Dell Endpoint Security Suite Enterprise for Mac

Administrator Guide v2.9

March 2021
Rev. A02

DELL EMC

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.

Contents

Chapter 1: Introduction **5**
Overview 5
FileVault Encryption 5
Contact Dell ProSupport 5

Chapter 2: Requirements **6**
Encryption Client 6
Encryption Client Hardware 6
Encryption Client Software 6
Advanced Threat Prevention 7
Advanced Threat Prevention Hardware 7
Advanced Threat Prevention Software 8
Advanced Threat Prevention Ports 8
Compatibility 8

Chapter 3: Tasks for the Encryption Client **11**
Install/Upgrade the Encryption Client 11
Interactive Installation or Upgrade 12
Command Line Installation/Upgrade 13
Enable Full Disk Access for Removable Media 15
Activate the Encryption Client 16
View Encryption Policy and Status 16
View Policy and Status in the Management Console 19
System Volumes 20
Enable Encryption 20
Encryption Process 21
Recycling FileVault Recovery Keys 23
User Experience 24
Recovery 25
Mount Volume 25
FileVault Recovery 26
Removable Media 30
Supported Formats 30
Encryption External Media and Policy Updates 30
Encryption Exceptions 30
Errors on the Removable Media Tab 30
Audit Messages 31
Collect Log Files for Endpoint Security Suite Enterprise 31
Uninstall the Encryption Client for Mac 31
Activation as Administrator 32
Activate 32
Activate Temporarily 32
Encryption Client Reference 32
About Optional Firmware Password Protection 32

Using Boot Camp....33
How to Retrieve a Firmware Password....35
Client Tool....35

Chapter 4: Tasks....38
Install Advanced Threat Prevention for Mac....38
Interactive Installation for Advanced Threat Prevention....38
Command Line Installation for Advanced Threat Prevention....41
Troubleshooting Advanced Threat Prevention for Mac....42
Verify the Advanced Threat Prevention Installation....43
Collect Log Files for Endpoint Security Suite Enterprise....44
View Advanced Threat Prevention Details....44
Provision a Tenant....46
Provision a Tenant....47
Configure Advanced Threat Prevention Agent Auto Update....47
Advanced Threat Prevention Troubleshooting....47

Chapter 5: Glossary....50

1

Introduction

The Endpoint Security Suite Enterprise for Mac Administrator Guide provides the information needed to deploy and install the client software.

Topics:

- Overview
- FileVault Encryption
- Contact Dell ProSupport

Overview

Endpoint Security Suite Enterprise for Mac offers Advanced Threat Prevention at the operating system and memory layers and encryption, all centrally-managed from the Dell Server. With centralized management, consolidated compliance reporting, and console threat alerts, businesses can easily enforce and prove compliance for all of their endpoints. Security expertise is built in with features such as pre-defined policy and report templates, to help businesses reduce IT management costs and complexity.

- Endpoint Security Suite Enterprise for Mac - a suite of software for client encryption of data and Advanced Threat Prevention.
- Policy Proxy - used to distribute policies
- Security Server - used for client encryption software activations
- Security Management Server or Security Management Server Virtual - provides centralized security policy administration, integrates with existing enterprise directories and creates reports. For the purposes of this document, both Servers are cited as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Security Management Server Virtual).

  These Dell components inter-operate seamlessly to provide a secure mobile environment without detracting from the user experience.

Endpoint Security Suite Enterprise for Mac has two .dmg files - one for the Encryption client and one for Advanced Threat Prevention. You can install both or one only.

FileVault Encryption

Dell Encryption can manage Mac FileVault full disk encryption. The *Dell Volume Encryption* policy must be set to **On** for encryption to take place and for other policy settings to function. For information on additional policies, see *AdminHelp*.

Only FileVault encryption is supported, which Endpoint Security Suite Enterprise will manage. If a computer has the *Dell Volume Encryption* policy set to **On** and *Encrypt Using FileVault for Mac* set to **Off**, a policy conflict message displays on the Encryption client. The administrator must set both policies to **On**.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

For phone numbers outside of the United States, check Dell ProSupport International Phone Numbers.

2

Requirements

Client hardware and software requirements are provided in this chapter. Ensure that the deployment environment meets the requirements before continuing with deployment tasks.

Topics:

- Encryption Client
- Advanced Threat Prevention

Encryption Client

Encryption Client Hardware

Minimum hardware requirements must meet the minimum specifications of the operating system.

Hardware
• 30 MB of free disk space
• 10/100/1000 or Wi-Fi network interface card
• System disk must be partitioned with the GUID Partition Table (GPT) partition scheme and can be formatted with one of these: ○ Mac OS X Extended Journaled (HFS+) - is converted to Core Storage to apply FileVault. ○ Apple File System (APFS)

Encryption Client Software

The following table details supported software.

Operating Systems (64-bit kernels)
• macOS High Sierra 10.13.6
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

NOTE: Dell Encryption does not support macOS Big Sur.

NOTE:

If you are using a network user account to authenticate, that account must be set up as a mobile account to fully configure FileVault 2 management.

Encrypted Media

The following table details the operating systems supported when accessing Dell-encrypted external media.

NOTE:

Encryption External Media supports:

- FAT32
- exFAT
- HFS Plus (MacOS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes. See Enable HFS Plus.

NOTE:

External media must have 55 MB available, plus open space on the media that is equal to the largest file to be encrypted, to host Encryption External Media.

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media
• Microsoft Windows 7 SP1 - Enterprise - Professional - Ultimate
• Microsoft Windows 8.1 - Windows 8.1 Update 1 - Enterprise - Pro
• Microsoft Windows 10 - Education - Enterprise - Pro v1607 (Anniversary Update/Redstone 1) through v1909 (November 2019 Update/19H2)
Mac Operating Systems (64-bit kernels) Supported to Access Encrypted Media
• macOS High Sierra 10.13.6 **NOTE:** Encryption External Media on macOS High Sierra 10.14.x requires Encryption Enterprise v8.16 or higher.
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

Advanced Threat Prevention

Uninstall other vendors' antivirus, antimalware, and antispyware applications before installing the Advanced Threat Prevention client, to prevent installation failures.

Advanced Threat Prevention Hardware

Minimum hardware requirements must meet the minimum specifications of the operating system.

Hardware
• 500 MB free disk space, depending on operating system • 2 GB RAM • 10/100/1000 or Wi-Fi network interface card

Advanced Threat Prevention Software

The following table details supported software.

Operating Systems (64-bit kernels)
• Mac OS X Mavericks 10.9.5 • Mac OS X Yosemite 10.10.5 • macOS Sierra 10.12.6 **NOTE:** Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5, and macOS Sierra 10.12 are supported with Advanced Threat Prevention only, not the Encryption client.
• macOS High Sierra 10.13.6 **NOTE:** Refer to Encryption Client Software for specific macOS High Sierra versions supported with the Encryption client.
• macOS Mojave 10.14.5 - 10.14.6 **NOTE:** You can install the ATP agent on macOS Mojave, but Memory Protection and Script Control features are automatically disabled and are not currently supported.
• macOS Catalina 10.15.3 - 10.15.4

NOTE:

There is no support for case-sensitive file systems.

