td>Configuration failure</td>
<td>Restart the appliance and reapply the configuration change.</td>
<td>Report</td>
</tr>
<tr>
<td></td>
<td>If the condition persists, contact Symantec Support.</td>
<td></td>
</tr>
<tr>
<td>Persistent connection failures</td>
<td>This failure indicates that the system cannot connect to Symantec services.</td>
<td>Report</td>
</tr>
<tr>
<td></td>
<td>The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the status_check command to validate if there is connectivity with the Symantec servers.</td>
<td></td>
</tr>
<tr>
<td>Device is encountering persistent connection failures</td>
<td>This failure indicates that the system cannot connect to Symantec services.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td></td>
<td>The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the status_check command to validate if there is connectivity with the Symantec servers.</td>
<td></td>
</tr>
<tr>
<td>Unexpected shutdown</td>
<td>This failure can be due to a number of reasons, such as a power outage, or a restart or shutdown from the hardware switch. Typically, restarting the appliance from ATP Manager reconciles this state. Check the state of the node that shut down. Restart it if necessary, and check the state of services after powering it on.</td>
<td>Report</td>
</tr>
<tr>
<td>Message/Cause</td>
<td>Recommended action</td>
<td>Message location</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Device experienced an unexpected shutdown</td>
<td>This failure can be due to a number of reasons, such as a power outage, or a restart or shutdown from the hardware switch. Typically, restarting the appliance from ATP Manager reconciles this state. Check the state of the node that shut down. Restart it if necessary, and check the state of services after powering it on.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Persistent service failure</td>
<td>Restart the appliance. If the condition persists, contact Symantec Support.</td>
<td>Report</td>
</tr>
<tr>
<td>Device encountered service name service failure</td>
<td>Restart the appliance. If the condition persists, contact Symantec Support.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Content update failure</td>
<td>LiveUpdate was not able to run. The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the status_check command to validate if there is connectivity with the Symantec servers.</td>
<td>Report</td>
</tr>
<tr>
<td>Device failed to connect to Symantec for content updates</td>
<td>LiveUpdate was not able to run. The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the status_check command to validate if there is connectivity with the Symantec servers.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Error in retrieving component health status</td>
<td>Restart the appliance. If the condition persists, contact Symantec Support.</td>
<td>ATP Manager</td>
</tr>
</tbody>
</table>
### Table 7-1  System Is Critical messages (continued)

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection Manager</td>
<td><strong>connection error</strong>&lt;br&gt;Check the Symantec Endpoint Protection Manager server to see if it is up and running. Also, check the Symantec Endpoint Protection Manager connection configuration in <strong>Settings &gt; Global &gt; Endpoint Detection and Response</strong> to ensure that all entries are correct.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Symantec Endpoint Protection Manager</td>
<td><strong>authentication error</strong>&lt;br&gt;Check the Symantec Endpoint Protection Manager connection configuration in <strong>Settings &gt; Global &gt; Endpoint Detection and Response</strong> to ensure that all entries are correct.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Symantec Endpoint Protection Manager</td>
<td><strong>unknown error</strong>&lt;br&gt;Check the Symantec Endpoint Protection Manager server to see if it is up and running. Also, check the Symantec Endpoint Protection Manager connection configuration in <strong>Settings &gt; Global &gt; Endpoint Detection and Response</strong> to ensure that all entries are correct.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Device encountered maximum disk space usage</td>
<td><strong>(1 GB) by reports</strong>&lt;br&gt;This indicates that saved reports have consumed 100% of the 1 GB of disk space that is allocated for them. When this allocation is reached, ATP automatically purges reports to free up 10% of your disk space, beginning with the oldest to newest. You can also manually delete the reports that you no longer need.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Synapse Email correlation is malfunctioning</td>
<td><strong>please call support</strong>&lt;br&gt;This indicates that the Synapse Symantec Email Security.cloud Correlation feature experienced an Internal Server or Cloud Service error. Contact Symantec Support.</td>
<td>ATP Manager</td>
</tr>
</tbody>
</table>
### Table 7-1  System Is Critical messages (continued)

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synapse Email correlation is malfunctioning: please check configuration.</td>
<td>This indicates that ATP encountered an error when enabling Synapse Symantec Email Security.cloud Correlation. You can view the error in ATP Manager in the Synapse pane (<strong>Settings &gt; Global Settings</strong>)::&lt;br&gt;- <strong>Invalid user credentials. Please try again.</strong>  &lt;br&gt;Ensure that the user name and password of the Email Security.cloud user login account are valid in the Symantec Email and Web Security.Cloud portal.::&lt;br&gt;- <strong>The user does not have the required 'View Statistics' role. Please try again.</strong>  &lt;br&gt;Ensure the Email Security.cloud user login account has 'View Statistics' permissions in the Symantec Email and Web Security.Cloud portal.::&lt;br&gt;- <strong>This account does not have the required ATP ESS service. Please try again.</strong>  &lt;br&gt;Ensure that the <strong>Email Advanced Threat Protection</strong> service is enabled in the Symantec Email and Web Security.Cloud portal. You may have to contact your Symantec account representative.::&lt;br&gt;- <strong>Connection error</strong>  &lt;br&gt;Ensure that your firewall or enterprise proxy allows access to <a href="https://datafeedapi.symanteccloud.com">https://datafeedapi.symanteccloud.com</a> from your ATP management platform.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Certificate validation error</td>
<td>This indicates that ATP encountered an untrusted certificate on your network proxy.</td>
<td></td>
</tr>
</tbody>
</table>

*Table 7-2 lists the System Needs Attention messages and the recommended actions to correct the cause.*
<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update available</td>
<td>Update the software.</td>
<td>Report</td>
</tr>
<tr>
<td>Software update available</td>
<td>Update the software.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Lost contact</td>
<td>Verify that the appliance is up and running, and that the management platform can connect to that appliance.</td>
<td>Report</td>
</tr>
<tr>
<td>Device lost contact with CIU</td>
<td>Verify that the appliance is up and running, and that the management platform can connect to that appliance.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Intermittent connection failure</td>
<td>This failure indicates that the system cannot reliably connect to Symantec services. The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the <code>status_check</code> command to validate if there is connectivity with the Symantec servers.</td>
<td>Report</td>
</tr>
<tr>
<td>Device is encountering intermittent connection failures</td>
<td>This failure indicates that the system cannot reliably connect to Symantec services. The most likely cause is either the appliance management port is unable to reach the Internet, or the proxy configuration is incorrect. Use the <code>status_check</code> command to validate if there is connectivity with the Symantec servers.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Temporary service failure</td>
<td>A process failed, but was recovered. No action is necessary. However, if the condition reoccurs, it becomes a Critical event.</td>
<td>Report</td>
</tr>
<tr>
<td>Device encountered a service malfunction but has recovered</td>
<td>A process failed, but was recovered. No action is necessary. However, if the condition reoccurs, it becomes a Critical event.</td>
<td>ATP Manager</td>
</tr>
</tbody>
</table>
### System Needs Attention messages (continued)

