


Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.11

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2012-2025 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Windows Vista®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States and other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

Chapter 1: Introduction.....	4
Contact Dell ProSupport for Software.....	4
Chapter 2: Get Started.....	5
Provision a Tenant.....	5
Provision a Tenant.....	5
Provisioning and Agent Communication.....	5
Enable BIOS Image Integrity Verification.....	8
Verification Process.....	8
Configure Advanced Threat Prevention Agent Auto Update.....	10
Assign or Modify Administrative Roles.....	10
Set Up Notifications.....	11
Chapter 3: Policies.....	12
Enable Advanced Threat Prevention.....	12
Recommended Policy Settings.....	12
Commit Policy Modifications.....	12
Chapter 4: Threats.....	13
Identify a Threat.....	13
Manage a Threat.....	16
Chapter 5: Disconnected Mode.....	18
Identify and Manage Threats in Disconnected Mode.....	18
Chapter 6: Troubleshooting.....	20
Recover Advanced Threat Prevention.....	20
Find the Product Code with Windows PowerShell.....	20
Advanced Threat Prevention.....	20

Introduction

Before you perform tasks explained in this guide, the following components must be installed:

- Endpoint Security Suite Enterprise - refer to *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*
- Security Management Server or Security Management Server Virtual Server - refer to *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Server Quick Start and Installation Guide*

This guide explains basic administration of Advanced Threat Prevention and should be used with *AdminHelp*, available in the Management Console.

Contact Dell ProSupport for Software

Before contacting Dell Support, run SupportAssist for a quick self-diagnostic test. Run [SupportAssist Quick Test](#).

For additional assistance, visit dell.com/support. Online support at dell.com/support provides access to drivers, manuals, technical advisories, FAQs, and information on emerging issues.

When contacting Dell Support, keep your Service Tag or Express Service Code ready. This helps route your request to the appropriate technical expert quickly.

For international contact details, see [Dell ProSupport for Software international phone numbers](#).

Get Started

This chapter details the recommended steps to begin administering Advanced Threat Prevention.

The recommended steps to begin administering Advanced Threat Prevention include the following phases:

- [Provision a Tenant for Advanced Threat Prevention](#)
 - Required to deploy Advanced Threat Prevention
 - Advanced Threat Prevention licenses must be present in the Dell Server
- [Configure Advanced Threat Prevention Agent Auto Update](#)
 - Enroll for Advanced Threat Prevention auto updates (optional)
 - Updates are released monthly
- [Assign or Modify Administrative Roles](#)
 - Provision or recover the Advanced Threat Prevention service
 - Back up and download existing Advanced Threat Prevention certificates
 - View, modify, and commit policies
- [Set up Notifications](#)
 - Set email and dashboard notifications for Advanced Threat Prevention alerts (optional)
 - Customize notifications based on your enterprise's needs

Provision a Tenant

A tenant must be provisioned in the Dell Server before Advanced Threat Prevention enforcement of policies becomes active.

Prerequisites

- Must be performed by an administrator with the system administrator role.
- Must have connectivity to the Internet to provision on the Dell Server.
- Must have connectivity to the Internet on the client to display the Advanced Threat Prevention online service integration in the Management Console.
- Provisioning is based off of a token that is generated from a certificate during provisioning.
- Advanced Threat Prevention licenses must be present in the Dell Server.