Advanced Threat Prevention Ports

- The Advanced Threat Prevention agents are managed by and report to the management console SaaS platform. Port 443 (https) is used for communication and must be open on the firewall in order for the agents to communicate with the console. The console is hosted by Amazon Web Services and does not have any fixed IPs. If port 443 is blocked for any reason, updates cannot be downloaded, so computers may not have the most current protection. Ensure that client computers can access the URLs, as follows.

Use	Application Protocol	Transport Protocol	Port Number	Destination	Direction
All Communication	HTTPS	TCP	443	Allow all https traffic to *.cylance.com	Outbound

Compatibility

The following table details compatibility with Windows, Mac, and Linux.

n/a - Technology does not apply to this platform.

Blank field - Policy is not supported with Endpoint Security Suite Enterprise.

Features	Policies	Windows	macOS	Linux	
File Actions					
	Auto Quarantine (Unsafe)	x	x	x	

Features	Policies	Windows	macOS	Linux	
	Auto Quarantine (Abnormal)	x	x	x	
	Auto Upload	x	x	x	
	Policy Safe List	x	x	x	
Memory Actions					
	Memory Protection	x	x	x	
Exploitation					
	Stack Pivot	x	x	x	
	Stack Protect	x	x	x	
	Overwrite Code	x	n/a		
	RAM Scraping	x	n/a		
	Malicious Payload	x			
Process Injection					
	Remote Allocation of Memory	x	x	n/a	
	Remote Mapping of Memory	x	x	n/a	
	Remote Write to Memory	x	x	n/a	
	Remote Write PE to Memory	x	n/a	n/a	
	Remote Overwrite Code	x	n/a		
	Remote Unmap of Memory	x	n/a		
	Remote Thread Creation	x	x		
	Remote APC Scheduled	x	n/a	n/a	
	DYLD Injection		x	x	
Escalation					
	LSASS Read	x	n/a	n/a	
	Zero Allocate	x	x		
Protection Settings					
	Execution Control	x	x	x	
	Prevent service shutdown from device	x	x		
	Kill unsafe running processes and their sub processes	x	x	x	
	Background Threat Detection	x	x	x	
	Watch for New Files	x	x	x	

Features	Policies	Windows	macOS	Linux	
	Maximum archive file size to scan	x	x	x	
	Exclude Specific Folders	x	x	x	
	Copy File Samples	x			
Application Control					
	Change Window	x		x	
	Folder Exclusions	x			
Agent Settings					
	Enable auto-upload of log files	x	x	x	
	Enable Desktop Notifications	x			
Script Control					
	Active Script	x			
	Powershell	x			
	Office Macros	x		n/a	
	Block Powershell console usage	x			
	Approve scripts in these folders (and subfolders)	x			
	Logging Level	x			
	Self Protection Level	x			
	Auto Update	x			
	Run a Detection (from Agent UI)	x			
	Delete Quarantined (Agent UI and Console UI)	x			
	Disconnected Mode	x		x	
	Detailed Threat Data	x			
	Certificate Safe List	x	x	n/a	
	Copy malware samples	x	x	x	
	Proxy Settings	x	x	x	
	Manual Policy Check (Agent UI)	x	x		

3

Tasks for the Encryption Client

Topics:

- Install/Upgrade the Encryption Client
- Activate the Encryption Client
- View Encryption Policy and Status
- System Volumes
- Recovery
- Removable Media
- Collect Log Files for Endpoint Security Suite Enterprise
- Uninstall the Encryption Client for Mac
- Activation as Administrator
- Encryption Client Reference

Install/Upgrade the Encryption Client

This section guides you through the the Encryption client for Mac installation/upgrade and activation process.

There are two methods to install/upgrade the Encryption client for Mac. Select **one** of the following:

- Interactive Installation/Upgrade and Activation - This method is the easiest method to install or upgrade the client software package. However, this method does not allow any customizations. If you intend to use Boot Camp or a version of operating system that is not yet fully supported by Dell (through .plist modification), you must use the command line installation/upgrade method. For information about using Boot Camp, see Using Boot Camp.
- Command Line Installation/Upgrade - This is an advanced installation/upgrade method that should only be used by administrators experienced with command line syntax. If you intend to use Boot Camp or a version of operating system that is not yet fully supported by Dell (through .plist modification), you must use this method to install or upgrade the client software package. For information about using Boot Camp, see Using Boot Camp.

  For more information on the Installer Command options, see the Mac OS X Reference Library at http://developer.apple.com. Dell highly recommends using remote deployment tools, such as Apple Remote Desktop, to distribute the client installation package.

  NOTE:

  Apple often releases new versions of operating systems between releases of Endpoint Security Suite Enterprise for Mac. To support as many customers as possible, a modification of the com.dell.ddp.plist file is allowed to support these cases. Testing of these versions begins as soon as Apple releases a new version, to ensure that they are compatible with the Encryption client for Mac.

Prerequisites

Dell recommends that IT best practices are followed during the deployment of client software. This includes, but is not limited to, controlled test environments for initial tests and staggered deployments to users.

Before beginning this process, ensure the following prerequisites are met:

- Ensure that the Dell Server and its components are already installed.

  If you have not yet installed the Dell Server, follow the instructions in the appropriate guide below.

  Security Management Server Installation and Migration Guide

  Security Management Server Virtual Quick Start Guide and Installation Guide

- Ensure that you have the Security Server and Policy Proxy URLs handy. Both are needed for client software installation and activation.

- If your deployment uses a non-default configuration, ensure that you know the port number for the Security Server. It is needed for client software installation and activation.
- Ensure that the target computer has network connectivity to the Security Server and Policy Proxy.
- Ensure that you have a domain user account in the Active Directory installation configured for use with the Dell Server. The domain user account is used for client software activation. Configuring Mac endpoints for domain (network) authentication is not required.

Before setting encryption policies, the *Dell Volume Encryption* policy must be *On.*. Be sure that you understand the *Encrypt Using FileVault for Mac* and *Volumes Targeted for Encryption* policies.

For more information about encryption policies, see Mac Encryption > Dell Volume Encryption.

Interactive Installation or Upgrade

To install or upgrade and activate the client software, follow the steps below. You must have an administrator account to perform these steps.

Interactive Installation

NOTE:

Before you begin, save the user's work and close other applications; immediately after the installation is complete, the computer must be restarted.

1. From the Dell installation media, mount the Dell-Encryption-Enterprise-<version>.dmg file.
2. Double-click the package installer. The following message displays:
   This package runs a program to determine if the software can be installed.
3. Click **Continue** to proceed.
4. Read the Welcome text, and click **Continue**.
5. Review the license agreement, click **Continue**, and then click **Agree** to accept the terms of the license agreement.
6. In the *Domain Address* field, enter the fully qualified domain for the target users, such as *department.organization.com*.
7. In the *Display Name (optional)* field, consider setting the *Display Name* to the NetBIOS (pre-Windows 2000) name of the domain, which is typically in uppercase.

   If set, this field is displayed instead of the Domain Address in the *Activation* dialog. This name provides consistency with the domain name that is shown in *Authentication* dialogs for domain-managed Windows computers.

8. In the *Security Server* field, enter the Security Server hostname.

   If your deployment uses a nondefault configuration, update the ports and *Use SSL* check box.

   Once a connection is established, the Security Server connectivity indicator changes from red to green.

9. In the *Policy Proxy* field, the Policy Proxy hostname is autopopulated with a host that matches the Security Server host. This host is used as the Policy Proxy if no hosts are specified in the policy configuration.