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device is encountering a low resource condition</td>
<td>No action is necessary unless this condition persists. If it does, restart the appliance. If the situation occurs, contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Content update error</td>
<td>The appliance is able to connect to LiveUpdate but is unable to retrieve the latest content for one of the content types. This situation typically resolves itself over time. If the problem persists, contact Symantec Support.</td>
<td>Report</td>
</tr>
<tr>
<td>Device encountered a problem retrieving some content</td>
<td>The appliance is able to connect to LiveUpdate but is unable to retrieve the latest content for one of the content types. This situation typically resolves itself over time. If the problem persists, contact Symantec Support.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Device is encountering high CPU usage</td>
<td>This may indicate a temporary heavy load on the appliance. If the situation continues for a long period of time, restart the appliance. If it is a recurring situation, contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Device is encountering high RAM usage</td>
<td>This may indicate a temporary heavy load on the appliance. If the situation continues for a long period of time, restart the appliance. If it is a recurring situation, contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Device is encountering low disk space on root drive</td>
<td>Contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Device is encountering low disk space on /var drive</td>
<td>This may be due to the database becoming too large. You can attempt to purge data to see if that addresses the issue (you may want to perform a backup first). If that does not address the situation, contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Device is encountering low disk space on /var/log drive</td>
<td>Contact Symantec Support.</td>
<td>Report and ATP Manager</td>
</tr>
</tbody>
</table>
### Table 7-2  System Needs Attention messages (continued)

<table>
<thead>
<tr>
<th>Message/Cause</th>
<th>Recommended action</th>
<th>Message location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device is encountering low disk space on /tmp drive</td>
<td>This condition may be due to reports or other temporary files which can be deleted. First, delete any stored reports which are no longer needed. If the situation persists, use the list command to see what files are in the temp area and consider deleting the files that are not needed.</td>
<td>Report and ATP Manager</td>
</tr>
<tr>
<td>Symantec Endpoint Protection Manager connection disabled</td>
<td>Check the Symantec Endpoint Protection Manager server to see if it is up and running. Also, check the Symantec Endpoint Protection Manager connection configuration in Settings &gt; Global &gt; Endpoint Detection and Response to ensure that all entries are correct.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Symantec Endpoint Protection Manager connection pending</td>
<td>Wait for a period while the connection to Symantec Endpoint Protection Manager is established. If the condition persists, check the Symantec Endpoint Protection Manager connection configuration in Settings &gt; Global &gt; Endpoint Detection and Response to ensure that all entries are correct.</td>
<td>ATP Manager</td>
</tr>
<tr>
<td>Device is encountering high disk space usage by reports</td>
<td>This indicates that saved reports have consumed 90% of the 1 GB of disk space that is allocated for them. When 100% of this allocation is reached, ATP automatically purges reports to free up 10% of your disk space, beginning with the oldest to newest. You can wait for this purge to occur, or you can manually delete the reports that you no longer need.</td>
<td>ATP Manager</td>
</tr>
</tbody>
</table>
Searching logs

This chapter includes the following topics:

- About Logging
- Searching the System Activity log

About Logging

Symantec Advanced Threat Protection (ATP) collects information about the activities that occur in your environment. It stores this information in the form of events, which are comprised of various fields that contain information about each event. These events are stored in logs.

In ATP, you can search the following logs for events based on queries that you create, or by using predefined Quick Filters:

- **Actions**
  You can view the status of the asynchronous actions that are taken on entities through ATP Manager as well as actions take through the API.

- **System Activity**
  The events in these logs pertain to the state of your ATP software, the hardware in your environment, and actions that were initiated by your users or by ATP itself. Searching these logs can help you troubleshoot system health issues.
  See “Searching the System Activity log” on page 131.

Searching the System Activity log

The System Activity log collects information about system-related activities that occur in your environment. It stores this information in the form of events, which are comprised of various fields that contain information about each event. In Symantec Advanced Threat Protection (ATP), you can search the System Activity log for events based on queries that you create, or by using predefined Quick Filters.
Searches can help you troubleshoot system health issues. They can also help you identify activities that were initiated by an ATP, user or by ATP itself.

**The types of System Activity events**

The System Activity logs include two types of events:

<table>
<thead>
<tr>
<th>System Health</th>
<th>These events pertain to the overall state of your ATP software, and the hardware that is in your network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Activity</td>
<td>These events pertain to:</td>
</tr>
<tr>
<td>■ Actions that your users initiated in ATP Manager. These actions include generating reports, performing and canceling searches, issuing commands, and so on.</td>
<td></td>
</tr>
<tr>
<td>■ Actions that ATP initiated. These actions include backing up your data, upgrading your ATP software, updating your content (such as LiveUpdate virus definitions), and so on.</td>
<td></td>
</tr>
</tbody>
</table>

**Working in the System Activity log**

Any user can perform a search from the Logging > System Activity page.

On the System Activity page, you can:

■ Search for activity based on a query that you create
■ Search for activity using Quick Filters
■ Refine your search results based on a time filter
■ Export your search results to a .CSV text file

---

**Note:** ATP Manager displays a maximum of 500 records in the Events Summary. However, ATP includes up to 10,000 records when you export them to a .CSV text file.

■ Expand an event to get additional information
■ Add and remove columns to the Event Summary

Click the following link to learn more about how to work in the Events Summary.

The Events Summary displays information for each event for the fields (columns) that are listed in Table 8-1.

**Table 8-1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time (in UTC format) when the event was logged.</td>
</tr>
</tbody>
</table>
Table 8-1  
(continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type_id</td>
<td>The type of event:</td>
</tr>
<tr>
<td></td>
<td>■ 1 = Application Activity</td>
</tr>
<tr>
<td></td>
<td>■ 2 = System Health</td>
</tr>
<tr>
<td>severity_id</td>
<td>The severity of the event:</td>
</tr>
<tr>
<td></td>
<td>■ 1 = informational</td>
</tr>
<tr>
<td></td>
<td>■ 2 = warning</td>
</tr>
<tr>
<td></td>
<td>■ 3 = minor</td>
</tr>
<tr>
<td></td>
<td>■ 4 = major</td>
</tr>
<tr>
<td></td>
<td>■ 5 = critical</td>
</tr>
<tr>
<td></td>
<td>■ 6 = fatal</td>
</tr>
<tr>
<td>message</td>
<td>The message associated with the event.</td>
</tr>
<tr>
<td>device_ip</td>
<td>The IP address of the ATP appliance that generated the event.</td>
</tr>
<tr>
<td>atp_node_role</td>
<td>The role of the ATP appliance that generated the event:</td>
</tr>
<tr>
<td></td>
<td>■ 0 = Pre-Bootstrap</td>
</tr>
<tr>
<td></td>
<td>■ 1 = Network Scanner</td>
</tr>
<tr>
<td></td>
<td>■ 2 = Management</td>
</tr>
<tr>
<td></td>
<td>■ 3 = Standalone Network</td>
</tr>
<tr>
<td></td>
<td>■ 4 = Standalone Endpoint</td>
</tr>
<tr>
<td></td>
<td>■ 5 = All in One</td>
</tr>
</tbody>
</table>
Updating the software

This chapter includes the following topics:

- About software updates
- Updating ATP software

About software updates

Symantec Advanced Threat Protection (ATP) software updates for improved performance, functionality, enhancements, or security for the appliance are available from Symantec under any of these circumstances:

- A patch or upgrade release
- A Symantec component or third-party library update
- An operating system update

The appliance automatically checks for updates daily. Update availability appears in ATP Manager on the Settings > Appliances page. You can also configure an email to be sent when an update is available. If a software update is available, the system shows a yellow status of System Needs Attention; mousing over the message displays a pop-up message that an update is available.

