Symantec™ Advanced Threat Protection 3.0 Upgrade 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. SYMANTECCORPORATION SHALL NOT BE LIABLEFOR 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

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>About upgrading Symantec Advanced Threat Protection to version 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About upgrading to ATP 3.0 with Endpoint Data Recorder</td>
</tr>
<tr>
<td></td>
<td>Prerequisites for ATP upgrade</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Upgrading Symantec Advanced Threat Protection (ATP) appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upgrading ATP appliances for ATP 3.0</td>
</tr>
<tr>
<td></td>
<td>Procuring the upgrade components</td>
</tr>
<tr>
<td></td>
<td>Installing the new hard drives</td>
</tr>
<tr>
<td></td>
<td>Replacing the memory modules</td>
</tr>
<tr>
<td></td>
<td>Configuring the new RAID 10 array</td>
</tr>
<tr>
<td></td>
<td>Configuring the RAID 10 array using iDRAC</td>
</tr>
<tr>
<td></td>
<td>Configuring the RAID 10 array using the RAID Controller BIOS</td>
</tr>
<tr>
<td></td>
<td>List of upgrade components for ATP appliances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Upgrading Symantec Advanced Threat Protection (ATP) VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About upgrading ATP virtual installations for ATP 3.0 with Endpoint Data Recorder enabled</td>
</tr>
<tr>
<td></td>
<td>Upgrading ATP VMs for ATP 3.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Running the expand_storage CLI tool</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Running the extend_storage tool</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Related documentation</td>
</tr>
</tbody>
</table>

## Related documentation
About upgrading Symantec Advanced Threat Protection to version 3.0

This chapter includes the following topics:

- About upgrading to ATP 3.0 with Endpoint Data Recorder
- Prerequisites for ATP upgrade

About upgrading to ATP 3.0 with Endpoint Data Recorder

You can upgrade the software of ATP 8840 appliance to ATP 3.0; however, the hardware of 8840 does not support ATP’s new endpoint data recorder and Endpoint Detection and Response (EDR) 2.0 features. The hardware of ATP 8880v1 and 8880v2 appliances can be upgraded to support the endpoint data recorder feature. The ATP 8880-30 requires no hardware or software upgrade to make use of the endpoint data recorder and EDR 2.0 features.

In the case of appliances, the upgrade involves increasing storage (hard drive) capacity and increasing memory (RAM). Virtual installations require that additional storage, RAM, and CPU cores are provisioned in the ATP VM. This document provides information and workflow instructions to upgrade existing appliance hardware and VMs to meet ATP 3.0 with Endpoint Data Recorder platform requirements.

Port and protocol changes

When you upgrade from ATP 2.3 or earlier, you must change the network port and possibly the protocol, depending on whether you want to use Endpoint Detection and Response (EDR) 1.0 or EDR 2.0. To take advantage of Endpoint Detection and Response (EDR) 2.0 functionality,
such as the endpoint data recorder, this change in protocol and port is required. See the following table for port and protocol requirements.

Note: When EDR 2.0 is enabled, HTTP 80 is no longer available, and thus, HTTP 8080 must be used for HTTP configurations. In the case that HTTPS 8443 was previously configured, the option to use this port and protocol is still available upon upgrade.

<table>
<thead>
<tr>
<th>EDR Version</th>
<th>Protocol-Port Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>HTTPS 8443 or HTTP 8080</td>
</tr>
<tr>
<td>2.0</td>
<td>HTTPS 443</td>
</tr>
</tbody>
</table>

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 by deleting your SEPM Controller configuration and then re-adding it.

Certificate requirements for upgrade

Immediately upon upgrading to ATP 3.0, EDR 2.0 is disabled (Private Insight Server settings are not affected). If you're 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 built-in SSL certificate to the SEP endpoints running SEP 14.0 RU1 or later. (Third-party certificates that have already been installed and pushed to the endpoints are also installed). The certificate ensures secure communications 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 secure communication with ATP.

Upgrade instructions

See the following sections of this guide for instructions to upgrade your type of installation:

- See “Upgrading ATP appliances for ATP 3.0” on page 11.
- See “Upgrading ATP VMs for ATP 3.0” on page 24.