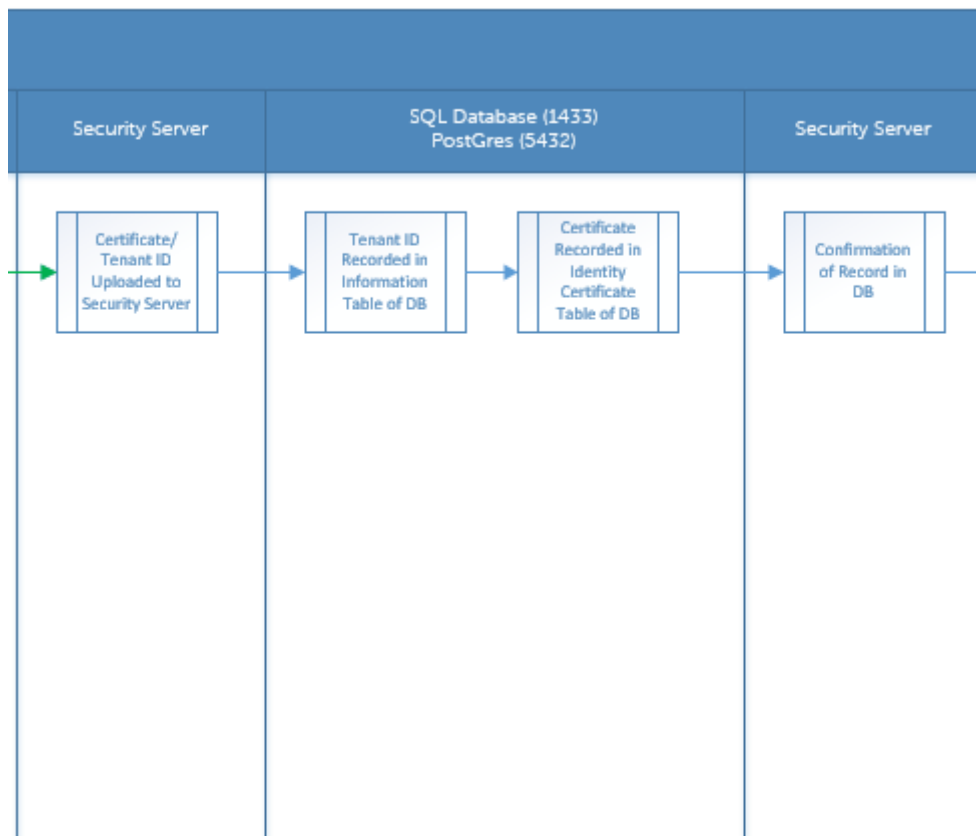
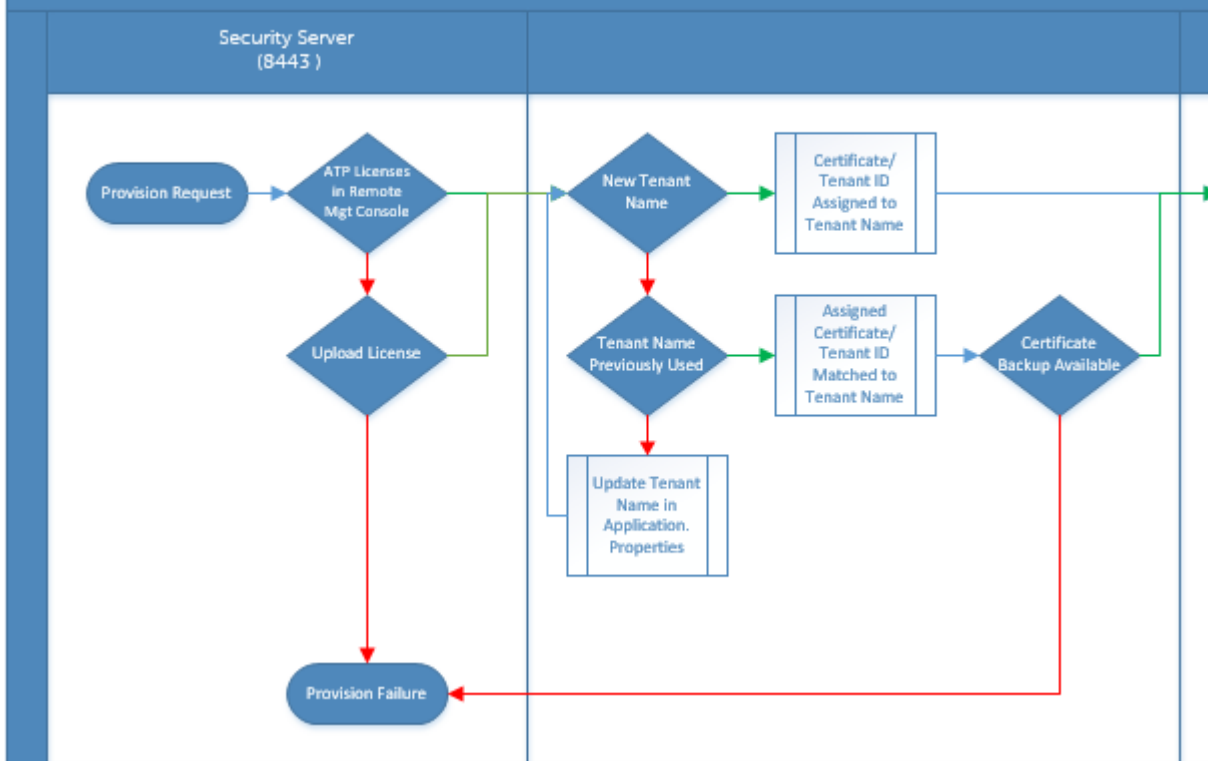
Provision a Tenant

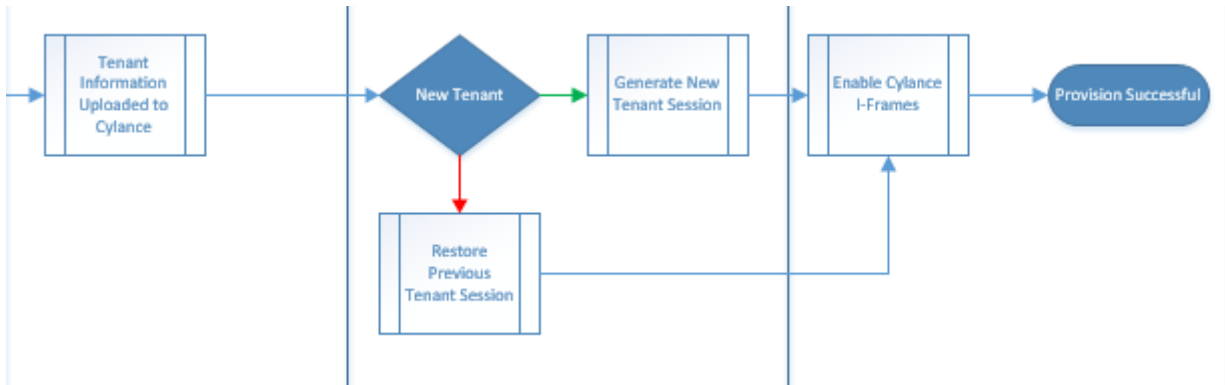
1. As a Dell administrator, log in to the Management Console.
2. In the left pane of the Management Console, click **Management > Services Management**.
3. Click **Set Up Advanced Threat Protection Service**. Import your Advanced Threat Prevention licenses if failure occurs at this point.
4. The guided set up begins once the licenses are imported. Click **Next** to begin.
5. Read and agree to the EULA and click **Next**.
6. Provide identifying credentials to the Dell Server for provisioning of the Tenant. Click **Next**. *Provisioning an existing Tenant that is Cylance-branded is not supported.*
7. Download the Certificate. This is required to recover if there is a disaster scenarios with the Dell Server. This Certificate is not automatically backed up. Back up the Certificate to a safe location on a different computer. Select the check box to confirm that you backed up the Certificate and click **Next**.
8. Set up is complete. Click **OK**.