Note: The Update Software option may not appear until 24-48 hours after the update is made publically available.

You can update ATP in ATP Manager or using the CLI.

See “update command” on page 152.

Each device must be updated separately. The management platform must be updated first, followed by the network scanners. When you update an all-in-one appliance or management platform, make sure that you back up the appliance first.
Updates require ATP to be taken offline. Never restart or shutdown the appliance during an update. The appliance restarts itself after the update.

See “Updating ATP software” on page 135.

## Updating ATP software

Before you begin the Symantec Advanced Threat Protection (ATP) software update, make sure that you back up the management platform or all-in-one appliance.

### To update the ATP software in ATP Manager

1. In ATP Manager, click **Settings > Appliances**.
2. Click the **Update Software** option for the device that you want to update.

   The management platform must be updated first. Once it is updated, you can initiate updates for each of the network scanners from ATP Manager.

   An update can take some amount of time. The appliance automatically restarts when an update is completed. If an error occurs during the update process, you can use the `update status` command in the command line interface to find out more information about the status of the last performed update.

### To update the ATP software using the CLI

- On the management platform or all-in-one appliance, run the `update` command with desired options.

  For example, to update to the latest version of ATP software, enter:

  ```
  update install
  ```

  **Note:** You can use the `status` option of the `update` command to obtain the status of a currently running update, or if the update is completed (or terminated) the status of the last performed update is provided.

See “Using the ATP command-line interface” on page 142.

See “About software updates” on page 134.
Updating the appliance

This chapter includes the following topics:

- Adding a scanner in your configuration
- Re-imaging a physical appliance
- Reinstalling a virtual appliance

Adding a scanner in your configuration

As your system operates over time, you may need to add network scanners to protect additional networks. To add a network scanner to an existing Symantec Advanced Threat Protection (ATP) management platform/network scanner configuration, install the new scanner as you would any other physical or virtual appliance. During bootstrap, you specify all the information the network scanner needs to establish a connection to the management platform.

After bootstrap is complete and the network scanner restarts, the management platform downloads the default configuration to the network scanner. When this download is complete, the new network scanner appears in ATP Manager. You can then customize the Appliances settings for the network scanner and enable scanning.

Note: If the network scanner does not appear in ATP Manager within 10 minutes after bootstrap completes, check the network connections. If the connections are correct, re-run bootstrap to ensure that you entered the correct gateway address, management platform IP address, and communications channel password.

Re-imaging a physical appliance

Symantec Advanced Threat Protection (ATP) physical appliances are shipped with the operating system already installed. If you need to reinstall the operating system, use the following procedure to re-image the drive from an ISO file.
ISO files are maintained on the Symantec FileConnect site. You need your maintenance serial number to access FileConnect and download the ISO file. You can find your serial number on the license certificate you received with your initial purchase or on a Version Upgrade Notification. If you need help locating your serial number, contact Symantec Customer Care.

To re-image a physical appliance

1. Download the ISO file from https://fileconnect.symantec.com and burn this file to a DVD.
2. Insert the DVD into the DVD drive on the appliance.
3. Restart the appliance.
   The appliance restarts from the DVD and begins the re-image process automatically. The entire sequence may take 10 minutes or more. When the process is complete, the appliance console displays.
4. Bootstrap the appliance. If you are replacing a management platform, ensure that you use the same IP address and communications password as you assigned to the old management platform. If you change the IP address or password, you must run bootstrap again on all the network scanners.
5. If the re-imaged device is an all-in-one appliance or management platform, run the setup wizard.
6. If the re-imaged device is a network scanner, wait for the scanner to appear on the Appliances page in ATP Manager.
   See “Adding a scanner in your configuration” on page 136.
7. Complete setup tasks as you would for a new appliance.
   See “Completing setup tasks” on page 19.
8. If you re-imaged a network scanner, run the restore command to restore the incident data from the last backup.
   See “Using the ATP command-line interface” on page 142.

Reinstalling a virtual appliance

To reinstall a Symantec Advanced Threat Protection (ATP) virtual appliance, you delete the old appliance and deploy the OVF file again.

Note: Reinstalling a virtual appliance from an ISO image is not supported.

OVF files are maintained on the Symantec FileConnect site. You need your maintenance serial number to access FileConnect and download the OVF file. You can find your serial number
To reinstall a virtual appliance

2. In VMWare VSphere™ Client, deploy the OVF.
3. Open a console window and bootstrap the appliance. If you are replacing a management platform, ensure that you enter the same IP address and communications channel password during bootstrap. If you change the management port IP address or communications channel password on a management platform, you must run bootstrap again on each scanner to update this information.
4. If the reinstalled device is an all-in-one appliance or management platform, run the setup wizard.
   If the reinstalled device is a network scanner, wait for the scanner to appear on the Appliances page in ATP Manager.
   See “Adding a scanner in your configuration” on page 136.
5. Complete setup tasks as you would for a new appliance.
   See “Completing setup tasks” on page 19.
6. If you replaced a network scanner, run the restore command to restore the incident data from the last backup.
   See “Using the ATP command-line interface” on page 142.
Ports, connectors, and indicators on the appliance

This appendix includes the following topics:

- About appliance ports, connectors, and indicators

About appliance ports, connectors, and indicators

Table A-1 describes the ports, connectors, and indicators on the back of Symantec Advanced Threat Protection (ATP) appliances.

<table>
<thead>
<tr>
<th>Port, connector, or indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB port</td>
<td>You can use this port to attach a keyboard or a mouse to use for the command-line interface.</td>
</tr>
<tr>
<td>VGA port</td>
<td>You can use this port for a monitor.</td>
</tr>
</tbody>
</table>
| WAN/Monitor1 Ethernet port (ATP 8840)        | In tap mode, connect the Monitor1 port to the network tap device or a monitoring port on a switch for SPAN.  
|                                               | In inline mode, connect the WAN port to a switch toward your Internet connection or to your firewall. |
| LAN/Monitor2 Ethernet port (ATP 8840)        | In tap mode, you may connect the Monitor2 port to the network tap device or a monitoring port on a switch for SPAN.  
|                                               | In inline mode, connect the LAN port to a switch that is connected to your internal network. |
In tap mode, connect the Monitor1 port to the network tap device or a monitoring port on a switch for SPAN. In inline mode, connect the WAN1 port to a switch toward your Internet connection or to your firewall.

