Symantec™ Advanced Threat Protection Platform 2.2 Release Notes

Documentation version: 2.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

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:

www.symantec.com/business/support/

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:

support.symantec.com

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_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Release Notes

This document includes the following topics:

Introduction to Symantec Advanced Threat Protection

Symantec Advanced Threat Protection (ATP) provides a single management interface for performing the critical security tasks of detecting, protecting, and responding to threats in your environment.

The ATP documentation set consists of the following:

- The *Symantec™ Advanced Threat Protection Installation Guide* provides complete explanations of the planning, installation, and setup tasks.
- The *Symantec™ Advanced Threat Protection Administration Guide* provides information on configuring and monitoring ATP after you install it.
- The *Symantec™ Advanced Threat Protection Security Operations Guide* describes how to investigate the incidents that ATP detects and how to contain and remediate those threats.

For more information about this release including the documentation, go to the following URL:

https://support.symantec.com/en_US/dpl.64123.html

To view the Online Help for ATP version 2.2, click a Help link in ATP Manager, or go to:

http://help.symantec.com/home/ATP_2.2?locale=EN_US

To learn about any issues that arose after the publication of the release notes, see Late Breaking News at the following URL:

https://support.symantec.com/en_US/article.ALERT2135.html

What's new in Symantec Advanced Threat Protection 2.2

Table 1-1 lists the new and enhanced features available in Symantec Advanced Threat Protection (ATP) 2.2.

Table 1-1 What's new in ATP 2.2

Feature	Description
ATP public APIs	ATP RESTful APIs allow for direct API access to the ATP appliance over SSL. ATP APIs use standard HTTP features and standard HTTP status codes to indicate errors. The REST APIs return JSON formatted data. All APIs exposed by the ATP appliance carry authentication tokens and other privileged data. To ensure the confidentiality of the data, the REST APIs exposed by ATP are only available on https://. Access ATP public APIs at the following URL: http://help.symantec.com/api-doc/atp_2.2/EN_US/

Table 1-1 What's new in ATP 2.2 *(continued)*

Feature	Description
Splunk® connector	ATP provides a connector that can replicate ATP event data to Splunk. This functionality lets you correlate the ATP data with other events collected in Splunk to get a broader picture of the activity that is occurring in your network. The connector is supported for Splunk Enterprise 6.4 and Splunk Cloud. For more information, see the *Symantec Advanced Threat Protection Connector for Splunk® Administration Guide* on the ATP Support site: https://support.symantec.com/en_US/dpl.64123.html
Integration with ServiceNow™	The ATP app lets you leverage the ticketing and workflow capabilities of ServiceNow to monitor and investigate possible threats in your organization by aggregating ATP incident and related event data from your ATP appliances into the ServiceNow console. For more information, see the *Symantec Advanced Threat Protection App 1.0 for ServiceNow™ Administration Guide* on the ATP Support site: https://support.symantec.com/en_US/dpl.64123.html
Event details	You can now click on any row on the Events page in the ATP Manager to view the corresponding Event details page. Event details pages provide in-depth information about the event, such as a description of the event, the files and domains involved in the event, platform information, DeepSight™ intelligence (when available), etc.
Incident Details Report	The new Incident Details Report provides the latest information about a specific incident, including its detection history, related events, and user-generated comments. The Incident Details Report is available in PDF format. You can run the report on-demand, or you can create a schedule to run it at regular intervals.

Table 1-1 What's new in ATP 2.2 *(continued)*

Feature	Description
Certificate Management	As an administrator, you can now view certificate information for each installed certificate, such as its status (Valid, Expiring Soon, Expired), name, issuing authority, recipient, and expiration date. 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.
Dynamic Adversary Intelligence	Dynamic Adversary Intelligence (DAI) is a Symantec feed that provides detailed information about the attackers (or "adversaries") that conduct targeted attacks. The DAI feed is delivered to ATP from LiveUpdate. ATP then correlates this data with your existing event data to see if threats from the feed are present in your organization. If so, ATP creates DAI events and incidents accordingly.
Automatic Report Purging	ATP allocates 1 GB of disk space for saved reports, and now regularly monitors this space to ensure that it is not exceeded. When this allocation is reached, ATP generates System Health warnings and automatically frees up 10 percent of this space by purging saved reports.
Endpoints Widget	The Actively Infected Endpoints section now displays the number of managed and unmanaged endpoints that were associated with a high priority incident within the last 7 days. The Active Managed Endpoints section displays the number of managed Symantec Endpoint Protection endpoints that incurred any type of event activity within the last 4 days.