   After a connection is established, the Policy Proxy connectivity indicator changes from red to green.

10. Once the Dell Configuration dialog is complete and connectivity has been established to the Security Server and Policy Proxy, click **Continue** to show the installation type.
11. Some installations on specific computers display a *Select a Destination* dialog before the *Installation Type* dialog displays. If so, select the current system disk out of the list of disks displayed. The icon of the current system disk displays a green arrow pointing to the disk. Click **Continue**.
12. After the installation type displays, click **Install** to continue the installation.
13. When prompted, enter the administrator account credentials. (The MacOS X Installer application requires credentials.)
14. Click **OK**.

    NOTE:

    Immediately after the installation is complete, you must restart the computer. If you have open files in other applications and are not ready to restart, click **Cancel,** save the work, and close the other applications.

15. Click **Continue Installation**. The installation begins.
16. When the installation is complete, click **Restart**.
17. With a new installation of Endpoint Security Suite Enterprise, a *System Extension Blocked* dialog displays.

For kext consent, one or both of these dialogs display.

System Extension Blocked	System Extension Blocked
a. Click **OK**. b. Click **OK**. c. To approve these extensions, select **System Preferences > Security & Privacy**. d. Click **Allow** next to *System software from developer Credant Technologies (Dell, Inc, formerly Credant Technologies)*. e. Click **OK**.	Complete these steps if the system extension for mounting FDEEM volumes could not be loaded. a. Click **Open System Preferences**. b. Click **OK**. c. Under the **General** tab, click **Allow** next to *System software from developer Credant Technologies (Dell, Inc, formerly Credant Technologies)*. d. Click **OK**.

The Allow button may be available for 30 minutes or less after installing. If you skip this step, the dialog continues to display about every twenty-five minutes until you complete this.

18. Continue to Activate the Encryption Client for Mac.

macOS 10.15 and higher with removable media

If an enterprise uses removable media with macOS 10.15 and higher, users must enable full disk access for external media. For more information, see Enable Full Disk Access for Removable Media.

Command Line Installation/Upgrade

To install the client software using the command line, follow these steps.

Command Line Installation

1. From the Dell installation media, mount the Dell-Encryption-Enterprise-<version>.dmg file.
2. Copy the **Install Dell Endpoint Security Suite Enterprise** package and the **com.dell.ddp.plist** file to the local drive.
3. In the Management Console, modify the following policies if needed. Policy settings override .plist file settings. Use .plist settings if policies do not exist in the Management Console.
   - **No Auth User List** - In some cases, you may want to edit this policy so that specified users or classes of users do not have to activate against the Dell Server. For example, in an educational facility, teachers would be prompted to activate their computer against the Dell Server, but individual students using lab computers would not. The lab administrator could use this policy and the account running the client tool so that student users could log in without being prompted to activate. For information on the client tool, see Client Tool. If an enterprise needs to know which user account is associated with each Mac computer, all users must activate against the Dell Server, so that enterprise would not edit this property. However, if a user wants to provision Encryption External Media, the user must be authenticated against the Dell Server.
4. Open the .plist file and edit any additional placeholder values:

   NOTE:

   Apple often releases new versions of operating systems between releases of Endpoint Security Suite Enterprise for Mac. To support as many customers as possible, Dell allows a modification of the .plist file to support these cases. As soon as Apple releases a new version, Dell begins testing these versions to ensure that they are compatible with the Encryption client for Mac.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>*</string>
  </array>
  </dict>
```

```
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain
name can log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in
without being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the
default .plist     file, it must be added to the file. Add from <key> through </
array> to allow a newer version of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443.
However, port number 8081 will still allow activations. In general, if your Dell
Server is v8.0 or later, use port 8443. If your Dell Server is pre-v8.0, use port
8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the
Dell Server by the same hostname it was activated with, regardless of changes to the
computer hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the
Domain URL that users will activate against]
   </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your
Policy Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an
existing port]
   </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy,
"Require password XXXX after sleep or screen saver begins." The acceptable range is
0-32400.]
  <key>EMSTreatsUnsupportedFileSystemAs</key>
```

```
  <string>ignore</string> [For handling Mac OS Extended media. Possible values
are ignore, provisioningRejected, or unshieldable. ignore - the media is usable
(default). provisioningRejected - retains the value in the Dell Server policy, EMS
Access to unShielded Media. unshieldable - If the EMS Access to unShielded Media
policy is set to Block, the media is ejected. If the EMS Access to unShielded Media
policy is not set to Block, it is usable as provisioningRejected. The key and value
are case sensitive.]
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The
time in seconds to give the Security Server time to respond to an activation attempt
before giving up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5. Save and close the .plist file.
6. For each targeted computer, copy the package to a temp folder and the com.dell.ddp.plist file to **/Library/Preferences**.
7. Perform a command line installation of the package using the **installer** command:
   `sudo installer -pkg "Install Dell Endpoint Security Suite Enterprise.pkg" -target /`
8. Restart the computer using the following command line: **`sudo shutdown -r now`**

   NOTE:

   System Integrity Protection (SIP) was hardened in macOS High Sierra (10.13) to require users to approve new third-party kernel extension. For information on allowing kernel extensions on macOS High Sierra, see KB article SLN307814.
9. Continue to Activate the Encryption Client for Mac.

macOS 10.15 and higher with removable media

If an enterprise uses removable media with macOS 10.15 and higher, users must enable full disk access for external media. For more information, see Enable Full Disk Access for Removable Media.

Enable Full Disk Access for Removable Media

If an enterprise uses removable media with macOS 10.15 and higher, users must enable full disk access for external media. Users see one of these prompts:

- After you install the client software, a prompt displays stating that you must provide Full Disk Access consent for external media. Click the **Go to Security and Privacy** button and continue the steps below.
- If not prompted after installation, users are prompted to enable full disk access when they first mount the removable media. A message displays, stating either that Dell Encryption External Media or EMS Explorer would like to access files on a removable volume. Click **OK**, and continue the steps below.

For more information, see KB article SLN319972.

1. In *System Preferences* > *Security and Privacy*, click the **Privacy** tab.
2. In the left pane, select **Full Disk Access**.
   The *Dell Encryption External Media* app does not display.
3. At the bottom, click the lock icon and provide credentials for a local administrator account.
   In the left pane > **Files and Folders**, the user can check the external media (EMS) components to provide the required permissions.
4. In the left pane, select **Full Disk Access**.

   The *Dell Encryption External Media* app now displays. However, when the request for approval is pending the check box for that app is not selected.
5. Grant permission by selecting the check box.

   If the *Dell Encryption External Media* app does not display:

   a. Click the plus icon (+) in the right pane.
   b. Go to **/Library/Dell/EMS**, and select **Dell Encryption External Media**.
   c. Click **Open**.
   d. In **Full Disk Access**, select the checkbox for *Dell Encryption External Media*.
6. Close **Security and Privacy**.

Activate the Encryption Client

The activation process associates network user accounts in the Dell Server to the Mac computer and retrieves each account's security policies, sends inventory and status updates, enables recovery workflows, and provides comprehensive compliance reporting. The client software performs the activation process for each user account it finds on the computer as each user logs in to their user account.

After the client software has been installed and the Mac has restarted, the user logs in:

1. Enter the user name and password managed by Active Directory.

   If the password dialog times out, click **Refresh** on the Policies tab. In View Policy and Status on the Local Computer, see step 1.