<table>
<thead>
<tr>
<th>Port, connector, or indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN1/Monitor1 Ethernet port (ATP 8880)</td>
<td>In tap mode, connect the Monitor1 port to the network tap device or a monitoring port on a switch for SPAN. In inline mode, connect the WAN1 port to a switch toward your Internet connection or to your firewall.</td>
</tr>
<tr>
<td>LAN1/Monitor2 Ethernet port (ATP 8880)</td>
<td>In tap mode, you may connect the Monitor2 port to the network tap device or a monitoring port on a switch for SPAN. In inline mode, connect the LAN1 port to a switch that is connected to your internal network.</td>
</tr>
<tr>
<td>WAN2/Monitor3 Ethernet port (ATP 8880)</td>
<td>In tap mode, you may connect the Monitor3 port to the network tap device or a monitoring port on a switch for SPAN. In inline mode, connect the WAN2 port to a switch toward your Internet connection or to your firewall.</td>
</tr>
<tr>
<td>LAN2/Monitor4 Ethernet port (ATP 8880)</td>
<td>In tap mode, you may connect the Monitor4 port to the network tap device or a monitoring port on a switch for SPAN. In inline mode, connect the LAN2 port to a switch that is connected to your internal network.</td>
</tr>
<tr>
<td>Management (Mgmt) Ethernet port</td>
<td>Connect the management port to a switch that is connected to your internal network. The management port must have access to the following: ■ Domain Name Server (DNS) ■ Required Internet services</td>
</tr>
<tr>
<td>Power</td>
<td>This connector provides power to the appliance. Your appliance may have an extra, redundant power connector.</td>
</tr>
<tr>
<td>iDRAC Ethernet port</td>
<td>You can connect the iDRAC port to a port on a switch or to a PC during initial bring up.</td>
</tr>
<tr>
<td>Bypass NIC LED indicators</td>
<td>There are three pairs of LED indicators on the bypass NIC card. The Link/Activity pair is solid green, and blinks green on activity when bypass mode is off. It is off when bypass mode is on. The Bypass pair is solid green when the appliance is running in bypass mode, and is off when bypass mode is off. The DISC pair is always off (not used).</td>
</tr>
</tbody>
</table>
Using the command-line interface

This appendix includes the following topics:

- Using the ATP command-line interface
- Opening the console window on a physical or virtual appliance
- backup command
- bootstrap command
- data_inspection_stat command
- delete command
- edrfeature command
- exportfdr command
- getpcap command
- grep command
- help command
- list command
- ntpsync command
- password command
- pieconfig command
- reboot command
Using the ATP command-line interface

Each Symantec Advanced Threat Protection (ATP) appliance (physical or virtual) has a set of commands that you can use to administer the product. The commands include standard Linux commands, plus ATP-specific Linux commands. You execute these commands from the system console.

On physical appliances, you can access the system console by using:

- A VGA monitor and keyboard connected directly to the appliance
- A virtual terminal accessible from the iDRAC

On virtual appliances, the system console is the VMware console.

If you use the `sshconfig enable` command, you can connect using ssh to physical or virtual systems.

See “Opening the console window on a physical or virtual appliance” on page 143.

The following standard Linux commands are supported and have not been modified for ATP:

- `cat`
- `clear`
- `date`
- `df`
- `dig`
- `ifconfig`
- `iostat`
- `ip`
Opening the console window on a physical or virtual appliance

During initial setup of the physical or virtual Symantec Advanced Threat Protection (ATP) appliance, you run bootstrap (and all other command-line utilities) from a console window.

To open the console window on a physical appliance

1. Press the power button on the front of the appliance.
   The appliance takes several minutes to start.

2. Launch a supported browser and type: `https://<static IP address of the iDRAC>` into the address line.
   For example, if you assigned the address 10.10.10.10 to the iDRAC, type `https://10.10.10.10` into the address line.

3. On the logon screen, type the ID `root` and the password that you assigned to the iDRAC.

4. In the Integrated Remote Access Controller window, click the Virtual Console Preview window, or click the Launch Console link under this window.

To open a console window on a virtual appliance

1. Make sure that the virtual appliance is powered on.

2. Right-click the virtual appliance and choose Open Console.

Refer to the VMware documentation for complete information.

- `less`
- `more`
- `nslookup`
- `netstat`
- `ping`
- `ping6`
- `route`
- `tail`
- `tcpdump`
- `traceroute`
- `traceroute6`
backup command

Description: Back up incident data on a management platform or on an all-in-one physical or virtual appliance.

Synopsis:

```
```

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Display the help for backup command and exit.</td>
</tr>
<tr>
<td>--debug</td>
<td>Provide extra output for troubleshooting.</td>
</tr>
<tr>
<td>--encrypt</td>
<td>Produce an encrypted backup archive (specify yes or no).</td>
</tr>
<tr>
<td>--host=</td>
<td>Specify the remote storage host.</td>
</tr>
<tr>
<td>--user=</td>
<td>Specify the user name for authentication with the remote machine, for example, FTP user or SSH user, depending on the chosen protocol.</td>
</tr>
<tr>
<td>--password=</td>
<td>Specify the password of the user for authentication with the remote machine, for example, the FTP user password or the SSH user password, depending on the chosen protocol. If SSH is chosen as the protocol and SSH public key authentication is selected, this password protects the RSA private key.</td>
</tr>
<tr>
<td>--path=</td>
<td>Specify a directory on the remote storage host.</td>
</tr>
<tr>
<td>--protocol=</td>
<td>Specify the protocol to transport backup data: FTP or SCP. <strong>Note:</strong> Specify the protocol name in lowercase characters.</td>
</tr>
<tr>
<td>--port=</td>
<td>Specify the port that the protocol uses. Use 21 for FTP, 22 for SCP.</td>
</tr>
<tr>
<td>--localuser=</td>
<td>Specify the local user name if SSH public key authentication is desired, as opposed to password authentication. Only applicable to SCP protocol.</td>
</tr>
<tr>
<td>--test</td>
<td>Verify remote backup mechanism works. This option transfers a test file to the remote storage with the specified options, but not with the actual backup data. If the test is successful, a message with a result of 0 is displayed. A result other than 0 means the test failed. The test file is automatically deleted.</td>
</tr>
</tbody>
</table>
bootstrap command

Description: Start the bootstrap process on a physical or virtual appliance. The bootstrap process starts automatically when you open a console window to the appliance after initial installation, and restarts the appliance after you finish. If you subsequently run `bootstrap` from the command line, your changes take effect and services are restarted, but the appliance does not restart automatically.

Synopsis: `bootstrap`

Option or argument: Not applicable.

data_inspection_stat command

Description: Get packet inspection statistics.

Synopsis: `data_inspection_stat [-s] [-i wan1_tap1 | lan1_tap2 | wan2_tap3 | lan2_tap4 -d 1 | 2]`

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Display packet inspection statistics.</td>
</tr>
<tr>
<td>-i &lt;interface&gt;</td>
<td>Specify the interface to display statistics for: <code>wan1_tap1</code>, <code>lan1_tap2</code>, <code>wan2_tap3</code>, or <code>lan2_tap4</code>.</td>
</tr>
<tr>
<td>-d 1</td>
<td>2</td>
</tr>
</tbody>
</table>

delete command

Description: Delete the certain files that can be shown with the `list` command.

Synopsis: `delete </path/filename>`

Option or argument: `</path/filename>`

edrfeature command

Description: Enable or disable the endpoint detection and response (EDR) feature in ATP or verify the current status of EDR.