Provisioning and Agent Communication

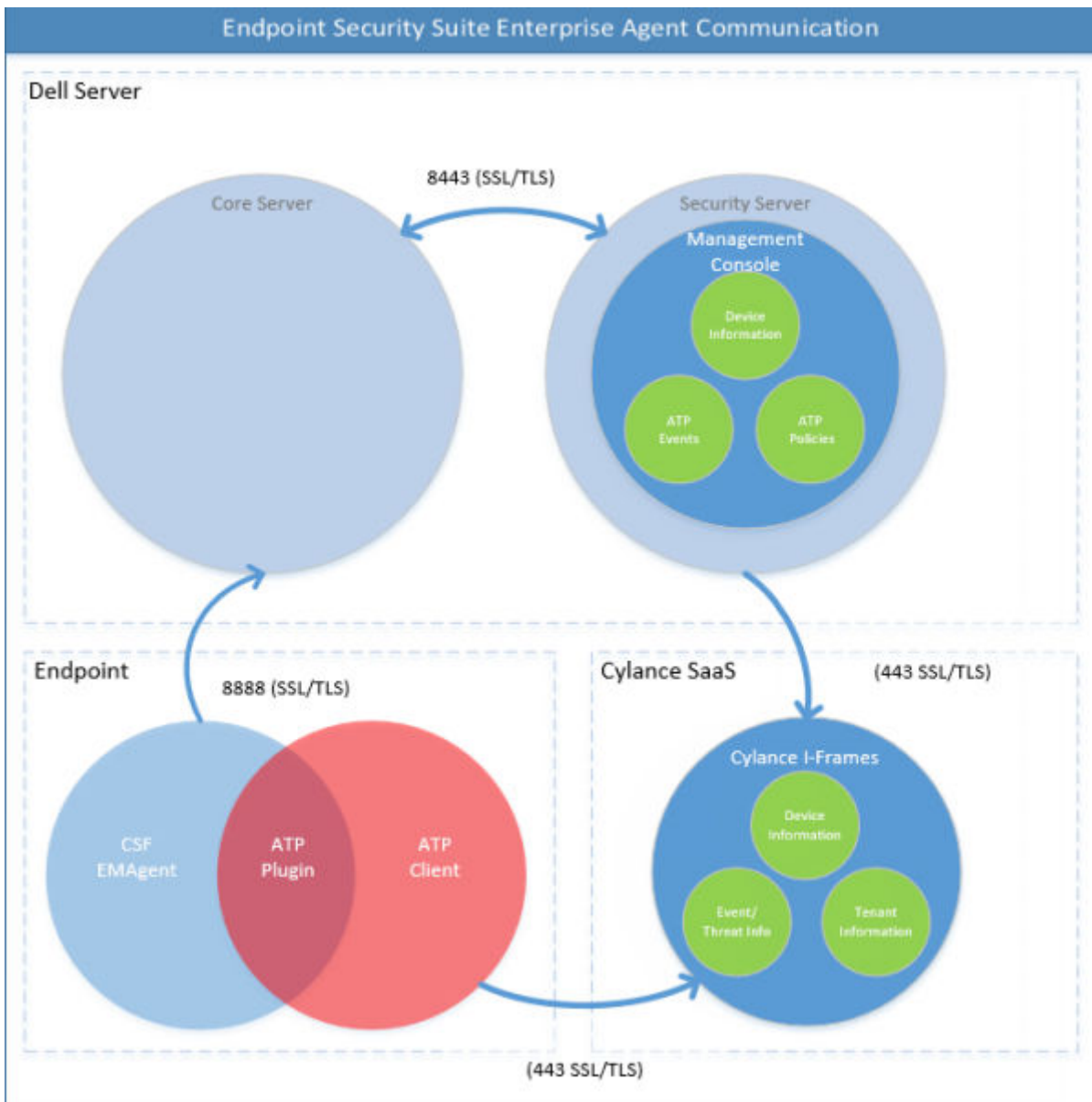
The following diagrams illustrate Advanced Threat Prevention service provisioning process.

Advanced Threat Prevention Service Provisioning Process





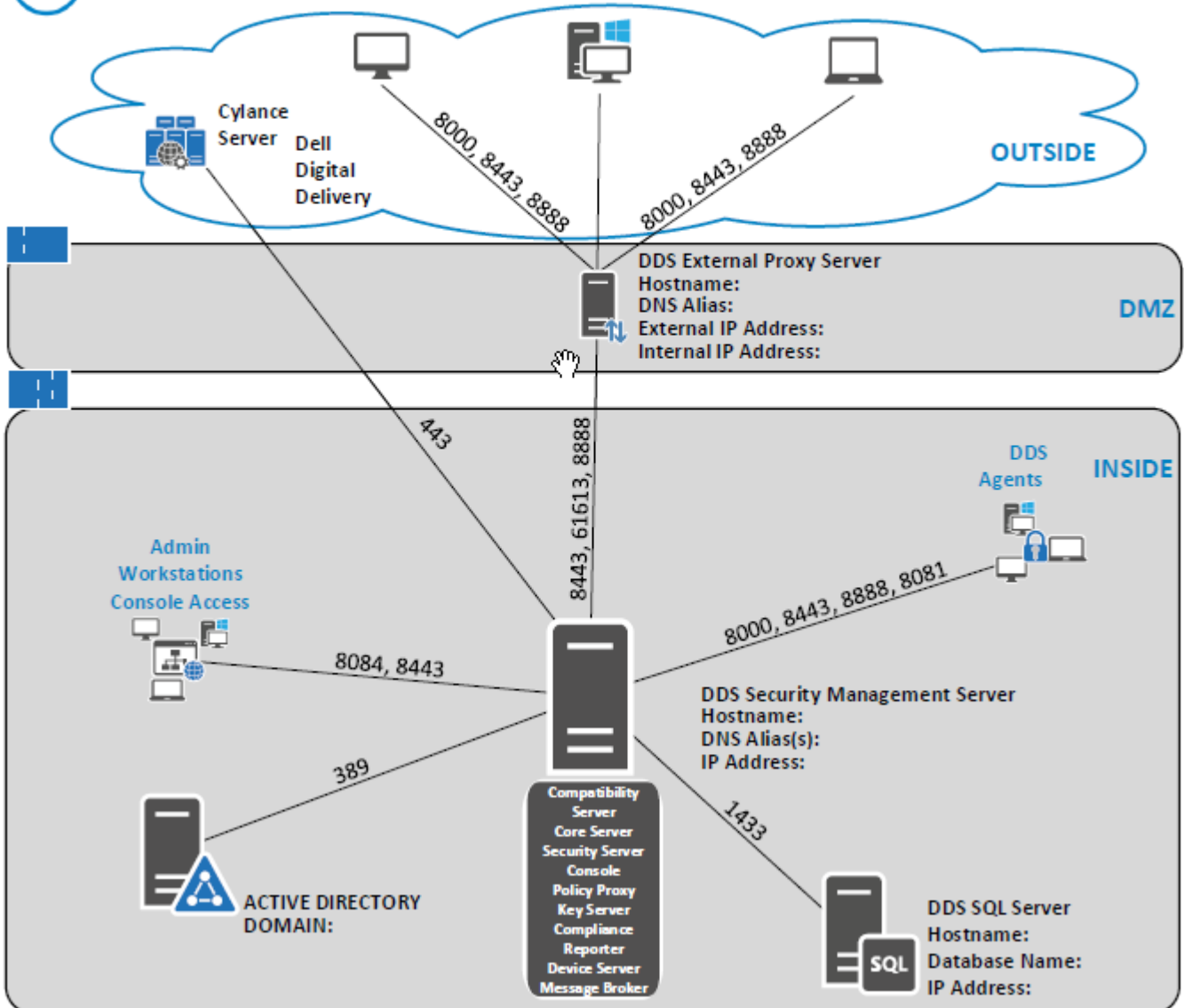
The following diagram illustrates the Advanced Threat Prevention agent communication process.