2. Select the Domain to log on to.

   If the Dell Server is configured for multi-domain support and a different domain must be used for activation, use the User Principle Name (UPN), which is of the form *<username>@<domain>*.

3. Options are:
   - Click **Activate**.
     - If activation succeeds, a message displays to indicate successful activation. The Encryption client for Mac is now fully operational and managed by the Dell Server.

       NOTE:

       If an alert displays regarding an Encryption External Media required resource, click the **Go to Security and Privacy** button and then click **Allow** for any system extension required by your organization. You must allow this extension for Encryption External Media to function properly.
     - If activation fails, the client software allows three attempts to enter correct domain credentials. If all three attempts fail, the prompt for domain credentials displays again at the next user login.
   - Click **Not Now** to dismiss the dialog, which displays again at the next user login.

     NOTE:

     When the administrator needs to decrypt a drive on a Mac computer, whether from a remote location, by running a script, or in person, the client software prompts the user to allow the administrator access and requires the user to enter their password.

     NOTE:

     If you set the computer for FileVault encryption and the files are encrypted, be sure to log into an account from which you can later boot the system.
4. Do one of these:
   - If encryption was **not** enabled prior to activation, continue to Encryption Process.
   - If encryption **was** enabled prior to activation, continue to View Encryption Policy and Status.

View Encryption Policy and Status

You can view the encryption policy and status on the local computer or in the Management Console.

View Policy and Status on the Local Computer

To view encryption policy and encryption status on the local computer, follow the steps below.

1. Launch *System Preferences* and click **Dell Encryption Enterprise**.
2. Click the **Policies** tab to view the current policy set for this computer. Use this view to confirm the specific encryption policies in effect for this computer.

   NOTE:

   Click **Refresh** to check for policy updates.

The Management Console lists Mac policies in these technology groups:

- **Mac Encryption**
- **Removable Media Encryption**

Policies that you set depend on the encryption requirements of your enterprise.

This table lists the policy options.

Mac Encryption > Dell Volume Encryption For High Sierra and higher, both of these policies must be enabled. For Sierra and earlier, see previous versions of the documentation.	
Dell Volume Encryption	*On* or *Off* This is the "master policy" for all other Dell Volume Encryption policies. This policy must be set to *On* for any other Dell Volume Encryption policies to be applied. *On* enables encryption and initiates encryption for unencrypted volumes, per the *Volumes Targeted for Encryption* **or** *Encrypt Using FileVault for Mac* policy. The default setting is *On*. Off disables encryption and initiates a decryption sweep for any fully or partially encrypted volumes.
Encrypt Using FileVault for Mac	If you plan to use FileVault encryption, be sure to first set Dell Volume Encryption to *On*. Ensure that the *Encrypt Using FileVault for Mac* policy is selected in the Management Console. When enabled, FileVault is used to encrypt the System Volume including Fusion Drives, based on the *Volumes Targeted for Encryption* policy setting.
Mac Encryption > Mac Global Settings	
Volumes Targeted for Encryption	*System Volume Only* or *All Fixed Volumes* *System Volume Only* secures only the currently running system volume. **All Fixed Volumes** secures all Mac OS Extended Volumes on all fixed disks, along with the currently running system volume.

3. For descriptions of all the policies, see *AdminHelp* which is available from the Management Console. To locate a specific policy in *AdminHelp*:
   a. Click the Search icon.
   b. In *Search*, enter the policy name with quotes.
   c. Click the topic link that displays. The policy name that you entered in quotes is highlighted in the topic.
4. Click the **System Volumes** tab to view the status of the volumes targeted for encryption.

State	**Description**
Excluded	The volume is excluded from encryption. This applies to unencrypted volumes when encryption is disabled, external volumes, volumes with formats other than Mac OS X Extended (Journaled), and non-system volumes when the *Volumes Targeted for Encryption* policy is set to System Volume Only.
Preparing volume for encryption	The client software is currently initiating the encryption process for the volume but has not begun the encryption sweep.
Volume cannot be resized	The client software cannot start encryption because the Volume cannot be resized appropriately. After receiving this message, contact Dell ProSupport and provide the log files.

State	Description
Needs repair before encryption begins	The volume failed Disk Utility verification. To repair a volume, follow the instructions in Apple Support article HT1782 (http://support.apple.com/kb/HT1782).
Encryption preparation complete. Pending restart	Encryption begins after restart.
Encryption policy conflict	The disk cannot be brought under policy because it is encrypted with an incorrect setting. See Encrypt Using FileVault for Mac.
Waiting to escrow keys with Dell Server	To ensure all encrypted data is recoverable, the client does not begin the encryption process until all encryption keys are successfully escrowed to the Dell Server. The client polls for Security Server connectivity while in this state until the keys are escrowed.
Encrypting	An encryption sweep is in progress.
Encrypted	The encryption sweep is complete.
Decrypting	A decryption sweep is in progress.
Restoring to original state	The client software is restoring the partition scheme to its original state at the end of the *Decrypting* process. This is the decryption sweep equivalent of the *Preparing volume for encryption* state.
Decrypted	The decryption sweep is complete.

Color	Description
Green	Encrypted portion
Red	Not encrypted portion
Yellow	Portion being re-encrypted For example, by a change in encryption algorithms. The data is still secure. It is just transitioning to a different type of encryption.

The System Volumes tab displays all volumes attached to the computer residing on GUID Partition Table (GPT) formatted disks. The following table lists examples of volume configurations for internal drives.

NOTE:

Badges and icons may differ slightly depending on your operating system.

Badge	Volume Type and Status
	The currently booted Mac OS X system volume. The X-folder badge denotes the current boot partition.
	A volume configured for encryption. The Security and Privacy badge denotes a FileVault-protected partition.

Badge	Volume Type and Status
	A non-boot volume configured for encryption. The Security and Privacy badge denotes a FileVault-protected partition.
	Multiple drives and no encryption. **NOTE:** The volume icon without a badge indicates that nothing has been done to the disk. This is not a boot disk.

5. Click the **Removable Media** tab to view the status of the volumes targeted for encryption. The following table lists examples of volume configurations for removable media.

   Badges and icons may differ slightly depending on your operating system.

Badge	Status
	A dimmed volume icon indicates an unmounted device. Reasons include: • User may have chosen not to provision it. • The media may be blocked. **NOTE:** A red circle/slash badge on this icon indicates a partition that is excluded from protection because it is not supported. This includes FAT32-formatted volumes.
	The saturated volume icon indicates a mounted device. The no-write badge indicates that it is read-only. Encryption is enabled, but the media is not provisioned and Encryption External Media Access to unencrypted Media is set to Read Only.
	Media encrypted by Encryption External Media, denoted by a Dell badge.

View Policy and Status in the Management Console

To view encryption policy and encryption status in the Management Console, follow the steps below.

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click **Populations > Endpoints**.
3. For Workstation, click an option in the *Hostname* field or, if you know the endpoint hostname, enter it in *Search*. You can also enter a filter to search for the endpoint.

   NOTE:

   The wild card character (*) may be used but is not required at the beginning or end of the text. Enter Common Name, Universal Principal Name, or sAMAccountName.
4. Click the appropriate endpoint.
5. Click the **Details & Actions** tab.

   The Endpoint Detail area displays information about the Mac computer.

The Shield Detail area displays information about the client software, including encryption sweep start and end times for this computer.