Synopsis: `edrfeature <status/enable/disable>`

Option or argument: `<status/enable/disable>`
**exportfdr command**

Description: The `exportfdr` command is an extension of the `backup` command which exports a full endpoint data recorder dump from the ATP database. The output is a compressed file that contains an Elasticsearch snapshot of a single index that contains the full dump. You view this data using the Elasticsearch snapshot restore API. The following is a link to the Elasticsearch website explaining perform this task:


Synopsis:


<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Display the help for <code>exportfdr</code> command and exit.</td>
</tr>
<tr>
<td>--debug</td>
<td>Provide extra output for troubleshooting.</td>
</tr>
<tr>
<td>--encrypt</td>
<td>Produce an encrypted archive (specify <code>yes</code> or <code>no</code>).</td>
</tr>
<tr>
<td>--host=</td>
<td>Specify the remote storage host. Specify the IP address — not the host name.</td>
</tr>
<tr>
<td>--user=</td>
<td>Specify the user name for authentication with the remote machine, for example, ftp user or ssh user, depending on the chosen protocol.</td>
</tr>
<tr>
<td>--password=</td>
<td>Specify the password of the user for authentication with the remote machine, for example, the FTP user password or the SSH user password, depending on the chosen protocol. If SSH is chosen as the protocol and SSH public key authentication is selected, this password protects the RSA private key.</td>
</tr>
<tr>
<td>--path=</td>
<td>Specify a directory on the remote storage host.</td>
</tr>
<tr>
<td>--protocol=</td>
<td>Specify the protocol to transport backup data: FTP or SCP. <strong>Note</strong>: Specify the protocol name in lowercase characters.</td>
</tr>
<tr>
<td>--port=</td>
<td>Specify the port that the protocol uses. Use 21 for FTP, 22 for SCP.</td>
</tr>
<tr>
<td>--localuser=</td>
<td>Specify the local user name if SSH public key authentication is desired, as opposed to password authentication. Only applicable to SCP protocol.</td>
</tr>
</tbody>
</table>
Option or argument | Description
--test | Verify remote that the export mechanism works. This option transfers a test file to the remote storage with the specified options, but not with the actual export data. If the test is successful, a message with a result of 0 appears. A result other than 0 means the test failed. The test file is automatically deleted.

getpcap command

Description: Copy *.pcap files from /home/admin on an ATP appliance to a remote host running sshd. A .pcap file is a text file output from the tcpdump command, and can be used to analyze tcp/ip traffic.

Synopsis: getpcap $<user>@$<host>:$<path>

Option or argument | Description
$<user> | Specify a user on a remote host. You are prompted to enter the password for that user.
$<host> | Specify the host name, FQDN, or IP address of the remote host.
$<psth> | Specify the path on the remote host for the .pcap files.

grep command

Description: Operate only on the files that are visible to the admin user.

Synopsis: Standard Linux synopsis for grep.
Option or argument: Standard Linux options or arguments for grep.

help command

Description: Display help for <command>. If no command is specified, show commands available.

Synopsis: help [command]
Option or argument: command
list command

Description: List certain files.

[--help]

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--all, -a</td>
<td>List all files.</td>
</tr>
<tr>
<td>--cores, -c</td>
<td>List core files.</td>
</tr>
<tr>
<td>--home, -m</td>
<td>Display the names of files that can be viewed with cat, tail, or more, or deleted with delete.</td>
</tr>
<tr>
<td>--logs, -l</td>
<td>Display the names of files in /home/admin.</td>
</tr>
<tr>
<td>--siege, -s</td>
<td>List log files.</td>
</tr>
<tr>
<td>--temp, -p</td>
<td>List siege files.</td>
</tr>
<tr>
<td>--top, -t</td>
<td>List temporary files.</td>
</tr>
<tr>
<td>--top, -t</td>
<td>List the largest files that can be deleted, and their sizes.</td>
</tr>
</tbody>
</table>

ntpsync command

Description: Force synchronization with the NTP server.

Synopsis: ntpsync

Option or argument: Not applicable.

password command

Description: Set or reset the password for the admin user.

Synopsis: password [--help] [--reset]

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help, -h</td>
<td>Show more extensive help.</td>
</tr>
<tr>
<td>--reset, -r</td>
<td>Reset the password to the factory default.</td>
</tr>
</tbody>
</table>
pieconfig command

Description: If you have a proxy server deployed as an enterprise proxy, specify whether the Packet Inspection Engine (PIE) should inspect internal or external network traffic.

Synopsis: pieconfig internal_proxy | external_proxy | proxy

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal_proxy</td>
<td>Inspect the traffic that flows from the internal network to the proxy.</td>
</tr>
<tr>
<td>external_proxy</td>
<td>Inspect the traffic that flows from the proxy to the external network.</td>
</tr>
<tr>
<td>proxy</td>
<td>List the traffic that is being inspected.</td>
</tr>
</tbody>
</table>

reboot command

Description: Restart the host.

Synopsis: reboot [--force] [--help]

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force, -f</td>
<td>Force a restart. Not recommended during a software update.</td>
</tr>
<tr>
<td>--help, -h</td>
<td>Show more extensive help.</td>
</tr>
</tbody>
</table>

restore command

Description: Retrieve a backup file and restore it on a CIU or on a standalone physical or virtual appliance.

Synopsis:

```
```

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--debug</td>
<td>Provide extra output for troubleshooting.</td>
</tr>
<tr>
<td>--filename=</td>
<td>Specify the backup file name to be restored.</td>
</tr>
<tr>
<td>--help</td>
<td>Display the help for restore and exit.</td>
</tr>
</tbody>
</table>
Option or argument | Description
--- | ---
--host= | Specify the remote storage host.
--localuser= | Specify the local user name if SSH public key authentication is desired, as opposed to password authentication. Only applicable to SCP protocol.
--password= | Specify the password of the user for authentication with the remote machine, for example, the ftp user password or the ssh user password, depending on the chosen protocol. If SSH is chosen as the protocol and SSH public key authentication is selected, this password protects the RSA private key.
--path= | Specify a directory on the remote storage host.
--port= | Specify the port that the specified protocol uses. Use 21 for FTP, 22 for SCP.
--protocol= | Specify the protocol to transport backup data: ftp or scp.
Note: Specify the protocol name in lowercase characters.
--user= | Specify the user name that is used to transport backup from the remote machine, for example, ftp user or ssh user, depending on the chosen protocol.

See “About backing up and restoring ATP data” on page 57.

show command

Description: Display system information.

Synopsis: show [--date] [--help] [--info] [--version]

Option or argument | Description
--- | ---
--date, -d | Display the current date and time.
--help, -h | Display the show man page.
--info, -i | Display system information, such as Service Tag, total memory, and disk size.
--version, -v | Display the appliance software version number.
shutdown command
Description: Shut down the host.
Synopsis: `shutdown [--force] [--help]

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force, -f</td>
<td>Force a shutdown. Not recommended during a software update.</td>
</tr>
<tr>
<td>--help, -h</td>
<td>Show more extensive help.</td>
</tr>
</tbody>
</table>

sshconfig command
Description: Start or stop SSH service.
Synopsis: `sshconfig enable | disable`

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Start the SSH service immediately and configure the system to start SSH on boot.</td>
</tr>
<tr>
<td>disable</td>
<td>Stop the SSH service immediately and configure the system to disable SSH on boot.</td>
</tr>
</tbody>
</table>

status_check command
Description: Check system status and server connectivity, such as management port status, interface status, and connectivity to Symantec servers in the cloud.
Synopsis: `status_check`
Option or argument: Not applicable.