The following diagram illustrates Dell Server architecture and communication.



DELL Data Security



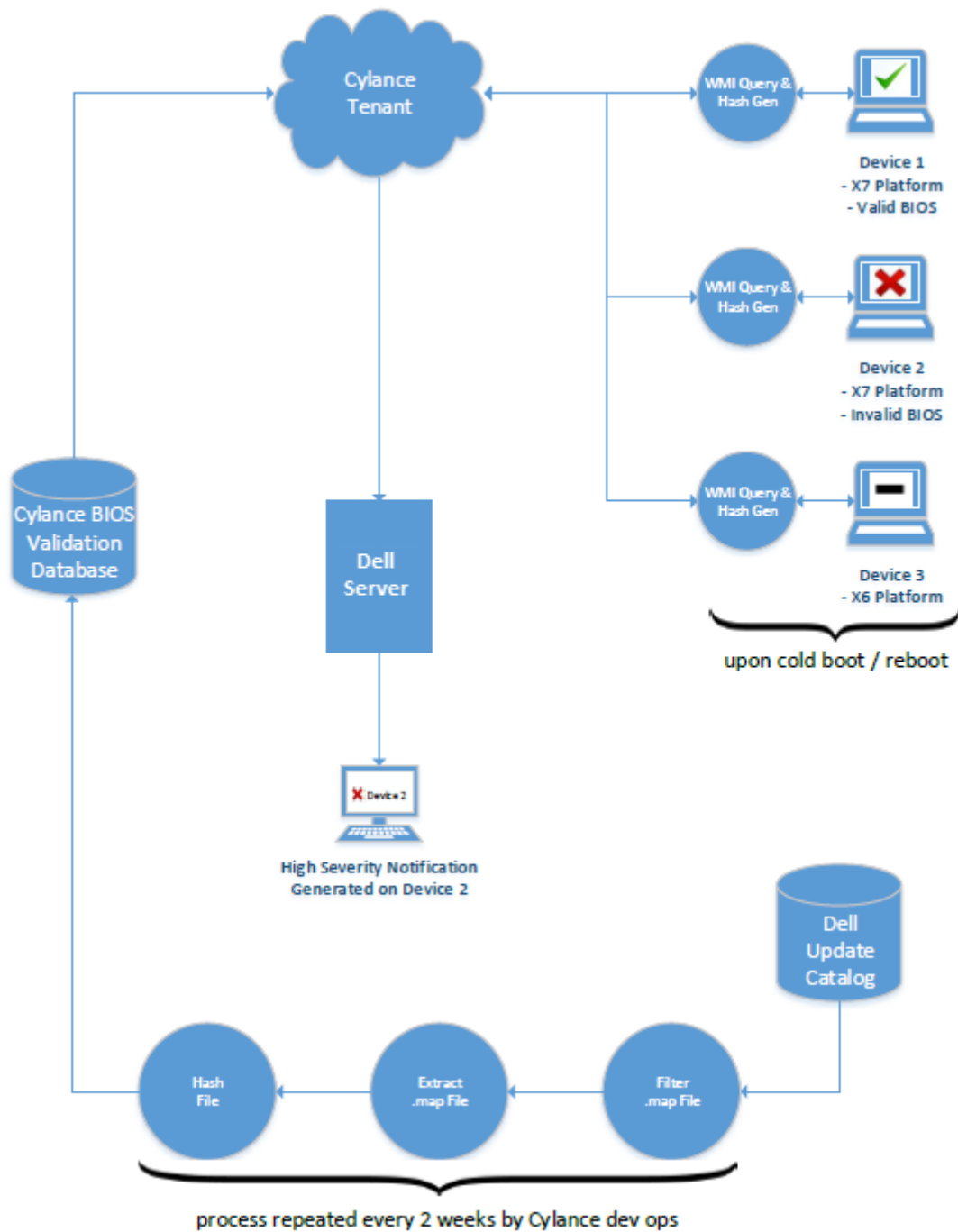
Enable BIOS Image Integrity Verification

The BIOS Image Integrity Verification policy is enabled by default when the master switch for Advanced Threat Prevention is enabled.

For an overview of BIOS Image Integrity Verification process, refer to [BIOS Image Integrity Verification Process](#).

Verification Process

The following diagram illustrates the BIOS image integrity verification process.



If the *Enable BIOS Assurance* policy is selected in the Management Console, the Cylance tenant validates a BIOS hash on endpoint computers to ensure that the BIOS has not been modified from the Dell factory version, which is a possible attack vector. If a threat is detected, a notification is passed to the Dell Server and the IT administrator is alerted in the Remote Management Console. For an overview of the process, see [BIOS Image Integrity Verification Process](#).

NOTE: A custom factory image cannot be used with this feature, as the BIOS has been modified.