Table 1-1 What's new in ATP 2.2 *(continued)*

Feature	Description
Symantec ATP:Roaming Correlation	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 from both your on-LAN and off-LAN (or "roaming") users. Using Synapse™, you can enable ATP to import conviction events from ATP:Roaming to correlate them with events from your other control points (such as Network, Endpoint, and Email). You can also search for these events from the Events page. **Note:** Symantec Advanced Threat Protection 2.2 is being released with the Symantec ATP:Roaming Correlation feature. However, this feature will not be functional until Symantec releases ATP:Roaming later this year.
Network Proxy Basic Access Authentication (BA)	You can now configure access to a network proxy that requires Basic Access (BA) Authentication.
VLAN support for Inline Monitor and Block mode	The ATP appliance can now inspect traffic that includes VLAN tags (including from stacked VLANs) for all three deployment modes: TAP, Inline Monitor, and Inline Block.

System requirements for physical appliance installation

This release of Symantec Advanced Threat Protection (ATP) runs on the following appliance models:

- ATP 8840
- ATP 8880

ATP appliances include an Integrated Dell Remote Access Controller (iDRAC). The iDRAC console requires the latest version of the Java Runtime Environment (JRE) installed on your administrative client.

See "System requirements for virtual appliance installation" on page 10.

System requirements for virtual appliance installation

Table 1-2 lists the system requirements for the virtual appliance.

Table 1-2 System requirements for the virtual appliance

Requirement	Minimum per VM for production environment
Disk space	500 GB
CPUs	4
Memory	32 GB

Table 1-3 lists the system requirements for the host.

Table 1-3 System requirements for the VMware ESXi host

Requirement	Minimum for production environment
Version	ESXi 5.5 and 6.0
Disk space	500 GB (per VM)
CPU cores	4
Memory	32 GB (per VM)
Hardware virtualization	Enabled

Table 1-4 lists the network interface requirements, based on the operating mode of the appliance.

Table 1-4 Network interface requirements for the VMware ESXi host

Operating mode	Minimum for production environment	Maximum for production environment
Management platform (management platform devices only)	1 (Management)	1 (Management)

Note: To avoid over-commitment of resources, it is recommended that you reserve the required resources on your ATP appliance virtual machine.

Refer to your VMware documentation for VMware system requirements and configuration of virtual machines.

See "System requirements for physical appliance installation" on page 10.

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 requirements for 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.

Client endpoints using Symantec Endpoint Protection version 12.1 RU 6 MP3 or later can be managed by ATP with full EDR functionality. Client endpoints using versions earlier than Symantec Endpoint Protection 12.1 RU5 are not supported. If your environment includes clients using 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 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 database. ATP can access external Microsoft SQL databases 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)

For Symantec Endpoint Protection Manager system requirements, refer to the Symantec Endpoint Protection documentation.

Browser requirements for ATP Manager

Table 1-5 lists the web browsers that are compatible with ATP Manager. JavaScript must be enabled in the browser. The minimum resolution for viewing ATP Manager is 1280x1024.

Table 1-5 Browser requirements for ATP Manager

Browser	Version
Microsoft Internet Explorer	11 or later
Mozilla Firefox	45 or later
Google Chrome	53 or later

Important information about updating Symantec Advanced Threat Protection

If you are running ATP 2.0.2, you can upgrade to 2.2 using the **Update Software** feature in ATP Manager.

If you are running ATP 2.0.0 or 2.0.1 you must upgrade to 2.0.2. If you are running ATP: Network 1.x, you will need to perform a one-time fresh installation in order to get onto the ATP 2.x product line.