To view effective polices, in the Actions area, click **View Effective Policies**.

6. Click the **Security Policies** tab. From this tab, you can expand the types of policies and change individual policies.
   a. When finished, click **Save**.
   b. In the left pane, click **Management** > **Commit**.

      NOTE:

      The number that displays by Pending Policy Changes is cumulative. It can include changes made on other endpoints, or made by other administrators who are using the same account.

   c. Enter a description of the changes in the *Comment* box and click **Commit Policies**.
7. Click the **Users** tab. This area displays a list of users activated on this Mac computer. Click the user's name to display the information for all computers this user is activated against.
8. Click the **Endpoint Groups** tab. This area displays all of the endpoint groups to which this Mac computer belongs.

System Volumes

Enable Encryption

The following are supported for encryption:

- Apple File System (APFS) volumes that share phyical media with the boot volume.
- Mac OS X Extended (Journaled) volumes and system disks that are partitioned with the GUID Partition Table (GPT) partition scheme

Use this process to enable encryption on a client computer if encryption was **not** enabled prior to activation. This process enables encryption only for a single computer. You can choose to enable encryption for all Mac computers at the Enterprise level if desired. For additional instructions about enabling encryption at the *Enterprise* level, see AdminHelp.

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click **Populations** > **Endpoints**.
3. For Workstation, click an option in the hostname column or, if you know the endpoint hostname, enter it in *Search*. You can also enter a filter to search for the endpoint.

   NOTE:

   The wild card character (*) may be used but is not required at the beginning or end of the text. Enter Common Name, Universal Principal Name, or sAMAccountName.

4. Click the appropriate endpoint.
5. On the *Security Policies* page, click the **Mac Encryption** technology group.

   By default, the *Dell Volume Encryption* master policy is toggled *On*.

6. If a Mac has a Fusion Drive, select the check box for the *Encrypt Using FileVault* for Mac policy.

   NOTE:

   This policy requires that *Dell Volume Encryption* policy is also set to *On*. However, when FileVault encryption is enabled, none of the other policies in the group are in effect. See Mac Encryption > Dell Volume Encryption.

7. If FileVault is deselected (macOS Sierra and lower), change other policies as desired.

   For descriptions of all the policies, see *AdminHelp* which is available from the Management Console.

8. When finished, click **Save**.
9. In the left pane, click **Management** > **Commit**.

   The number that displays by Pending Policy Changes is cumulative. It can include changes made on other endpoints, or made by other administrators who are using the same account.

10. Enter a description of the changes in the Comment box and click **Commit Policies**.
11. To see the policy setting on the local computer after the Dell Server sends the policy, in the Policies pane of Dell Encryption Enterprise Preferences, click **Refresh**.

Encryption Process

The encryption process varies depending on the state of the boot volume when encryption is enabled.

NOTE:

To maintain the integrity of user data, the client software does not begin encrypting a volume until the verification process is successful on that volume. If a volume fails verification, the client software notifies the user and reports the failure in Dell Data Protection Preferences. If you need to repair a volume, follow the instructions in Apple Support article HT1782 (http://support.apple.com/kb/HT1782). The client software re-attempts verification on the next computer restart.

Select one of these:

- FileVault encryption of an unencrypted volume
- Assume Management of an Existing FileVault-Encrypted Volume

FileVault Encryption of an Unencrypted Volume

With FileVault encryption, an additional unnamed user displays in the PBA. Do not delete this user as it allows the Dell Server to enforce policy on the device. If the PBA user is removed, the user will need to take action to begin policy-mandated decrypts.

1. After installation and activation, you must log into the account you want to boot from after FileVault encryption is active.
2. Wait for validation of the drive and verification of the volume to complete.
3. Enter the password for the account.

   NOTE:

   If you allow this dialog to time out, you must reboot or log in for the password dialog to display again.
4. Click **OK**.
5. Be sure that each user has a secure token. See https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.

   If the account the user was logged into is a non-mobile network account, a dialog displays. After the boot drive is encrypted, the drive can be booted only by the user who was logged in during FileVault initialization.

   This account must be a local or network mobile account. To change non-mobile network accounts to mobile accounts, go to **System Preferences > Users and Groups**. Do one of the following:

   - Make the account a mobile account.

     OR

   - Log into a local account and initialize FileVault from that location.
6. Click **OK**.
7. After encryption preparation is complete, restart the computer.

   NOTE:

   Depending on the User Experience policies set in the Management Console, the client software may prompt the user to restart the computer.
8. After the computer restarts, it must be connected to the network for the client software to escrow recovery information to the Dell Server.

   The client software can begin and complete the encryption process, as well as report encryption status to the Management Console, all before user login. This allows you to enforce compliance across all Mac computers without requiring user interaction.

Modify Policy to Add FileVault Users

FileVault secures the data on a disk by automatically encrypting it. In a managed FileVault boot volume, to allow multiple users to unlock the disk, you can modify a policy in the Management Console and use your dictionary of OpenDirectory record names and values to then allow users to add themselves to the FileVault disk.

1. In the Management Console's advanced *Mac Global Settings* policies, scroll to the *FileVault 2 PBA User List* policy.
2. In the *FileVault 2 PBA User List* policy field, enter a rule that matches the users you plan to specify. For example, matching `<string>*</string>` for any key should match all users that the bound OpenDirectory server has.

   Tags are case sensitive, and the entire value must be properly formed as dictionary and array elements in a property list. Dictionary keys are AND'd together. Array values are or'd together so matching any element in an array matches for the entire array.

   NOTE:

   If a rule is improperly formed, an error displays in the *Dell Encryption Enterprise > Preferences* tab.

   The following <dict> lists examples for two keys:

```
<dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
     <string>;Kerberosv5;;user1@LKDC:*</string>
     <string>;Kerberosv5;;user2@LKDC:*</string>
     <string>;Kerberosv5;;user3@LKDC:*</string>
     <string>;Kerberosv5;;z*@LKDC:*</string>
    </array>
    <key>dsAttrTypeStandard:NFSHomeDirectory</key>
    <string>/Users/*</string>
</dict>
```

   - The sample *AuthenticationAuthority* key entries specify a pattern of *user1*, *user2*, and *user3* or any user id that begins with *z*. To view the dialog that provides the correct syntax for each user, press the **Control-Option-Command** keys on the client. Copy the syntax for the user, and paste it to the Management Console.

     NOTE:

     For this example, trailing asterisks represent the latter part of the authentication authority records. Typically, to avoid under-specifying, include the complete record instead of a trailing asterisk because the asterisk matches any information after the colon in the OpenDirectory record.
   - The NFSHomeDirectory key requires that any user passing the first key must also have a home directory in */Users/*.

     NOTE:

     You must create the home folder if one does not exist for a user.
3. Reboot the computers.
4. Notify users to enable FileVault booting for their user account. The user must have a local or mobile account. Network accounts are automatically converted to mobile accounts.

For a user to enable their FileVault account:

1. Launch **System Preferences**, and click **Dell Encryption Enterprise**.
2. Click the **System Volumes** tab.
3. Control-click the System Volume drive, and select **Add FileVault users to FileVault Booting**.
4. In *Search*, enter a user's name or scroll down. User accounts display only if they meet the criteria set by policy.

   For local and mobile users, an *Enable User* button displays.

   For network users, a *Convert & enable user* button displays.