Dell Computer Models supported with BIOS Image Integrity Verification	
<ul style="list-style-type: none"> Latitude 3470 Latitude 3570 Latitude 7275 Latitude 7370 Latitude E5270 Latitude E5470 	<ul style="list-style-type: none"> OptiPlex 5040 OptiPlex 7040 OptiPlex 7440 Precision Mobile Workstation 3510 Precision Mobile Workstation 5510 Precision Workstation 3620

Dell Computer Models supported with BIOS Image Integrity Verification	
<ul style="list-style-type: none"> • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240 	<ul style="list-style-type: none"> • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550

Configure Advanced Threat Prevention Agent Auto Update

In the Management Console, you can enroll to receive Advanced Threat Prevention agent auto updates. Enrolling to receive agent auto updates allows clients to automatically download and apply updates from the Advanced Threat Prevention service. Updates are released monthly.

NOTE:

Agent auto updates are supported with Dell Server v9.4.1 or later.

Receive agent auto updates

To enroll to receive agent auto updates:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. On the *Advance Threats* tab, under *Agent Auto Update*, click **On** then click **Save Preferences**.

It may take a few moments for the information to populate and for auto updates to display.

Stop receiving agent auto updates

To stop receiving agent auto updates:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. On the *Advance Threats* tab, under *Agent Auto Update*, click **Off** then click **Save Preferences**.

Assign or Modify Administrative Roles


View or modify existing Administrator privileges from the Administrators page in the Management Console.

Administrator Roles

Administrator login is integrated with Active Directory to simplify the process of managing administrators and to allow you to leverage your existing user authentication infrastructure. Administrators are assigned roles that define what level of access each administrator is allowed. For example, some administrators may only be allowed to implement help desk assisted recovery while others have full access to edit security policies. You can assign administrator roles to Active Directory groups so you can easily change the level of administrator access users have with a simple change to AD group membership. Non-domain users can be granted reporting-only access via Compliance Reporter.

The System administrator role is required to perform the following tasks:


- Provision or recover the Advanced Threat Prevention service
- Enroll for Advanced Threat Prevention auto updates
- Set email or dashboard notifications for Advanced Threat Prevention alerts
- Back up and download existing Advanced Threat Prevention certificates

 NOTE: The security administrator role is required to view, modify, or commit policies.

To view or modify existing administrator privileges, follow these steps:

1. In the left pane, click **Populations > Administrators**.
2. Search or select the row that displays the user name of the appropriate administrator to display User Detail.

3. View or modify administrator roles in the right pane.
4. Click **Save**.

 **NOTE:** Dell recommends assigning administrator roles at the Group level rather than at the User level.

To view, assign, or modify administrator roles at the Group level, follow these steps:

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group name, then the **Admin** tab. The user group detail page displays.
3. Select or deselect the administrator roles assigned to the Group.
4. Click **Save**.

If you remove a Group that has Administrative privileges and later re-add the Group, it remains an Administrator Group.

To view, assign, or modify Administrator Roles at the User level, follow these steps:

1. In the left pane, click **Populations > Users**.
2. Search or select a user name, then the Admin tab.
3. Select or deselect the administrator roles assigned to the user.
4. Click **Save**.

Administrator Roles - Assign or modify roles for the user and click **Save**.

Inherited Group Roles - A read-only list of roles that the user inherited from a Group. To modify the roles, click the **User Groups** tab for that user and select the Group Name.

Designated Roles - Delegate administrator rights to a user.

Set Up Notifications

In the Remote Management Console, you can enroll to receive notifications. The Notifications list provides a configurable summary of news, alerts, and events to display on the Dashboard or to be sent as email notifications.

Notification Types

You can select the notification types to include in the list. Notifications of the remaining types are hidden. **Threat Protection** and **Advanced Threat Event** notifications pertain to Advanced Threat Prevention.


Types include:

- **Update** - News of upcoming product updates. To view and receive product updates, you must enroll to receive them. Select **Services Management > Product Notifications**, click **On**, then click **Save Preferences**.
- **Config** - News about configuration changes.
- **Knowledge Base** - Summaries and links to knowledge base articles with in-depth technical information such as work-arounds and configuration methods.
- **Announcement** - News of upcoming releases and new products.
- **License** - Alerts when your volume license availability is low, or when your client access license count has been exceeded.
- **Threat Protection** - A threat alert from Advanced Threat Prevention.
- **Advanced Threat Event** - An event detected by Advanced Threat Prevention. The summary contains a listing of Critical, Major, Minor, Warning, and Information events, with links to more detailed information.
- **Threat Event** - An event detected by Threat Protection.
- **Certificate** - Certificate expiration notification.
- **Dell Server Exceptions** - A Dell Server communication issue is impacting the deliveries of the following notifications: Threat Protection, Update, Config, Knowledge Base, and Announcement.

After selecting one or more types, click in the neutral space above the list to apply the selections.

Select **Clear selected items** to reset the selections in this list.

Priority Levels

 **NOTE:** Notification priority levels are not related to priority levels displayed on the dashboard other than in the Notifications area.

Priorities are Critical, High, Medium, and Low. These priority levels are only relative to one another within a type of notification.

You can select priority levels of notifications to include in the dashboard notifications area or email notifications lists. Notifications of the remaining priority levels are not included in the dashboard or email notifications lists.

Select **Clear selected items** to reset the selections in this list. All notifications will display (unless filtered elsewhere).

Policies

This chapter details policy management for Advanced Threat Prevention.

- [Enable Advanced Threat Prevention](#)
- [Recommended Policy Settings](#)
- [Commit Policy Modifications](#)

For the complete list of Advanced Threat Prevention policies and their descriptions, refer to *AdminHelp*, available in the Management Console.

Enable Advanced Threat Prevention

The Advanced Threat Prevention policy is toggled **Off** by default and must be toggled **On** to enable Advanced Threat Prevention policies. Advanced Threat Prevention policies are enforceable at the Enterprise, Endpoint Group, and Endpoint levels.

To enable the Advanced Threat Prevention policy at the Enterprise level, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click **Threat Prevention**.
3. Toggle the Advanced Threat Prevention master switch from **Off** to **On**.

To enable the Advanced Threat Prevention policy at the Endpoint Group level, follow these steps:

1. In the left pane, click **Populations > Endpoint Group**.
2. Click **Threat Prevention**.
3. Toggle the Advanced Threat Prevention master switch from **Off** to **On**.