Note: This document does not address the configuration changes required to make a customer-provided appliance compatible with ATP 3.0.
Prerequisites for ATP upgrade

The following prerequisites apply to both, appliance and VM upgrades:

- It is strongly recommended that you back up your ATP data before you upgrade. See the Symantec™ Advanced Threat Protection 3.0 Administration Guide for information about backing up your ATP data.

- You must upgrade the ATP software to version 3.0 before you perform hardware platform upgrades. Virtual installations install the software after upgrades to the VM resource allocations are made.

- Make sure that ports 443 and 8080 are open to traffic.

IMPORTANT: Endpoint Data Recorder is not enabled by default. Perform the upgrade before enabling Endpoint Data Recorder. Also, make sure your network infrastructure is able to handle the increased traffic incurred by Endpoint Data Recorder. See the Symantec™ Advanced Threat Protection 3.0 Installation Guide for requirements and recommended network configurations.
Upgrading Symantec Advanced Threat Protection (ATP) appliances

This chapter includes the following topics:

- Upgrading ATP appliances for ATP 3.0
- Procuring the upgrade components
- Installing the new hard drives
- Replacing the memory modules
- Configuring the new RAID 10 array
- Configuring the RAID 10 array using iDRAC
- Configuring the RAID 10 array using the RAID Controller BIOS
- List of upgrade components for ATP appliances

Upgrading ATP appliances for ATP 3.0

The hardware upgrade procedures affect hard drives and memory. The exact hardware upgrades required depend on which ATP appliance(s) you have:

- ATP 8880 v1, based on the Dell R720XL platform
- ATP 8880v2, based on the Dell R730XL platform
Note: You can upgrade the software of the ATP 8840 appliance to ATP 3.0; however, the hardware of the 8840 does not support ATP’s new endpoint data recorder and EDR 2.0 features.

See Table 2-2 on page 22. for a list of the necessary hardware components to upgrade your appliance.

Warning: Installing non-Dell components on the appliance voids the Dell warranty. You must procure the upgrade hardware directly from Dell.

Before you start, download or otherwise procure the owner’s manual for your appliance platform:

The hardware upgrade workflow proceeds as follows:

Table 2-1 Hardware upgrade workflow

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Determine the model of the appliance – whether R720 or R730 and then procure the necessary upgrade components directly from Dell. See Table 2-2 on page 22. for component part numbers and specifications. See “Procuring the upgrade components” on page 13.</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade the appliance software to ATP 3.0. <strong>Note:</strong> The hardware upgrade will not be successful unless you first install ATP 3.0 (A connection via port 443 to swupdate.brightmail.com must be available). See the Symantec™ Advanced Threat Protection Platform 3.0 Installation Guide for instructions.</td>
</tr>
<tr>
<td>3</td>
<td>Power down the appliance, install the hard drives, and replace the memory modules, closely following the steps highlighted in the Dell owner’s manual appropriate for your appliance. See “Installing the new hard drives” on page 13.</td>
</tr>
<tr>
<td>4</td>
<td>Configure a second RAID 10 hard drive array to address the four new 1.8TB hard drives. See “Configuring the new RAID 10 array” on page 15.</td>
</tr>
<tr>
<td>5</td>
<td>Run the extend_storage CLI tool. See “Running the extend_storage tool” on page 25.</td>
</tr>
</tbody>
</table>
Table 2-1: Hardware upgrade workflow (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Use the Show Info feature to validate the installation and configuration of drives and memory.</td>
</tr>
</tbody>
</table>

**Procuring the upgrade components**

You first determine which platform model you have and then procure the appropriate Dell components for it. See Table 2-2 on page 22. If you don’t know which appliance you have, do one of the following:

- Prior to powering down the appliance, look up the appliance details on the ATP manager.

![ATP Manager Screen]

- Use the service tag number (located in the small drawer under the DVD drive) to find the model number at the Dell Warranty Support page.

- If you have access to the entire machine (e.g., it’s not in a rack), the model number is imprinted on an ID sticker applied to the left side of the chassis.