When a software update is available, you see the following notification in the upper right corner of ATP Manager: **ATP Needs Attention**. When you hover over this notification, you see the following message: **Software update available**. Additionally, an email is sent to all of your administrators notifying them of the update.

Do the following when you update the software on your physical appliance or virtual appliance:

- Run a backup.
  To mitigate risks, complete a full backup before you perform a software update.
- Upgrade the management platform before you upgrade remote scanners.
- Click the **Update Software** button only once.
  If you click the button more than once, you may experience unexpected behavior.
- Do not power off your appliance or restart ATP during the upgrade process.
- Do not change any of your configuration settings during the upgrade process.
  If you change your settings during the upgrade process, you may corrupt your database.

Note: The **System Health** notification indicating that there is a pending software upgrade no longer appears after the upgrade finishes.

To upgrade Symantec Advanced Threat Protection

1. From ATP Manager, select **Settings** > **Appliances**.
2. On the Appliances page, do one of the following:
   - From the Appliances list, click the **Update Software** button for the appliance that you want to upgrade.
   - From the Appliances list, click the appliance you want to upgrade. From the Appliance Details page, click **Update Software**.

Note: The upgrade may take awhile to download. Following the upgrade, your appliance automatically reboots. After the reboot, check to ensure that the upgrade was successful by verifying the latest version number of ATP. This number appears on the Appliance Details page.

Important information about the Symantec Advanced Threat Protection virtual appliance

The Symantec Advanced Threat Protection virtual appliance has all of the same features and functionality as the hardware appliances, but there are some details to note:

- When you deploy a virtual appliance as a scanner, the preferred mode is Tap mode.
  Symantec does not recommend that you deploy a virtual appliance as a scanner if you intend to operate the scanner in Inline Block or Inline Monitor mode. Physical appliances have a bypass NIC that allows traffic through if the system is offline. Virtual appliances do not have this bypass NIC.
- ATP can require a large amount of computing power and network bandwidth. Exercise caution when you consider sharing virtual resources between ATP and any other virtual machine.
- If the your host loses sync with your NTP server, you must use the VMware virtual clock, which is the host computer's physical clock. Set the NTP server in the VMware client **Configuration > Software > Time Configuration > Properties** to UTC.

Important information about SHA SSL certificates

The National Institute of Standards and Technology (NIST) has determined that the SHA-128 (SHA-1) cryptographic algorithm could be vulnerable to attacks in the near future. Currently, SHA-1 is safe and there are no reported critical breaches with SSL SHA-1 SSL certificates. However, Symantec has already committed to replacing expiring SSL certificates used by our Symantec Advanced Threat Protection backend infrastructure for software updates with SHA-2 SSL certificates.

If you are using Symantec Advanced Threat Protection 2.0.1, or an earlier release, you must update to version 2.0.2 or a later release in order to get future updates via the software update mechanism.

Since the current SSL certificate used by software updates is issued from the **Class 3 Public Primary Certificate Authority –G5** SHA-1 root CA, it has not been trusted by ATP releases prior to 2.0.2. ATP 2.0.2 and later releases will only support SHA-2 certificates. If you do not update to ATP 2.0.2 or a later release, you will be unable to update new appliance software. If you are running ATP 2.0.0 or 2.0.1 you can update via the software update mechanism. If you are running ATP: Network 1.x, you will need to perform a one-time fresh installation in order to get onto the ATP 2.x product line. ATP 2.0.2 includes inline mode for network and reporting.

Resolved issues in Symantec Advanced Threat Protection 2.2

Table 1-6 lists the issues that are resolved in this release.