To enable the Advanced Threat Prevention policy at the Endpoint level, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Click **Threat Prevention**.
3. Toggle the Advanced Threat Prevention master switch from **Off** to **On**.

Recommended Policy Settings

- For the most up-to-date list of recommended policy settings, see KB article [SLN301562](#).

Commit Policy Modifications

To commit policies that have been modified and saved:

1. In the left pane of the Management Console, click **Management > Commit**.
2. In Comment, enter a description of the change.
3. Click **Commit Policies**.

A policy publication/commit occurs when an administrator clicks **Commit Policies**. The following information displays:

- Pending Policy Changes - The number of policy changes ready to commit.
- Date Committed - Date and time the policies were committed.
- Changed by - User name of the administrator who performed the policy commit.
- Comment - Any comments that were added when the policies were committed.
- Version - The number of policy saves since the last policy commit plus the previous Version.

Threats

This chapter details how to identify and manage threats encountered in an enterprise environment following the installation of Advanced Threat Prevention.

- [Identify a Threat](#)
 - View Threat Events
 - Cylance Score and Threat Model Updates
 - View Detailed Threat Data
- [Manage a Threat](#)
 - Export Threat Data to CSV
 - Manage the Global Quarantine list

Identify a Threat

Email and Dashboard Notifications

If you have set up email notifications for Threat Protection and Advanced Threat Events, an administrator is notified by email of Advanced Threat Prevention events and threats.

The dashboard Notifications Summary in the Management Console displays Advanced Threat Prevention threats and events as Threat Protection and Advanced Threat Events notification types.

- Threat Protection type - A threat alert from Advanced Threat Prevention.
- Advanced Threat Event type - An event detected by Advanced Threat Prevention. An event is not necessarily a threat.

The following table details threat labels, severity, and threat information.

Label	Severity	Detail
ThreatFound	Critical	Indicates a Portable Executable (PE) has been identified on a device, but has not been blocked or otherwise quarantined on the endpoint, indicating an active threat on the system.
ThreatBlocked	Warning	Indicates a Portable Executable has been identified on the device, though its execution has been blocked. This threat has not been specifically quarantined, and is likely due to either the policy to Automatically Quarantine has not been enabled, or that the file is in a location that we are unable to write to with the local SYSTEM account (network share, USB device that has been removed, etc).
ThreatTerminated	Warning	Indicates a Portable Executable (PE) has been identified on the device, and it's process was killed, as it was found to be actively running. This does not indicate that the file was also quarantined, as the PE could have been executed from another location. It is suggested to look for another event correlated with this endpoint and executable to validate that the threat was properly contained.
MemoryViolationBlocked	Warning	Indicates that an executable or script attempted to run, but was in violation of the Memory Protection or Script Control policy. The execution of the executable or script was subsequently blocked. Typically this denotes the correlating Memory Protection or Script Control policy outlined was set to Block.
MemoryViolationTerminated	Warning	Indicates that an executable or script was found to be actively running and in violation of the Memory Protection or Script Control policy. The executable or script was subsequently terminated.

Label	Severity	Detail
		Typically this denotes the correlating Memory Protection or Script Control policy outlined was set to Terminate.
MemoryViolation	Warning	Indicates that an executable or script was found that was in violation of the Memory Protection or Script Control Policy. The executable or script had no action taken against it, likely due to policy being set to Allow.
ThreatRemoved	Information	Indicates that a previously flagged Portable Executable (PE), that was considered to be a threat, was removed from the endpoint. This could indicate that the PE was removed from quarantine, or removed from the initial location. This is common to see with PEs that were initially detected on removable media (USB, CD-ROM, etc)
ThreatQuarantined	Information	Indicates that a Portable Executable (PE) was determined to be a potential threat, and was subsequently placed within the quarantine successfully. This indicates that the policy to Automatically Quarantine threats based on it's classification of Abnormal (Cylance Score of 0 – 60) or Unsafe (Cylance Score of 60 – 100) is enabled.
ThreatWaived	Information	Indicates a Portable Executable (PE) that was determined to be a potential threat, has been Waived based on the Global SafeList or by a local Waive. This could also indicate that the SHA256 hash has been added to the "Waive" or "Global Safe List" policies within the Dell Security Management Server.
ThreatChanged	Information	Denotes when a Portable Executable's (PE) Cylance score has changed. This typically happens due to the two-step scoring that is done by Cylance. The local scoring engine's analysis of the threat may have not matched the Cylance cloud engine's analysis. In these instances, due to the additional data that the Cylance cloud engine has, the score derived by the Cylance cloud engine is used. This may also indicate that an update to Cylance has initialized a re-analysis of files that were previously deemed threats, and a new score was calculated that resolved this PE to no longer be considered a threat.
ProtectionStatusChanged	Information	Denotes when an endpoint has had any protection status changed. This is triggered when the Dell Encryption Management Agent re-connects to the Cylance services through the Cylance Plugins. This is commonly triggered when an endpoint has rebooted, as there is a small period where the CSF may have not connected to the Cylance Plugins during boot.

Click a notification for more details. The summary includes links to additional threat or event detail.

The Advanced Threats tab

The Advanced Threats tab provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events.

To access the Enterprise Advanced Threats Tab, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.

Information about events, devices, and actions are organized on the following tabs:

- **Protection** - Lists potentially harmful files and scripts ad details about them, including the devices on which the files and scripts are found.
- **Agents** - Provides information about devices running the Advanced Threat Prevention client as well as the option to export the information or remove devices from the list.
- **Global List** - Lists files in the Global Quarantine and Safe List and provides the option to move files to these lists.

- **Options** - Provides a way to integrate with Security Information Event Management (SIEM).
- **Certificate** - Allows certificate upload. After upload, certificates display on the Global List tab and can be Safe listed.

Tables on the tabs can be organized in these ways:

- Add or remove columns from the table - Click the arrow next to any column header, select **Columns**, then select the columns to display. Clear the check box of columns to hide.
- Sort the data - Click a column header.
- Group by a column - Drag the column header up until it turns green.

Advanced Threat Events tab

The Advanced Threat Events tab displays information about events for the entire enterprise based on information available in the Dell Server.