Note: By default, Cynic attempts to contact the closest server to the submitting computer's location unless you enable the option to use the U.K. Cynic Server on the Settings > Global page.
Default Cynic server: https://api.us.dmas.symantec.com
U.K. Cynic server: https://api.eu.dmas.symantec.com

tcp_check command
Description: Test the connectivity to a server inside the client environment.
Synopsis: tcp_check [--ip_address] [--port]

Option or argument | Description
--- | ---
--ip_address | Specify the IP address of the server you want to check connectivity with.
--port | Specify the port number of the server you want to check connectivity with.

**update command**

Description: Invoke a software update.

Synopsis: update clean_all | clean_metadata | clean_packages | download | install | list | rpmdb_repair | status

**Note:** A notification is sent to ATP Manager once an update download is complete. You must modify the atp_schedule setting in the MariaDB to receive this notification.

<table>
<thead>
<tr>
<th>Option or argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clean_all</td>
<td>Perform clean_metadata and clean_packages.</td>
</tr>
<tr>
<td>clean_metadata</td>
<td>Remove any cached data that is related to the software repository.</td>
</tr>
<tr>
<td>clean_packages</td>
<td>Undo update download and remove any cached packages.</td>
</tr>
<tr>
<td>download</td>
<td>Download the latest version of ATP software.</td>
</tr>
<tr>
<td>install</td>
<td>Update to the latest version of ATP software.</td>
</tr>
<tr>
<td>list</td>
<td>Display available versions of ATP software.</td>
</tr>
<tr>
<td>rpmdb_repair</td>
<td>Remove any lock files that might remain if a software update was interrupted.</td>
</tr>
<tr>
<td>status</td>
<td>Display the status of the update command. If the update is currently progressing, the status is given for the current update. If the update has completed or terminated, the status is given for the last attempted update.</td>
</tr>
</tbody>
</table>

**Restoring data from a backup file using command-line**

Restore your Symantec Advanced Threat Protection (ATP) backups using the command-line interface.
To restore data from a backup file using the CLI

- On the management platform or all-in-one appliance, run the `restore` command with the desired options.

For example, to restore data from a directory on a remote server using FTP, type:

```
restore --host=(hostname) --protocol=ftp --port=21 --user=(username)
--password=(password) --path=<directory> --filename=<backup archive name>
--ignorerunningcommands (ignore the warning prompt for in-progress commands detected when performing the restore)
```

---

**Warning:** ATP checks to see if there are any endpoint searches that are currently in progress when you begin a restore. If so, ATP displays a warning along with the option to either continue with, or cancel, the restore. If you continue with the restore, the results of those searches are added to your restored data when those searches are complete. (Depending on the availability of the endpoints, this may take several days.) However, you will not be able to access the results of those searches because their Search Descriptions are overridden when the restore is complete.

It is therefore recommended that you cancel the restore, cancel the searches in ATP Manager, and then begin the restore again.

---

When you perform a restore, ATP logs an event in the System Activity Log that lists the start and end time of the restore, its success or failure, the files it restored, etc.

See “Using the ATP command-line interface” on page 142. for more information on the options for the restore command.

See “About backing up and restoring ATP data” on page 57.
System Requirements

This appendix includes the following topics:

- System requirements for ATP integration with Symantec Endpoint Protection management interfaces and embedded databases

System requirements for ATP integration with Symantec Endpoint Protection management interfaces and embedded databases

Symantec Advanced Threat Protection (ATP) can integrate with Symantec™ Endpoint Protection for enhancing event information and providing Endpoint Detection and Response (EDR) functionality. ATP has certain version requirements based on various components of Symantec Endpoint Protection.

The minimum Symantec Endpoint Protection Manager version is 12.1 RU6 or later. ATP can connect to multiple Symantec Endpoint Protection sites, but ATP only supports up to ten connections to Symantec Endpoint Protection Manager hosts and one connection per Symantec Endpoint Protection site.

ATP can manage client endpoints that run Symantec Endpoint Protection version 12.1 RU 6 MP3 or later with full EDR functionality. Client endpoints that run versions earlier than Symantec Endpoint Protection 12.1 RU5 are not supported. If your environment includes clients that run a version between Symantec Endpoint Protection 12.1 RU5 and 12.1 RU6 MP3, some functionality may be limited depending upon the version of the client. The ATP documentation has descriptions for the specific functions that are limited by the version of the Symantec Endpoint Protection client.

Symantec Endpoint Protection Manager can store logs either in an internal embedded database or in an external Microsoft SQL Server database. ATP can access external Microsoft SQL Server database without any special host system requirements. When Symantec Endpoint Protection Manager uses an embedded database, ATP uses a log collector on the Symantec
Endpoint Protection Manager host. This log collector requires the Symantec Endpoint Protection Manager host to be running one of the following operating systems:

- Windows 7 (64-bit only)
- Windows 8 (64-bit only)
- Windows Server 2008
- Windows Server 2012
- Windows Server 2012 R2 or later (recommended)

See the Symantec Endpoint Protection documentation for Symantec Endpoint Protection Manager system requirements.
Required Firewall Ports

This appendix includes the following topics:

- Required firewall ports

Required firewall ports

Depending on your network layout, you may need to open some ports on your firewall and edit your firewall rules to allow certain Web addresses that are essential for Symantec Advanced Threat Protection (ATP) operations.

Table D-1 lists the Web and IP addresses to which ATP require access.

<table>
<thead>
<tr>
<th>Web addresses/IP Address</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>licensing.dmas.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to get the Cynic license</td>
</tr>
<tr>
<td>api.us.dmas.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to perform queries to the Cynic US and UK servers (required)</td>
</tr>
<tr>
<td>api.eu.dmas.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to perform queries to the Cynic US and UK servers (required)</td>
</tr>
<tr>
<td>liveupdate.symantec.com</td>
<td>TCP</td>
<td>80</td>
<td>Used to check for and download definitions for Symantec's detection technologies</td>
</tr>
<tr>
<td>ratings-wrs.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to query Norton Safe Web server to identify malicious websites</td>
</tr>
<tr>
<td>stnd-avpg.crsi.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to send detection telemetry to Symantec</td>
</tr>
<tr>
<td>stnd-ipsg.crsi.symantec.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to send detection telemetry to Symantec</td>
</tr>
<tr>
<td>register.brightmail.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to register the ATP appliance</td>
</tr>
</tbody>
</table>
### Table D-1  ATP Web and IP addresses (continued)

<table>
<thead>
<tr>
<th>Web addresses/IP Address</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>swupdate.brightmail.com</code></td>
<td>TCP</td>
<td>443</td>
<td>Used to check for and download new releases of ATP</td>
</tr>
<tr>
<td><code>shasta-rrs.symantec.com</code></td>
<td>TCP</td>
<td>443</td>
<td>Used to perform reputation lookups for Windows executable and APK installable files</td>
</tr>
<tr>
<td><code>shasta-mrs.symantec.com</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>datafeedapi.symanteccloud.com</code></td>
<td>TCP</td>
<td>443</td>
<td>Used to download ATP:Roaming and Email Security.cloud events</td>
</tr>
<tr>
<td><code>stats.norton.com</code></td>
<td>TCP</td>
<td>443</td>
<td>If configured, used to send statistics telemetry to Symantec</td>
</tr>
<tr>
<td><code>telemetry.symantec.com</code></td>
<td>TCP</td>
<td>443</td>
<td>If configured, used to send file telemetry and to upload diagnostic packages to Symantec</td>
</tr>
<tr>
<td><code>synapse.symantec.com</code></td>
<td>TCP</td>
<td>443</td>
<td>If configured, used to send Synapse telemetry</td>
</tr>
<tr>
<td><code>198.6.48.16</code></td>
<td>TCP</td>
<td>443</td>
<td>If configured, used to send Synapse telemetry. (The server is accessed via an IP address and not a domain.)</td>
</tr>
</tbody>
</table>

Table D-2 describes the ports that ATP uses for communications, content updates, and interactions with Symantec.cloud detection services.