   NOTE:

   A green indicator displays next to user accounts that can boot FileVault.

5. Click **Enable User** or **Convert & enable user**.
6. Enter the password for the selected account and click **OK**. A progress indicator displays.
7. After a success dialog, click **Done**.

Assume Management of an Existing FileVault-Encrypted Volume

If the computer already has a FileVault-encrypted volume and FileVault encryption is enabled in the Management Console, Dell Encryption can assume management of the volume.

If Dell Encryption detects that the boot volume is already encrypted, the Dell Encryption Enterprise dialog displays. To allow Dell Encryption to assume management of the volume, follow these steps.

1. Select either **Personal Recovery Key *or* Bootable Account Credentials**.

   NOTE:

   For macOS High Sierra and Apple File System (APFS), you must select **Bootable Account Credentials**.

   - **Personal Recovery Key - if you have the personal recovery key you received when the drive was FileVault-encrypted.**
     a. Enter the key.

        If a user does not have the existing key, they can request it from the administrator.

     b. Click **OK**.

     NOTE:

     After the assumption process is complete, a new personal recovery key is generated and escrowed. The previous recovery key is invalidated and removed.
   - **Bootable Account Credentials - if you have the username and password of an account that is currently authorized to boot from the volume.**
     a. Enter the user name and password.

     b. Click **OK**.

2. When a dialog displays indicating that Dell now manages encryption of the volume, click **OK**.

   If Dell Encryption detects that a non-boot volume is already encrypted, a passphrase prompt displays.

3. (FileVault-encrypted non-boot volumes only) To allow Dell Encryption to assume management of the volume, enter the passphrase to access the volume. This is the password that was assigned to the volume when it was originally FileVault-encrypted.

   Once Dell manages the volume's encryption, the old password is no longer valid. Your Dell administrator can retrieve a recovery key for your volume in the event that you should need recovery assistance.

   If you choose not to enter the password, the volume's contents are accessible and are encrypted with FileVault but the encryption is not managed by Dell.

NOTE:

In the Management Console, the administrator can see that the Dell Server now manages the endpoint.

Recycling FileVault Recovery Keys

If you have security issues with a recovery bundle or if a volume or keys are compromised, you can recycle the key material for that volume.

You can recycle keys for boot and non-boot drives on Mac OS X.

To recycle the key material:

1. Download a recovery bundle from the Management Console and copy it to the computer's desktop.
2. Launch *System Preferences* and click **Dell Encryption Enterprise**.
3. Click the **System Volumes** tab.
4. Drag the recovery bundle from step 1 to the appropriate partition.

   A dialog prompts you to cycle the FileVault keys.

5. Click **OK**.

   A dialog confirms success for cycling keys.

6. Click **OK**.

   NOTE:

   Keys in the recovery bundle for this drive are now obsolete. You must download a new recovery bundle from the Management Console.

User Experience

For maximum security, the client software disables the *Automatic Login* feature of Mac OS X computers.

Additionally, the client software automatically enforces the Mac OS X feature *require password after sleep or screen saver begins*. Also, a configurable amount of time is allowed in sleep/screen saver mode before enforcing authentication. The client software allows a user to set a value up to five minutes before authentication is enforced.

Users can use the computer normally as the encryption sweep progresses. All data on the currently booted system volume is being encrypted, including the operating system, while the operating system continues to operate.

If the computer is restarted or enters system sleep, the encryption sweep pauses and then automatically resumes after the restart or wake.

The client software does not support the use of hibernation images, which the Mac OS X *Safe Sleep* feature uses to wake the computer if the battery is fully discharged during sleep.

To reduce user impact, the client software automatically updates the system sleep mode to disable hibernation and enforces this setting. The computer can still enter sleep, but the current system state is maintained only in memory. Therefore, the computer is fully restarted if completely shut down during sleep, which could occur if the battery runs down or is replaced.

Copy allowlist rule

A hidden menu item allows a user to copy a allowlist rule for removable media.

1. Launch **System Preferences** and click **Dell Encryption Enterprise**.
2. Select the **Removable Media** tab.
3. Right-click a drive row, and simultaneously press the command key.

   A hidden menu item displays.
4. Click **Copy allowlist rule** for the current removable media. The allowlist rule is copied to the Clipboard.
5. Access the Clipboard, copy the allowlist rule, and send it to your administrator.

If the *Mac Media Encryption* policy is toggled **On**, data is encrypted, including Thunderbolt drives.

To exclude a device or group of devices to prevent writing encrypted data to the Thunderbolt drive or to Encryption External Media, use the allowlist rule to modify the values.

Use the complete rule to specify a particular drive for allowlisting, for example:

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=001CC0EC3447AA308699119F

NOTE:

Be sure to replace the sample values with the information for your drive.

NOTE:

You must enable HFS Plus. See Enable HFS Plus.

To exclude SATA devices from Mac Media Encryption policy enforcement when connected via Thunderbolt:

tbolt=1;bus=SATA

You can also allowlist or exclude media from Encryption External Media based on:

- **Media size**

  Allowlist rule to exclude large media from Encryption External Media protection:

size <op> <size specifier>

<op> can be =, <=, >=, <, >

<size specifier> is of the form decimal integer with an optional suffix from {K, M, G, T} aligned on 1000, not 1024. For example, to exclude media or a drive greater than 500000000 bytes from Encryption External Media, use one of these:

size >= 500000000

size >= 500000K

size >= 500M

- **File system type**

  Allowlist rule:

  fstype=<fstype>

  <fstype> can be ExFAT, FAT, or HFS+

To exclude both, here is an example for 1TB and greater HFS+ media:

size>=1T;fstype=HFS+

Recovery

Occasionally, you may need access to data on encrypted disks. As a Dell administrator, you can access encrypted disks without decrypting them, saving you valuable time.

You might need to access a user's encrypted data for many reasons, but a few common use cases are as follows:

- Someone leaves the company, and no one knows the password.
- A user cannot recall the password.

This section guides you through the process of using FileVault Recovery when FileVault encryption is on the endpoint to be recovered. FileVault can be used with the Encryption client running on macOS Sierra 10.12.6. FileVault recovery is also used on Fusion Drives.

Mount Volume

Prerequisites

- An unencrypted external recovery volume or computer to run the recovery utility
- A FireWire or Thunderbolt cable, depending on your hardware
- The Device ID/Unique ID of the computer targeted for recovery - In most cases, you can find the computer targeted for recovery in the Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Unique ID/Device ID is "John Doe's MacBook.Z4291LK58RH".
- The Dell installation media

Process

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click **Management > Recover Endpoint**.
3. In *Search*, enter the fully qualified domain name of the endpoint to recover and click the search icon.
4. Click the device's **Recover** link.
5. If the endpoint requires enhanced recovery, a prompt for a password displays. Assign a new password to the encryption key bundle that you are about to download.

   NOTE:

   You must remember this password to access the recovery keys.
6. To save the recovery bundle to the external recovery volume or computer to run the recovery utility to perform the recovery operation, click **Download** and click **Save**.

The recovery file <machine_name.domain>.csv is downloaded.

7. Boot the target computer from a pre-created external recovery volume. You can accomplish this by either launching the Startup Disk pane in System Preferences and selecting the recovery volume, or by holding down the **Option** key while you restart this computer and selecting the recovery volume in the preboot Startup Manager.

   or

   Boot the computer targeted for recovery into Target Disk Mode. You can accomplish this by either launching the Startup Disk pane in System Preferences and clicking **Target Disk Mode**, or by holding down the **T** key while you restart this computer.