The tab displays if the Advanced Threat Prevention service is provisioned and licenses are available.

To export data from the Advanced Threat Events tab, click **Export** and select **Excel** or **CSV** file format.

 **NOTE:** Excel Files are limited to 65,000 rows. CSV has no size limit.

Cylance Score and Threat Model Updates

A Cylance score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.

The predictive threat model used to protect devices receives periodic updates to improve detection rates.

Two columns on the Protection page in the Management Console show how a new threat model affects your organization. Display and compare the Production Status and New Status columns to see which files on devices might be impacted by a model change.

To view the Production Status and New Status columns:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.
3. Click the **Protection** tab.
4. Click the down-arrow on a column header in the table.
5. Hover over **Columns**.
6. Select the **Production Status** and **New Status** columns.

Production Status - Current model status (Safe, Abnormal or Unsafe) for the file.

New Status - Model status for the file in the new model.

For example, a file that was considered Safe in the current model might change to Unsafe in the new model. If your organization needs that file, you can add it to the Safe list. A file that has never been seen or scored by the current model might be considered Unsafe by the new model. If your organization needs that file, you can add it to the Safe list.

Only files found on device in your organization and that have a change in its Cylance Score are displayed. Some files might have a Score change but still remain within its current Status. For example, if the Cylance Score for a file goes from 10 to 20, the file status may remain Abnormal and the file displays in the updated model list (if this file exists on devices in your organization).

Compare Current Model with New Model

You can now review differences between the current model and the new model.

The two scenarios you should be aware of are:

Production Status = Safe, New Status = Abnormal or Unsafe

- Your Organization considers the file as Safe
- Your Organization has Abnormal and/or Unsafe set to Auto-Quarantine

In the above scenarios, the recommendation is to Safelist the files to allow in your organization.

Identify Classifications

To identify classifications that could impact your organization, Dell recommends the following approach:

1. Apply a filter to the New Status column to display all Unsafe, Abnormal, and Quarantined files.
2. Apply a filter to the Production Status column to display all Safe files.
3. Apply a filter to the Classification column to only show Trusted - Local threats.

Trusted - Local files have been analyzed by Cylance and found to be safe. Safelist these items after review. If you have a lot of files in the filtered list, you may need to prioritize using more attributes. For example, add a filter to the Detected By column to

review threats found by Execution Control. These were convicted when a user attempted to execute an application and need more urgent attention than dormant files convicted by Background Threat Detection or File Watcher.

The information for the model comparison comes from the database, not your devices. So no re-analysis is done for the model comparison. However, when a new model is available and the proper Agent is installed, a re-analysis is done on your organization and any model changes are applied.

Refer to *AdminHelp* for more information.

View Web Protection and Firewall Events

Threats are categorized as Malware/Exploit, Web Filter, Firewall, or Uncategorized events. The list of threat events can be sorted by any of the column headers. You can view threat events for the entire enterprise or for a specific endpoint. To view threat events of a specific endpoint, from the Enterprise Threat Events tab, select the device in the Device ID column.

To view threat events in the enterprise, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click the **Threat Events** tab.
3. Select the desired severity level and time period for which to display events.

To view threats on a specific endpoint, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Threat Events** tab.

Manage a Threat

You can Quarantine, Safe List, Waive, and Export threats.

Perform the following actions at the Enterprise level:

- Export a threat or script that has triggered an alert
- Quarantine a threat
- Safe List a threat
- Manually edit the Global List

To manage a threat identified at the Enterprise level:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.
3. Select Protection.

From the Script Control Table, you can Export a script that is listed in the table as a potential threat.

Manage Enterprise Advanced Threats

The Protection tab provides information about files and scripts that are potentially harmful.

Threats Table

From the Threats table, you can Export, Quarantine, or Safe List a threat. You can also manually add a threat to the Global Quarantine List.


The table lists all events found across the organization. An event may also be a threat but is not necessarily so.

View additional information about a specific threat either by clicking on the threat name link to view the details displayed on a new page or by clicking anywhere in the row of the threat to view details at the bottom of the page.

To view additional threat information in the table, click the drop-down arrow on a column header to select and add columns. Columns display metadata about the file, such as Classifications, Cylance Score (confidence level), AV Industry conviction (links to VirusTotal.com for comparison with other vendors), Date first found, SHA256, MD5, File information (author, description, version) and Signature details.

Commands

- **Export** - Export threat data to a CSV file. Select the rows to export, and then click **Export**.
- **Global Quarantine** - Add file to the global quarantine list. The threat is permanently quarantined from all devices.
- **Safe** - Add a file to the safe list. The file is permanently treated as safe across all devices.

 **NOTE:** Occasionally, a "good" file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

- **Edit Global List** - Add or remove files from the global quarantine list.

- **Waive** - Add a file to the Waived list on a computer. This file is allowed to execute on the computer.

Manage Endpoint Advanced Threats

To manage a threat identified on a specific computer:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.
3. Select Agents.
4. Select a specific agent name, and select the appropriate command: **Export**, **Quarantine**, or **Waive** a threat.

Disconnected Mode

Disconnected mode allows a Dell Server to manage Advanced Threat Prevention endpoints without client connection to the Internet or external network. Disconnected mode also allows the Dell Server to manage clients without Internet connection or a provisioned and hosted Advanced Threat Prevention service. The Dell Server captures all event and threat data in Disconnected mode.

To determine if a Dell Server is running in Disconnected mode, click the gear icon at the top right of the Remote Management Console and select About. The About screen indicates that a Dell Server is in Disconnected mode, below the Dell Server version.

Disconnected mode is different than a standard connected installation of Dell Server in the following ways.

Client Activation

An install token is generated when the administrator uploads an Advanced Threat Prevention license, which allows the Advanced Threat Prevention client to activate.

Management Console

The following items are **not available** in the Management Console when Dell Server is running in Disconnected mode:

- The following areas specific to Advanced Threat Prevention: Advanced Threats by Priority, (Advanced Threat) Events by Classification, Advanced Threats Top Ten, and Advanced Threat Prevention Events.
- **Enterprise > Advanced Threats** tab, which provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events.
- (Left navigation pane) Services Management, which allows enabling of the Advanced Threat Prevention service and product notifications enrollment.