### Table D-2  ATP ports and settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up</td>
<td>FTP; SSH</td>
<td>20 TCP, UDP</td>
<td>Management platform or all-in-one appliances</td>
<td>Configured backup storage server (Internal traffic)</td>
<td>FTP server: FTP ports 20, 21. SSH server: SSH port 22.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21 TCP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>22 TCP, UDP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email notifications</td>
<td>SMTP</td>
<td>25 TCP</td>
<td>Management platform or all-in-one appliance</td>
<td>SMTP server (Internal traffic)</td>
<td>Communication with the SMTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>587 TCP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Content updates</td>
<td>HTTP</td>
<td>80 TCP</td>
<td>All appliances</td>
<td>Symantec (External traffic)</td>
<td>Virus and Vantage definitions, and other content that LiveUpdate delivers. This is required for proper functioning of the product.</td>
</tr>
<tr>
<td>Statistics delivery</td>
<td>HTTP</td>
<td>80 TCP</td>
<td>All appliances</td>
<td>Symantec (External traffic)</td>
<td>Sends data to Symantec for statistical and diagnostic purposes. Private data is not sent over this port.</td>
</tr>
<tr>
<td>Endpoint detection and response (EDR) 2.0</td>
<td>HTTPS</td>
<td>443</td>
<td>Symantec Endpoint Protection</td>
<td>ATP management platform</td>
<td>Endpoint searches, ability to take action on endpoint entities, endpoint live response, and endpoint data recorder.</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Symantec Endpoint Protection</td>
<td>ATP management platform</td>
<td></td>
</tr>
<tr>
<td>EDR 1.0</td>
<td>HTTP</td>
<td>8080</td>
<td>Symantec Endpoint Protection</td>
<td>ATP management platform</td>
<td>Endpoint searches, ability to take action on endpoint entities, statuses of endpoints.</td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td>8443</td>
<td>Symantec Endpoint Protection</td>
<td>ATP Manager</td>
<td></td>
</tr>
<tr>
<td>RRS feed</td>
<td>HTTPS</td>
<td>443</td>
<td>Symantec Endpoint Protection</td>
<td>ATP Manager</td>
<td>Symantec Endpoint Protection Manager private cloud that lets endpoints communicate with ATP.</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Symantec Endpoint Protection</td>
<td>ATP Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With proxy certificate</td>
<td>8443</td>
<td>Symantec Endpoint Protection Manager</td>
<td>ATP Manager</td>
<td></td>
</tr>
<tr>
<td>Symantec cloud detection, analysis, and correlation services and telemetry services</td>
<td>If endpoint data recorder enabled</td>
<td>443 TCP</td>
<td>All ATP appliances</td>
<td>Symantec (External traffic)</td>
<td>Cloud service queries and telemetry data exchanges. If the endpoint data recorder is enabled Symantec Endpoint Protection sends conviction events directly to ATP.</td>
</tr>
<tr>
<td></td>
<td>If endpoint data recorder disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Anti-virus and intrusion prevention conviction information</td>
<td>HTTPS</td>
<td>HTTP 8080 TCP or HTTPS 443 TCP HTTP 80 TCP or HTTPS 8443 TCP</td>
<td>Symantec Endpoint Protection clients</td>
<td>ATP management platform</td>
<td>Information about files and the network traffic detected by Symantec Endpoint Protection.</td>
</tr>
<tr>
<td>Anti-virus and intrusion prevention conviction information</td>
<td>HTTP</td>
<td>80</td>
<td>ATP management platform</td>
<td>Symantec (External traffic)</td>
<td>Information about files and the network traffic detected by Symantec Endpoint Protection.</td>
</tr>
<tr>
<td>Product updates</td>
<td>HTTPS</td>
<td>443 TCP</td>
<td>All appliances</td>
<td>Symantec (External traffic)</td>
<td>Finds and delivers new versions of ATP.</td>
</tr>
<tr>
<td>ATP Manager</td>
<td>HTTPS</td>
<td>443 TCP</td>
<td>Client connecting to manage an appliance</td>
<td>Management platform or all-in-one appliance (Internal traffic)</td>
<td>ATP Manager access for an all-in-one appliance or management platform.</td>
</tr>
<tr>
<td>ATP Manager, network scanners, and all-in-one</td>
<td>SSH</td>
<td>22</td>
<td>Client connecting to manage an appliance</td>
<td>Management platform, scanner, or all-in-one appliance (Internal traffic)</td>
<td>Command line access for an all-in-one appliance or management platform.</td>
</tr>
<tr>
<td>Synapse Symantec Endpoint Protection Manager connection with Microsoft SQL Server (optional)</td>
<td>JDBC</td>
<td>1433 TCP (default)</td>
<td>Management platform or all-in-one appliance</td>
<td>Symantec Endpoint Protection Manager MS SQL Server (Internal traffic)</td>
<td>Required if using the Microsoft SQL Server for Symantec Endpoint Protection Manager and Synapse. Symantec Endpoint Protection Manager administrators can configure a different port for this communication.</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>From</td>
<td>To</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Communication channel (management platform and network scanner installations only)</td>
<td>AMQP</td>
<td>5671 TCP, 5672 TCP</td>
<td>Network scanner appliance</td>
<td>Management platform</td>
<td>Communications between the management platform and network scanners. Not required for an all-in-one installation. After the initial exchange on this port, the communication is secured.</td>
</tr>
<tr>
<td>Blocking page (Inline Block mode only)</td>
<td>HTTP</td>
<td>8080 TCP</td>
<td>Network scanner</td>
<td>Protected endpoints</td>
<td>Sends the blocking page when content is blocked at an endpoint. Not required for Inline Monitor or Tap/Span modes.</td>
</tr>
<tr>
<td>Synapse Symantec Endpoint Protection Manager connection with Embedded DB (optional)</td>
<td>HTTPS</td>
<td>8081 TCP (default)</td>
<td>Management platform or all-in-one appliance</td>
<td>Symantec Endpoint Protection Manager server (Internal traffic)</td>
<td>Required if using the embedded database for Synapse connection to Symantec Endpoint Protection Manager.</td>
</tr>
<tr>
<td>Synapse Symantec Endpoint Protection Manager connection with the Symantec Endpoint Protection Manager web services Remote Management and Monitoring (RMM) service (optional)</td>
<td>HTTPS</td>
<td>8446 TCP (default)</td>
<td>Management platform or all-in-one appliance</td>
<td>Symantec Endpoint Protection Manager Server</td>
<td>Required if connecting to the Symantec Endpoint Protection Manager server for executing management operations. For example, adding or removing items from the blacklist or placing an endpoint under quarantine.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog</td>
<td>TCP (preferred) or UDP port should be the same as configured in ATP Manager for Syslog</td>
<td>All appliances</td>
<td>Configured Syslog server (Internal or external traffic based on your environment)</td>
<td>If configured, this connection delivers log messages to remote syslog.</td>
</tr>
</tbody>
</table>