**IMPORTANT:** Retain your Customer Purchase Order details (number, dates, items purchased) for your component upgrade order. This information is required by Dell if the appliance requires hardware support or if there are warranty issues. Newly added Dell components are covered in the remaining support period of the appliance. Also make a note of the service tag for the appliance being updated with these newer components.

**Installing the new hard drives**

The Dell R720 and R730 platforms have eight hard drive bays. Both platforms ship with four 300GB, 15K, SAS hard drives configured as a RAID 10 array. This array provides approximately 550 GB of disk space. To scale the appliances for ATP 3.0, four additional hard drives are installed and configured as a second RAID 10 array. These extra hard drives are added to the four empty hard drive slots of the R720 and R730.
Note: In addition to the SAS drives, the Dell R730 also ships with a 400GB SSD in a fifth bay. Before you upgrade the appliance, the SSD must be removed. See the R730 owner’s manual for instructions to access and remove the SSD.

The new array uses four 1.8TB, 10K, SAS drives. The available space of the volume after RAID 10 configuration is approximately 3.3TB. After scaling, the physical appliance has two RAID 10 arrays: the original as-shipped RAID 10 array (with ~550GB), and the additional 3.3 TB RAID 10 array, for a total of ~3.8 TB.

To install the drives, follow the instructions provided in the Dell owner's manual for the appliance.

### Replacing the memory modules

**IMPORTANT**: You are replacing the existing memory modules, not adding to them. Be sure that you follow all module handling precautions as indicated by Dell. Mishandling memory modules can render them unusable due to static discharge or other damage incurred through improper insertion.

Upgrading the memory requires that you do the following:

- Power down the machine and disconnect the system from the electrical outlet.
- Let the machine cool down for 5-10 minutes (memory modules can be hot to the touch right after power-down).
- Gain access to the top of the machine so that you can remove the top panel and cooling shroud from the interior compartment. You may need to un-rack the machine or slide it out if it's mounted on slide rails.
- Carefully follow the instructions provided in the owner's manual to:
  - Gain access to the memory modules
  - Remove the existing modules
  - Insert the new modules
  - Verify the new modules are recognized by the operating system

The memory modules you are replacing are obvious by their physical appearance. Non-used slots are populated with blank modules that feature a plastic trim piece along the top. Leave these in place! The actual memory modules do not have the trim pieces. The memory modules you replace are indicated by the red arrows in the following image:

**Warning**: Memory module orientation is reversed for some of the slots- if the module does not readily insert, reverse its orientation and try again. **DO NOT FORCE THE MODULES INTO PLACE!**
After you replace the memory modules, replace the cooling shroud and top panel, and plug the unit back into the electrical outlet. Follow the instructions in the manual to verify that the memory is properly recognized.

Configuring the new RAID 10 array

After installing the hard drives, you must configure them as a second RAID 10 array. You have two options to configure the array:

- Using iDRAC
  See “Configuring the RAID 10 array using iDRAC” on page 15.

- Using the RAID controller BIOS
  See “Configuring the RAID 10 array using the RAID Controller BIOS” on page 18.

Unless your security policies restrict its use, iDRAC is the easiest method. Use the BIOS method if security policies prevent the use of iDRAC.

Configuring the RAID 10 array using iDRAC

After installing the new drives, perform the following steps to configure the RAID 10 drive array using iDRAC.

To configure the RAID 10 array using iDRAC

1. Connect the appliance to the network, and then access its iDRAC web interface at https://<iDRAC IP>.
2. On the iDRAC front page, click Reset to reset the iDRAC.
3 In the left pane, select Storage and then in the right pane on the Summary tab, verify that eight total disks exist, four in Ready state, and four in Online state.

4 In the left pane, expand Storage and select Virtual Disks. In the right pane, on the menu bar, click Create.

5 In the Settings section, enter a new name for the virtual disk, and for the Layout, choose RAID-10. Verify that Read Policy is set to Read Ahead, Write Policy is Write Back and Strip Size Element is 64KB.

6 Leave the rest of the settings at their default values.
7 Scroll down to **Internal Disks**, select all four available disks, and verify the value for **Capacity**.