Table 1-6 Resolved Issues

Issue	Resolution
ATP permits the use of blank administrator passwords during bootstrap.	ATP requires administrators to provide a password during the bootstrap installation. http://www.symantec.com/docs/TECH230998
Use of non-English keyboards can have undesired results.	ATP supports the use of non-English language keyboards with the physical ATP appliance. http://www.symantec.com/docs/TECH234442

Table 1-6 Resolved Issues *(continued)*

Issue	Resolution
Customers that change the default SEPM domain cannot send commands to other domains in their organization.	Customers that change the default Symantec Endpoint Protection Manager domain cannot send commands to other domains in their organization. http://www.symantec.com/docs/TECH234362
SNMPv3 configuration does not recover from out-of-sync condition once encountered.	This issue occurred as a result of the previous issue (where the snmpd.conf file is not configured properly, which throws the SNMPv3 with an out-of-sync condition). This issue is now resolved. http://www.symantec.com/docs/TECH234360
Error when revoking a blacklist file.	The issue with revoking blacklisted files (un-blacklisting) is resolved. http://www.symantec.com/docs/TECH233795
Moving a single node in the Incident graph moves the entire graphic.	Using Internet Explorer 11, when you were on the Incident details page in the Incident graph and attempted to move or arrange any entity node, the entire graphic moved. This issue is resolved. http://www.symantec.com/docs/TECH233796
ATP does not return results when the end date is earlier than the start date when you filter events on the Events page.	ATP Manager validates that the start date precedes the end date in the filter and returns an error message if it does not. http://www.symantec.com/docs/TECH233798
Searches that contain special characters return all results on the **Events** page.	ATP does not support the use of special characters in **Events** page filter searches. ATP does not treat special characters as literal characters on the **Events** page for filter searches. Symantec recommends that you avoid using special characters (such as *, ~, &, +, |, ?) in your search criteria. http://www.symantec.com/docs/TECH233800

Known issues in Symantec Advanced Threat Protection 2.2

Table 1-7 lists the known issues in Symantec Advanced Threat Protection 2.2.

Table 1-7 Known issues

Issue	Description
SEPM Controller Connection failure	You see the following error when you try to add a SEPM Controller if the hostname is something other than `localhost.local domain`: Failed to configure SEPM Controller connection· Workaround: Use the hostname command to change the local host to `localhost.localdomain`. https://www.symantec.com/docs/TECH235975
Unable to configure Synapse or SEPM database after performing a database restore.	Restart the appliance after you restore a large database, then attempt to configure Synapse / SEPM. http://www.symantec.com/docs/TECH235968
ATP has "Invalid credentials" error message in the ATP Manager and loses connectivity with SEPM after running for a day.	Try re-entering your credentials. http://www.symantec.com/docs/TECH235969
Duplicate entries for delete a file command.	When selecting to delete a file from an endpoint, you may see multiple rows for the same endpoint listed in the delete file dialog box. The display is conveying that there are two or more file instances with a different file name/path on the same endpoint. ATP does not currently display the file name or path in this grid. http://www.symantec.com/docs/TECH235967

Table 1-7 Known issues *(continued)*

Issue	Description
When SEP is taken offline and brought back online, the quarantine command continues to return an error.	When you remove the SEP client from SEPM, the sep_unique_id maintained on the ATP side becomes outdated. When you add the SEP client back to SEPM, ATP needs time (approximately 1 hour) to get the latest SEP Endpoint info from SEPM. Then ATP can issue the quarantine successfully to SEPM. www.symantec.com/docs/TECH235940
Isolate action failed after updating the SEPM domain with a long name (100 characters).	When the SEPM domain name is long (i.e., 100 characters or more), the isolate action fails on the endpoint. Keep SEPM domain names under 100 characters. www.symantec.com/docs/TECH235941
Endpoint IP address mismatch on Event details page and endpoint entity page	ATP does not support using a NAT device between endpoints and ATP if you use the SEP proxy. www.symantec.com/docs/TECH235918
Incorrect username, password, or domain provided for SEPM when trying to connect ATP 2.0.3 or earlier to SEP 14.	You must be running ATP version 2.2.0 or later to connect to SEP 14. https://www.symantec.com/docs/TECH235887
Malicious email attachment may result in multiple events in ATP.	When ATP generates a conviction event for a malicious file in an email attachment, multiple events may appear in ATP Manager for what should be a single event. This situation occurs when multiple detection engines identify the malware. www.symantec.com/docs/TECH235881
You must re-upload license after addressing proxy SSL certificate error.	If ATP has detected a configured Network Proxy is intercepting SSL communications, after the interception issue has been resolved, you must re-upload your license through the Global Settings page to recover ATP communication with Symantec servers. www.symantec.com/docs/TECH235882