   NOTE:

   Firmware password protection blocks the ability to use the T key at startup to enter Target Disk Mode. More information about Target Disk Mode is available from Apple at http://support.apple.com/kb/HT1661.

   Now connect this computer to the host computer that will perform the recovery operation using a FireWire or Thunderbolt cable, depending on your hardware.

8. Mount the Dell-Encryption-Enterprise-<version>.dmg.

   NOTE:

   The Recovery Utility must be the same or newer version than the version of client software installed on the computer targeted for recovery.

9. Select the volume or drive that needs recovery and click **Continue**.

   Selecting the drive recovers all volumes on the drive at once.

10. Select the recovery bundle (saved in step 6) and click **Open**.
11. Click **Close**.

You can now open a Finder window and access data on the encrypted volume as you would a normal volume. All data is transparently encrypted and decrypted as files are transferred between the volumes.

FileVault Recovery

Recovery of a managed FileVault-encrypted volume is dictated by Apple and is automated where possible but requires a few more steps.

The Dell Recovery Utility simplifies the operation of Apple's recovery tools with scripts to assist with mounting a volume or, in some cases, decrypting it. FileVault recovery functionality is determined by the operating system installed on the Recovery HD and the paired target partition.

A FileVault-encrypted volume can be recovered only from a Recovery HD partition that is written to all disk drives running Mac OS X 10.9.5 or later. This requirement eliminates the possibility of performing a recovery operation directly from the Dell Recovery Utility.

Two recovery methods exist, based on whether the FileVault recovery key is a personal or institutional recovery key. One valid recovery key always exists. If a personal recovery key exists, Dell recommends that you use the most recent entry for that key. If that key does not work, then use the institutional recovery keychain.

- Personal Recovery Key - Existing FileVault encryption is managed by the Dell Server. If the most recent entry in the recovery bundle contains a RecoveryKey entry, follow the Personal Recovery Key steps. Here is a RecoveryKey example:

  ```
  RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
  ```

- Recovery Keychain (rarely used) - This recovery method is based on use of a FileVault institutional recovery key.

  If the most recent entry in the recovery bundle contains a KeychainKey entry, follow the Recovery Keychain steps. Here is a KeychainKey example:

  ```
  KeychainKey</key><data>a3ljaAABAAAAA...
  ```

Personal Recovery Key

Generally, the best practice is to recover the boot volume before recovering non-boot volumes since that mounts any other volume that was encrypted. Recovering the boot volume typically corrects issues with non-boot volumes.

Prerequisites

- An external bootable drive
- The Device ID/Unique ID of the computer targeted for recovery. In most cases, you can find the computer targeted for recovery in the Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Device ID/Unique ID is "John Doe's MacBook.Z4291LK58RH".
- The Dell installation media

Management Console - Save the recovery bundle

1. Open the Management Console.
2. In the left pane, click **Populations > Endpoints**.
3. Search for the device to recover.
4. Click the device name to open the Endpoint Detail page.
5. Click the **Details & Actions** tab.
6. Under *Shield Detail*, click the **Device Recovery Keys** link.
7. To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download** and click **Save**.
8. Enter a location for the recovery bundle and click **Save**.

Process - Mount the .dmg

1. Copy the recovery bundle and the **Dell-Encryption-Enterprise-<version>.dmg** file to the bootable USB drive.
2. Boot the target computer from a pre-created external full-operating system install volume by holding down the **Option** key while you restart this computer and then selecting the external full-operating system install volume in the pre-boot Startup Manager. To create a bootable volume, refer to https://support.apple.com/en-us/HT202796.
3. Mount the **Dell-Encryption-Enterprise-<version>.dmg**.

Process - Launch the Dell Recovery Utility and recover the FileVault volume

1. In the Utilities folder located in the Dell installation media, launch the Dell Recovery Utility.

   The *Dell Recovery Utility > Select Volumes* dialog displays.

   NOTE:

   The Recovery Utility must be the same or newer version than the version of client software installed on the computer targeted for recovery.
2. In the *Dell Recovery Utility > Select Volumes*, select the FileVault volume.
   - When recovering an operating system, the best practice is to boot to a computer with the same operating system or higher.
   - If you have non-boot volumes encrypted, typically, you will recover the boot partition first.
3. Click **Continue**.
4. Locate and select the recovery bundle (saved earlier) and click **Open**.
5. If the *Select Recovery Record* dialog displays, view the *Escrow Date* column, select the most recent date for the Personal Recovery Key type, and click **Continue.**

   NOTE:

   With an older escrow date, the key may no longer be valid.

   The *Recovery Operation Result* displays.
   - For boot drives, the recovery tool provides a personal recovery key that allows you to boot using standard Apple FileVault recovery. You can boot into the target partition and enter the personal recovery key for Pre-Boot-Authentication, which may vary depending on the operating system.
   - For non-boot drives, only the personal recovery key displays. An Unlock button is provided to unlock and mount the volume.
6. Do one of these:
   - Recover the boot volume (most common)
   - Recover a non-boot volume (rarely used)

Recover the boot volume (most common)

For most recovery cases, use this option to recover the boot volume:

1. Either write down the key or click **Print recovery key**.
2. Click **Close**.
3. Boot the volume you want to recover, using the preboot Startup Manager if necessary.

   The computer displays icons for multiple users or requests a password.
4. Select a user if applicable, then click **?** at the login screen.
5. Click the arrow that displays.
6. Type the recovery key and press **Enter**.
7. At the dialog, enter a new password for the user.

Recover nonboot volume options (rarely used) - Perform one of these:

Recover a nonboot volume

If the boot volume is damaged or erased and secondary volumes exist, you can mount these nonboot volumes.
1. Click **Unlock**. The volume mounts.
2. Click **Close**.

Decrypt volume - click the button
1. Click **Decrypt**. A dialog and progress bar indicate the decryption process.
2. When it completes, click **Close**.
3. Boot into the decrypted volume to use it.

Decrypt volume - run the command from Terminal
1. Copy the command in the *Decrypt Volume* area.
2. Click **Close**.
3. Run the command in Terminal.

Recovery Keychain

You must run the Dell Recovery Utility while it is booted to a non-encrypted recovery volume.

Prerequisites

- An external recovery volume or computer that will be running the recovery utility
- A USB drive
- A Firewire cable
- The Dell installation media

Management Console - Save the recovery bundle
1. Open the Management Console.
2. In the left pane, click **Populations > Endpoints**.
3. Search for the device to recover.
4. Click the device name to open the Endpoint Detail page.
5. Click the **Details & Actions** tab.
6. Under *Shield Detail*, click the **Device Recovery Keys** link.
7. To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download** and click **Save**.
8. Enter a location for the recovery bundle and click **Save**.

Process
1. Connect an external drive to the system to be recovered.

   The external drive must have a Mac OS boot volume.
2. Boot to the external drive by pressing and holding the **Option** key, and use the boot picker to select and boot from this volume.
3. Copy the recovery bundle from the Management Console.
4. Mount the installation .dmg file.

5. In the Utilities folder, run the Dell Recovery Utility.

   The *Dell Recovery Utility > Select Volumes* dialog displays.