![Image of iDRAC interface showing internal disks and RAID configuration]

8 On the **Apply Operation Mode** drop-down menu, choose either **Apply Now**, **Add to Pending Operations**, or **At Next Reboot**.

**Note:** The **At Next Reboot** option requires you to reboot the appliance before the virtual disk is initialized.

9 In the lower right corner, click **Create Virtual Disk** and at the prompt, click **OK**. Refresh the page.

**Note:** If you see a message that the capacity is out of range, remove the last decimal value from **Capacity** and try again.

A reboot may be required on the R720 to initialize the new virtual disk.

10 In the left pane, select **Storage**. Verify that all eight disks are in the **Ready** state, and the **Virtual Disks** count is 2.
Configuring the RAID 10 array using the RAID Controller BIOS

These instructions assume you’ve already installed the new hard drives and the server is powered down.

To configure the RAID 10 Array using the RAID Controller BIOS

1. Turn on the server and press **Ctrl+R** during the boot sequence to enter the RAID Controller Configuration utility.

2. Make sure that your hard drives are detected by the RAID Configuration Utility.
3. Select the controller name, press **F2**, and select **Create New VD**.

![Create New VD](image)

4. In the **RAID Level** field, select **RAID-10** and then under **Physical Disks**, select all the drives.

Under **Basic Settings**, keep the default **VD Size** and optionally, name the VD.

![Basic Settings](image)
5. Click **Advanced** and on the **Create Virtual Disk-Advanced** panel, select **Initialize** and click **OK**.

---

**Note:** Verify that the **Read Policy** is set to **Read Ahead**, **Write Policy** is **Write Back**, and **Strip Size** is 64KB.
6 After the initialization is complete, click **OK**, and then click **OK** again.

![RAID Controller BIOS](image1.png)

7 Press **Esc** then **Ctrl+Alt+Delete** to reboot the server.

![RAID Controller BIOS](image2.png)
List of upgrade components for ATP appliances

The ATP 8880 appliance upgrade components are specific to each platform model:

<table>
<thead>
<tr>
<th>Platform Model Number</th>
<th>Quantity</th>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>R720XL</td>
<td>4</td>
<td>Hard Drive- Dell Part # 400-AJQM</td>
<td>1.8TB 10K RPM SAS 512e 2.5in Hot-plug Hard Drive with 12G Customer Kit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16 GB RDIMM Memory Module- Dell Part # A7187318</td>
<td>Dell 16GB Certified Memory Module - 2Rx4 DDR3 RDIMM 1866MHz SV.</td>
</tr>
<tr>
<td>R730XL</td>
<td>4</td>
<td>Hard Drive- Dell Part # 400-AJQP</td>
<td>1.8TB 10K RPM SAS 512e 2.5in Hot-plug Hard Drive, with 13G Customer Kit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16 GB RDIMM Memory Module- Dell Part # 370-ACNU or A8711887</td>
<td>Dell 16GB RDIMM, 2400MT/s, Dual Rank, x8 Data Width</td>
</tr>
</tbody>
</table>
Upgrading Symantec Advanced Threat Protection (ATP) VMs

This chapter includes the following topics:

- About upgrading ATP virtual installations for ATP 3.0 with Endpoint Data Recorder enabled
- Upgrading ATP VMs for ATP 3.0

About upgrading ATP virtual installations for ATP 3.0 with Endpoint Data Recorder enabled

To support ATP 3.0 with Endpoint Data Recorder enabled, the available resources of existing ATP virtual installations must be increased:

**Note:** The VM must be upgraded before you can install ATP 3.0

- Memory is increased from 32GB RAM to 48GB RAM.
- CPU is increased from 4 cores to 12 cores.
- Hard disk is increased from 1x 500GB to ~2.5TB by adding an additional 2TB drive.

The workflow proceeds as follows:

1. Use the VMware vSphere Client to increase the resources for the VM.
2. Run the `extend_storage` tool to configure the storage for use by ATP 3.0.

See “Running the `extend_storage` tool” on page 25.
3. Install ATP 3.0.