The following item **is available** to the Management Console to support Disconnected mode:

- **Enterprise > Advanced Threat Events** tab, which lists events information for the entire enterprise based on information available in the Dell Server, even when running in Disconnected Mode.

Functionality

The following functionality is not available in the Management Console when Dell Server is running in Disconnected mode:

- Security Management Server upgrade, update, and migration
- Security Management Server Virtual auto update - update must be done manually
- Cloud profile update
- Advanced Threat Prevention auto update
- Upload of Unsafe or Abnormal Executable files for Advanced Threat Prevention analysis
- Advanced Threat Prevention file upload and log file upload

The following functionality differs:

- The Dell Server sends the Global Safe List, Quarantine List, and Safe List to agents.
- The Global Safe List is imported to the Dell Server through the Global Allow policy.
- The Quarantine List is imported to the Dell Server through the Quarantine List policy.
- The Safe List is imported to the Dell Server through the Safe List policy.

These policies are available only in Disconnected mode. For more information about these policies, see *AdminHelp* available in the Remote Management Console.

For more information about Disconnected mode, see "Disconnected Mode" in *AdminHelp*, available in the Management Console.

Identify and Manage Threats in Disconnected Mode

To manage threats in Disconnected, mode, you must first set the following Advanced Threat Prevention policies as applicable for your organization:

- Global Allow
- Quarantine List
- Safe List

These policies are sent to the Advanced Threat Prevention client only if the Dell Server detects a Disconnected Mode install token, which is prefixed with "DELLAG."

Refer to *AdminHelp* for examples of these policies.

To view files that Advanced Threat Prevention identifies as potential threats, navigate to **Enterprise > Advanced Threat Events** tab. This tab contains a list of events information for the entire enterprise and action taken, such as Blocked or Terminated.

Troubleshooting

Recover Advanced Threat Prevention

Recover Service

You will need your backed up certificate to recover Advanced Threat Prevention service.

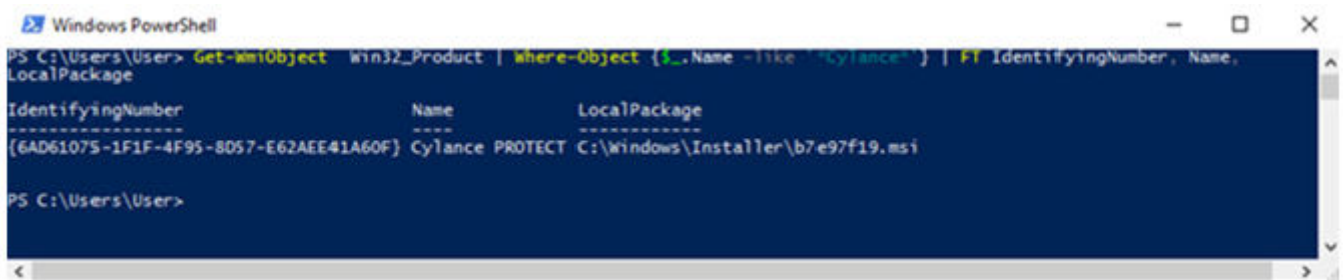
1. In the left pane of the Management Console, click **Management > Services Management**.
2. Click **Recover Advanced Threat Prevention Service**.
3. Follow the guided service recovery and upload the Advanced Threat Prevention certificate when prompted.

Find the Product Code with Windows PowerShell

- You can easily identify the product code, if the product code changes in the future, using this method.

```
Get-WmiObject Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT IdentifyingNumber, Name, LocalPackage
```

The output will result with the full path and .msi file name (the converted hex name of the file).



```
Windows PowerShell
PS C:\Users\User> Get-WmiObject Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT IdentifyingNumber, Name, LocalPackage

IdentifyingNumber      Name      LocalPackage
-----
{6AD61075-1F1F-4F95-8057-E62AEE41A60F} Cylance PROTECT C:\Windows\Installer\b7e97f19.msi

PS C:\Users\User>
```

Advanced Threat Prevention

- To have the Advanced Threat Prevention plugin monitor HKLM\SOFTWARE\Dell\Dell Data Protection for changes to the LogVerbosity value, and update the client log level accordingly, set the following value.

```
[HKLM\SOFTWARE\Dell\Dell Data Protection]
```

```
"LogVerbosity"=DWORD:<see below>
```

```
Dump: 0
```

```
Fatal: 1
```

```
Error 3
```

```
Warning 5
```

```
Info 10
```

```
Verbose 12
```

```
Trace 14
```

```
Debug 15
```

The registry value is checked when the Advanced Threat Prevention service starts or whenever the value changes. If the registry value does not exist, there is no change to the logging level.

Use this registry setting for testing/debugging only, as this registry setting controls log verbosity for other components, including Encryption and Encryption Management Agent.

- Compatibility Mode allows applications to run on the client computer while Memory Protection or Memory Protection and Script Control policies are enabled. Enabling compatibility mode requires adding a registry value on the client computer.

To enable compatibility mode, follow these steps:

1. In the Management Console, disable the *Memory Protection Enabled* policy. If the *Script Control* policy is enabled, disable it.
2. Add the CompatibilityMode registry value.
 - a. Using the Registry Editor on the client computer, go to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
 - b. Right-click **Desktop**, click **Permissions**, then take ownership and grant yourself Full Control.
 - c. Right-click **Desktop**, then select **New > Binary Value**.
 - d. For the name, type `CompatibilityMode`.
 - e. Open the registry setting and change the value to 01.
 - f. Click **OK**, then close Registry Editor.

To add the registry value with a command, you can use one of the following command line options to run on the client computer:

- (For one computer) Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
CompatibilityMode /t REG_BINARY /d 01
```

- (For multiple computers) Invoke-Command cmdlet:

```
$servers = "testComp1","testComp2","textComp3"
$credential = Get-Credential -Credential {UserName}\administrator
Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
-Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
01}
```

3. In the Management Console, re-enable the *Memory Protection Enabled* policy. If the *Script Control* policy was previously enabled, re-enable it.