**Table D-2** ATP ports and settings *(continued)*
<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATP: Roaming</td>
<td>HTTPS</td>
<td>443 TCP</td>
<td>Management platform or all-in-one appliance</td>
<td>Symantec</td>
<td>This connection allows ATP to collect conviction events from ATP: Roaming and ATP: Email when Synapse Correlation is enabled for either one of these services.</td>
</tr>
<tr>
<td>ATP: Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>LDAPS</td>
<td>636</td>
<td>Management platform or all-in-one appliance</td>
<td>Active Directory server</td>
<td>This connection allows ATP to integrate with Active Directory for user authentication.</td>
</tr>
</tbody>
</table>
A
Active Directory
- adding a domain 106
- adding a group 109
- deleting a domain 109
- integrating with ATP 98
- preparing for integration with ATP 105
- updating the certificate 109
all-in-one device
- enabling scanning 74
antivirus 13
appliance 69
appliance settings
- custom configuration 69
- default 68
- rebooting 73
- shutting down 73
ATP
- about 12
- features by license type 14
ATP Manager 18
See also certificates
See also password
accessing 17–18
creating local user accounts 101
user accounts
- creating local user accounts 98
- integrating with Active Directory 98
- user roles 97

B
back up 57–58
Blacklist 13, 113, 117, 120
blocking pages 64
bypass mode
- NIC LED indicators 140

C
campaigns
- purging 66
certificates 62
- about 18
- expiring 62
- for endpoints 56
- third-party 18
- updating 62
- viewing status 62
CLI commands
- about 142
- back up 144
- bootstrap 145
- data_inspection_stat 145
- delete 145
- edrfeature 145
- exportfdr 146
- getpcap 147
- grep 147
- help 147
- list 148
- ntpsync 148
- password 148
- pieconfig 149
- reboot 149
- restore 149
- show 150
- shutdown 151
- sshconfig 151
- status_check 151
- tcp_check 151
- update 152
client. See Symantec Endpoint Protection
cloud-based sandboxing. See sandbox
command-line interface. See CLI commands
connections
- read-only account for Symantec Endpoint
  Protection Manager SQL database 34
- Symantec Endpoint Protection Manager 39
- Symantec Endpoint Protection Manager
  database 38
console access
- physical appliance 143
- virtual appliance 143
control point 12  
Cynic 13, 22, 93  

D  
data handling options 23  
databases  
  Symantec Endpoint Protection Manager log collection 36  
  Symantec Endpoint Protection Manager SQL database 34  
default settings 68  
DNS server 82  
domain  
  blacklisting 120  
  whitelisting 120  
domain name service. See DNS server  

E  
EDR (Endpoint Detection and Response)  
  about 15  
  enabling and disabling 46  
endpoint data recorder  
  about 45  
  configuring 43, 47, 52  
  enabling and disabling 46  
  exceptions 54  
  exclusions 56  
  integrating with endpoint control point 12  
endpoint data recorder  
  about 45  
  configuring 43, 47, 52  
  enabling and disabling 46  
  exceptions 54  
  exclusions 56  
  integrating with endpoint control point 12  
  Endpoint Detection and Response. See EDR  
  endpoints at risk  
  purging 66  
  events. See incidents  
  Synapse correlation 25  

F  
file  
  blacklisting 120  
  whitelisting 120  
firewall 156  

H  
Host Integrity policy 30  

I  
incidents  
  backing up and restoring 57  
  in syslog messages 84, 86  
  purging 66  
  Synapse correlation 24, 27, 29  
Inline Block mode 74  
Inline block mode 77  
Inline Block/Monitor mode  
  blocking pages 64  
Inline Monitor mode 74  
Inline monitor mode 77  
Insight 13  
  integration with Symantec Endpoint Protection 27, 29  
  internal networks 77  
ISO file  
  reimaging from 136  

L  
license 14, 60  
Linux commands 142  
load point 45  
log collector for Symantec Endpoint Protection Manager 36  
login credentials  
  ATP Manager 101  
  console 143  
  iDRAC 143  

M  
Malware Analysis 93  
  See also sandbox  
management platform/network scanner  
  adding or deleting a scanner 136  
  deleting a scanner 72  
  enabling scanning 74  
messages, system health 122  
Mobile Insight 13  

N  
NIC card 140  
notifications 101  
NTP server 83  

O  
on-premises sandboxing. See sandbox  
OVF template 137
P

password
  ATP Manager 103–104
  console 143
  iDRAC 143
  Web UI 102
physical appliance
  reimaging 136
policy
  about 112
  creating Blacklist 113
  creating Whitelist 115
  managing 120
  supported match values 117
ports
  LAN/WAN Port Settings panel in ATP Manager 74
  on firewall 156
  on physical appliance 139
  used by ATP 156
PowerShell 45
process launch 45
process terminate 45
proxy server
  ATP proxy for Symantec Endpoint Protection clients 42
  enterprise proxy 80
  network proxy 79
purge data 66

Q
Quarantine Firewall policy 30

R
reboot appliance 73
reimage, physical appliance 136
reinstall, virtual appliance 137
restart appliance 73
restore 57, 149
restore backup 152

S
sandbox 22, 68, 93
  See also Cynic
  See also Malware Analysis
scanning
  enabling and disabling 74
Search
  System Activity 131
shut down appliance 73
SIEM system 85
SMTP 63
SNMP 91
software updates 134
SONAR 14
SSL
  ATP and Symantec Endpoint Protection 56
  static routes 96
Symantec Advanced Threat Protection. See ATP Symantec ATP:Roaming correlation
  about 26
Symantec Email Security.cloud 12
Symantec Endpoint Protection 12
  communicating with 50
  integration 27, 29
  proxy configuration 42
  securing communication 56
  supported ATP features 31
Symantec Endpoint Protection Manager
  connection configuration 39
  database connection 38
  embedded database 36
  replication 39
  SQL database 34
Synapse 26
Synapse correlation
  about 24
  Symantec Endpoint Protection Manager configuration 27, 29
  system requirements 154
  with Email Security.cloud 25
syslog
  about 84
  CEF format 85
  configuring 88
system health, indicators and messages 122

T
Tap/Span mode
  enabling scanning 74
testing
  blocking pages 65
time server. See NTP server
update software 134–135

user accounts
   about managing ATP users 97
   creating local user accounts 98, 101
   editing local user accounts 103
   enabling and disabling local user accounts 104
   integrating with Active Directory 98
   requesting a new password 104

V
Vantage 13
virtual appliance
   reinstalling 137
VLAN
   configuring ATP for 74, 77

W
Whitelist 13, 115, 117, 120