Before you start

Before you start the VM upgrade procedure, be aware of the following:

- Make sure the ESX server hosting the virtual ATP instance has enough resources to support the upgrade.
- The virtual upgrade requires a reboot of the virtual machine so be sure to schedule a service interruption and notify concerned users and management. In testing, the upgrade procedure requires about 30 minutes, however you may want to schedule more time to avoid unmet expectations should the procedure take longer.
- Leave the existing 500GB hard drive intact; you are adding an additional 2 TB hard drive.

Upgrading ATP VMs for ATP 3.0

Use the following procedure to add additional storage to the existing ATP VM:

To Add Additional Storage

1. In the VMware vSphere Client, choose: View > Inventory > Hosts and Clusters.
2. Right-click ATP VM, and choose Edit Settings.
3. Under Hardware, choose Add....
4. Select Hard Disk and click Next.
5. For Disk Size, enter 2 TB, select Thick Provision Lazy Zeroed, Store with the virtual machine, and click Next.
6. Accept the default Advanced options, and click Next.
7. Click Finish.
8. To change the memory allocation, under Hardware, select Memory and increase the memory to 48 GB.
   To change the CPU cores, select CPU and on the Number of cores per socket drop-down menu, increase the number of cores to 12.
9. Click OK.
Running the expand_storage CLI tool

This chapter includes the following topics:

■ Running the extend_storage tool

Running the extend_storage tool

After you increase the storage capacity of your Symantec Advanced Threat Protection (ATP) appliance or VM, you must run the extend_storage tool to complete the upgrade process.

The tool does the following:

■ Detects and partitions the new drive.
■ Generates log messages regarding tool execution.
■ Allots 45% of the new storage to Elasticsearch, and 55% to backup and restore.

Warning: Backup ATP data before using this tool. All data is erased during the execution of this tool!

Caveats

Be aware of the following caveats regarding the operation of the tool:

■ The tool operates on one disk per tool run. To extend disk space using multiple disks, you must run the tool for each disk.
■ The minimum free disk space required on an extendable disk is 10GB.
■ The maximum free disk space on an extended disk is 2TB for virtual and 16TB for physical.
■ The tool displays up to five disks to choose from at each session.
- The tool only checks for SCSI and SATA controllers.

Use the following procedure to run the extend_storage tool:

**To run the extend_storage tool**

1. Open a command-line interface on the upgraded ATP appliance or VM instance.
2. Type `extend_storage` and press Enter.
   
   The current data store size (total and available) is displayed along with a message strongly recommending you to back up your ATP data before extending storage.

3. At the `Do you want to proceed? [Y/N]` prompt, type `Y` and then press Enter. The tool proceeds to convert the backup partition and check the disk(s).
   
   A message is displayed: **Invalid new disks detected**, and the new disk is listed along with information about the available space on the disk.

4. You are prompted to select a new disk. Enter the appropriate number and then press Enter.

   The tool runs and displays status information and the available space, followed by a message that the tool has run successfully.

The following screen shot provides an example:

```
localhost> extend_storage
The current data store has 109.9GB in total and 104.3GB available,
Backup ATP data is strongly recommended before extending storage.

Do you want to proceed? [Y/N]: y
Converting the backup partition. . . . . . . Done
Checking disks...

Invalid new disks detected:
- Disk: /dev/sdd, Free: 200MB, Needed: 10GB to 2TB

Please choose from the following new disks:

(1) Disk: /dev/sdb, Free: 10GB, Data Store Increase: 3.3GB, Backup Store Increase: 6.7GB

Please select a disk or choose 0 to exit. [1-1]: 1
Please wait. This may take many minutes to complete.
Creating partition in the selected disk:/dev/sdb ........ Done
Configuring the mount point for new storage. . . . . . . Done.
Configuring the data store. . . . . Done
The current data store has 113.1GB in total and 107.3GB available,
Extend storage is completed successfully.
```
Related documentation

This chapter includes the following topics:

- Related documentation

Related documentation

See the following documentation for more information about Symantec™ Advanced Threat Protection 3.0:

- Symantec™ Advanced Threat Protection 3.0 Installation Guide
- Symantec™ Advanced Threat Protection 3.0 Administration Guide
- Symantec™ Advanced Threat Protection 3.0 Security Operations Guide
- Symantec™ Advanced Threat Protection Platform 3.0 Release Notes