Table 1-7 Known issues *(continued)*

Issue	Description
The software update from ATP 2.0.3 to ATP 2.2 database migration may break event/incident connections.	After the software update from ATP 2.0.3 to ATP 2.2, new events corresponding to a pre-existing incident will not be correctly associated in the database. New incidents created after the update will correctly associate all events going forward. www.symantec.com/docs/TECH235891
Database initialization will fail if bootstrap is performed immediately after the appliance starts.	Wait 2 minutes or longer after the appliance starts to perform the bootstrap to ensure a stable state. www.symantec.com/docs/TECH235892
After configuring multiple SEPM controllers in ATP 2.2, the subsequent SEPM controllers' settings are not processed immediately.	It may take up to an hour for the ATP to process the subsequent SEPM controllers and reflect their endpoints in the Dashboard reports. www.symantec.com/docs/TECH235894
The Dashboard generates the following error: "A script on this page may be busy, or it may have stopped responding."	This may be due to a large amount of data that the Dashboard is unable to process. There is no workaround once this issue has occurred, so you must exit the Dashboard. To prevent this issue from occurring, ensure that all endpoints have their time set correctly. http://www.symantec.com/docs/TECH234811
After upgrading to ATP 2.0.2, fields on the Executive Report show no data.	The Recently Infected Endpoints and Domains Showing Threat Behavior sections of the Executive Report do not show any data when you run the report shortly after upgrading to ATP 2.2. These sections only include data from threat activity that is detected by ATP after you upgrade to ATP 2.0.2. No data appears for prior releases. There is no workaround. http://www.symantec.com/docs/TECH235896

Table 1-7 Known issues *(continued)*

Issue	Description
Successful file deletion shows as failed.	When you successfully delete a file on an endpoint from ATP, the Action Manager indicates that the deletion failed. http://www.symantec.com/docs/TECH234827
Non-ASCII characters are not supported in user accounts.	Non-ASCII characters are not supported when you create user accounts during bootstrap or in ATP Manager. You must use ASCII characters for the **Display Name**, **Login**, **Password**, and **User Email** when you create user accounts. http://www.symantec.com/docs/TECH230965
Duplicate entries can be entered for Symantec Endpoint Protection Manager connections in **Global > Settings**.	If multiple Symantec Endpoint Protection Manager connections from the same Symantec Endpoint Protection site or the same Symantec Endpoint Protection Manager connection is listed multiple times in ATP Manager, connection errors will occur. Do not enter the same Symantec Endpoint Protection Manager connection multiple times, and only enter one Symantec Endpoint Protection Manager connection per Symantec Endpoint Protection site. Delete the duplicate entries in the Symantec Endpoint Protection Manager connections list in ATP Manager, and also delete the entries in the Web Service Application Registration of Symantec Endpoint Protection Manager. Reconnect when you have made the corrections. http://www.symantec.com/docs/TECH233761

Table 1-7 Known issues *(continued)*

Issue	Description
Connection to Symantec Endpoint Protection Manager fails when Symantec Endpoint Protection Manager administrator account uses Active Directory.	If you create a Symantec Endpoint Protection Manager administrator account that specifies to use Active Directory for authentication, the connection fails when you try to use this account to create a Symantec Endpoint Protection Manager controller connection in ATP, even if the connection can be successfully made directly to Symantec Endpoint Protection Manager. Do not specify Active Directory as the authentication mechanism for Symantec Endpoint Protection Manager administrator accounts that you intend to use when creating a Symantec Endpoint Protection Manager controller connection in ATP. http://www.symantec.com/docs/TECH233780
When an endpoint is moved from one Symantec Endpoint Protection Manager to another, ATP may not recognize that the endpoint is now managed by another Symantec Endpoint Protection Manager instance.	You may notice the effect of this if whitelist, blacklist, or other commands sent by ATP are not reaching endpoints managed by Symantec Endpoint Protection Manager, or group and user information for endpoints may not be accurately listed in ATP Manager. Make certain to remove an endpoint client from a Symantec Endpoint Protection Manager configuration before moving it to a different Symantec Endpoint Protection Manager instance. http://www.symantec.com/docs/TECH233813
Refresh when using the browser **Back** button.	Clicking the **Back** button in the browser when using ATP Manager does not always reflect configuration changes made on the previous screen. For example, if you enable scanning on an appliance, then click the **Back** button on the browser, the appliance may not correctly display that scanning has been enabled. Click the **Refresh** button on the browser to refresh the page information. http://www.symantec.com/docs/TECH233782

Table 1-7 Known issues *(continued)*

Issue	Description
Changing the role of your only Administrator account.	ATP allows you to edit the role of your only Administrator account to that of a non-Administrator. This leaves you without an Administrator account. Create a second Administrator account before editing the first. http://www.symantec.com/docs/TECH233794
Error message appears when you install a license file.	ATP only supports the installation of license files with the .slf extension. Ensure that the license file that you are installing ends with the .slf extension. Contact Symantec Support if your license file is valid and does have the .slf extension, but you continue to receive an error message. http://www.symantec.com/docs/TECH233797

Troubleshooting

The following describes problems that can occur in your environment and provides suggestions to resolve them.

Virtual Machine Configuration

When you are running in a virtual environment, it is important to properly configure the virtual machines on which your ATP appliances run. The following are some configuration notes:

- Make certain your virtual machine has the proper resources allocated. Also, make sure to reserve VM resources (CPU, memory, disk) for the ATP appliance, or you may experience disk space or high-memory usage errors.
- Use the proper block size, depending upon the VMFS version of your system. If your ESXi server is using VMFS-2, then your block size must be set to 4 MB or greater. If you are using a file system later than VMFS-2, set your block size to 8 MB. If the block size is not properly set, the deployment of the OVA can fail with a message about the disk capacity of the machine being greater than the amount available on the datastore.
- When deploying a network scanner on a virtual machine and you have mapped the WAN port to a physical NIC through a vswitch, change the configuration of

the vswitch to allow all VLAN IDs in the port group properties. Without this setting, some network traffic may not be captured by ATP.

Connections to Symantec Endpoint Protection Manager

The System Health can display a connection error to your Symantec Endpoint Protection Manager host in a number of situations. Perform the following checks in order to determine the cause and proper resolution to the problem:

1. Check to make sure the Symantec Endpoint Protection Manager host is up and running and that you can connect to your Symantec Endpoint Protection Manager management interface. If the host is not up and running, make sure the host is up and that you can connect to Symantec Endpoint Protection Manager normally.
2. Check to make sure the account used to login to Symantec Endpoint Protection Manager is not locked, for example, due to multiple attempts to login with the wrong password. Under some situations, the account can become locked or become expired. In this case, remove the connection configuration in ATP Manager then create a new connection configuration with the correct credentials.
3. In all other cases, remove the Symantec Endpoint Protection Manager connection configuration from ATP Manager and re-enter the configuration.

When you create a Symantec Endpoint Protection Manager connection configuration in ATP Manager, a few situations can cause errors so that the connection cannot be created:

- Check to make sure the Symantec Endpoint Protection Manager administrator account you are using is not specified to use Active Directory as the authentication mechanism. This type of account cannot be used in a Symantec Endpoint Protection Manager connection configuration in ATP.
- Check that the certificate you are using for secure communication is valid. An invalid certificate can be created by the Symantec Endpoint Protection Manager administration interface if you have changed the server name or IP address. See the following link for the correct procedure for changing a server's name or IP address: http://www.symantec.com/connect/videos/changing-sepm-server-name-and-ip-address. Once a valid certificate is obtained from Symantec Endpoint Protection Manager, you can create the connection in ATP Manager.

Updating an appliance

In ATP Manager, a message appears that details the update can take some time, but if you perform the operation from the command line, you may not be warned of the length of the operation.

If you are using ATP2.0.2 or higher, you can check the current state of a software update by typing the following command from the command-line interface:

```
update status
```