6. Select the FileVault volume to recover and click **Continue.**

   The *Choose recovery bundle* dialog displays.

7. Select the recovery bundle and click **Open**.

   If more than one recovery key exists for that disk, the *Select Recovery Record* screen displays.

8. In the Escrow Date column, select the most recent date for the Keychain recovery type, and click **Continue.**

   NOTE:

   With an older escrow date, the key may no longer be valid.

   The *FileVault recovery instructions* dialog displays.

9. Read the instructions and click **Continue**.

   The *Confirm recovery operation* dialog displays.

10. Highlight the FileVault volume to recover and click **Continue.**

    The *Choose location for recovery files* dialog displays, prompting you to select a location to store the recovery files.

    This location must be the location you will use for recovery since the scripts contain absolute paths to the data files. Do **not** copy these files to the Recovery HD.

    Dell recommends that you save these files at the root of a removable drive, such as a USB drive.

    NOTE:

    Ensure that all users have read/write access to the USB or other disk you use to store the recovery key and that the disk has adequate space. If you do not have rights to a selected disk or if the disk is out of space, an error displays indicating that the recovery keys have not been stored.

11. Select a location and click **Save**.

    The *Recovery Operation Result* dialog displays, indicating the files have been created.

12. Click **Close.**

13. After the Recovery HD volume boots, enter the name and path of the script.

    NOTE:

    Storing the files close to the root of a volume shortens the path to type.

    The Recovery Operation Result displays the key.

    The Recovery Utility outputs the files to the selected location, then displays the exact commands needed to run from the Recovery HD volume to mount or decrypt the FileVault volume.

14. After these files are generated, copy the command strings shown on the final *Recovery Operation Result* dialog.

15. Reboot to the Recovery HD in one of these ways:

    - Simultaneously press and hold the **Command-R** keys before the Power-On/Self-Test chime and during the computer boot-up.

      or

    - For earlier versions of Apple, press the **Option** key and use the boot picker to select the Recovery HD.

      The *Mac OS X Utilities* dialog displays.

16. From the Tools menu, select **Utilities > Terminal**.

17. To mount the volume so you can copy files from the Terminal or image the disk from Disk Utility: In Terminal, type the full path and the script name **fv2mount.sh**, for example:

    /Volumes/recoveryFOB/fv2mount.sh

18. Reboot the computer.

Removable Media

Supported Formats

FAT32, exFAT, or HFS Plus (Mac OS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes are supported. You must enable HFS Plus.

NOTE:

Mac currently does not support CD/DVD burning for Encryption External Media. However, access to CD/DVD drives is not blocked, even if the *EMS Block Access to UnShieldable Media* policy is selected.

Enable HFS Plus

To enable HFS Plus, add the following to the .plist file.

<key>EMSHFSPlusOptIn</key>

<true/>

NOTE:

Dell recommends testing this configuration before introducing it into the production environment.

HFS Plus does not support:

- Versioning - Existing versioning data is removed from the disk.
- Hard links - During an encryption sweep of the removable media, the file is not encrypted. A dialog recommends ejecting the media.
- Media containing Time Machine backups:
  - Media recognizably used by the computer as a Time Machine backup destination is automatically allowlisted to allow backups to continue.
  - All other removable media with Time Machine backups is based on policy governing unprovisioned media and unprotected media. See *EMS Access to unShielded Media* and *EMS Block Access to UnShieldable Media* policies.

    NOTE:

    For a new drive that does not yet have backups, the user must copy their allowlist rule and send you the rule to specify their Time Machine drive for allowlisting. See Copy allowlist rule.

Encryption External Media and Policy Updates

On the system where the removable media was provisioned (or recovered), policies are updated on the removable media at mount time.

Encryption Exceptions

Extended attributes are not encrypted on removable media.

Errors on the Removable Media Tab

- On an unshielded computer, do not replace an encrypted file with a decrypted version of the file. Later, this could prevent decryption. This may also display as an error on the Removable Media tab.
- If an end-of-file marker is invalidated, for example if a file is overwritten with new content outside of Encryption External Media control, and then you mount in Encryption External Media, an end-of-file error displays on the Removable Media tab.
- When you convert files, the media must have more free space than the size of the largest file to be converted. If a yellow warning triangle displays in the Removable Media status area, click it. If a message indicates *Insufficient space*, do the following:

  1. Note the amount of space that must be freed on the device. The report displays a list of files and the size.

2. Empty the trash. As you free space, Encryption External Media automatically encrypts additional files.
3. If you delete any files or folders, be sure to re-empty the trash.

Audit Messages

Audit messages are sent to the Dell Server.

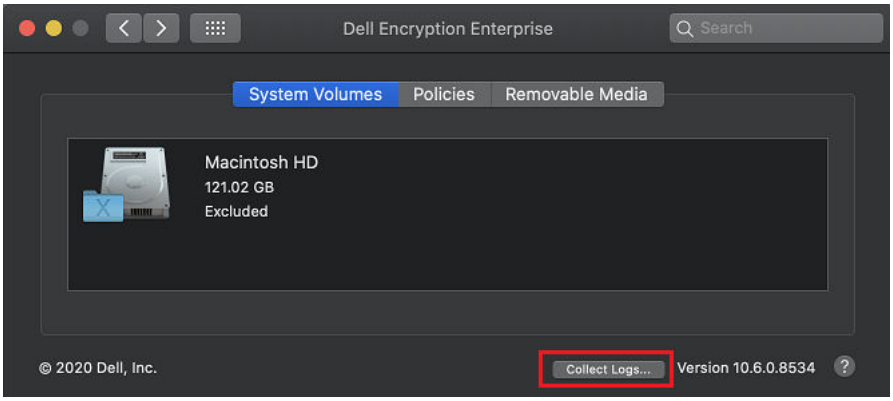
For Endpoint Security Suite Enterprise for Mac, to view audit messages:

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click **Populations > Enterprise or Endpoints**.
3. Select the **Advanced Threat Events** tab.

For more information, see *AdminHelp*.

Collect Log Files for Endpoint Security Suite Enterprise

In *System Preferences* > *Dell Encryption Enterprise* > *System Volumes*, a *Collect Logs* button at the bottom right allows an administrator to pre-generate logs for support. This action may impact performance while logs are collected.



DellLogs.zip contains the logs for Mac Encryption Enterprise and Advanced Threat Prevention. For information about how to collect the logs, see http://www.dell.com/support/article/us/en/19/SLN303924.

Uninstall the Encryption Client for Mac

The client software may be uninstalled by running the **Uninstall Dell Encryption Enterprise** application. To uninstall the client software, follow the steps below.

NOTE:

Before running the uninstall application, the disk must be fully decrypted.

1. If the disk is currently encrypted, set the computer's *Dell Volume Encryption* policy to **Off** in the Management Console and commit the policy.

   A dialog displays to ask for access to System Preferences and control of the computer so that the client software can decrypt the disk.

   a. Click **Open System Preferences**.

      If **Deny** is selected, the uninstallation and decryption are unable to continue.

   b. Enter the administrator password.
2. After the disk is fully decrypted, restart the computer (when prompted).
3. After the computer restarts, launch the **Uninstall Dell Encryption Enterprise** application (located in the Utilities folder in the Dell-Encryption-Enterprise-<version>.dmg in the Dell installation media).

Messages display the status of the uninstallation.

The Encryption client for Mac is now uninstalled, and the computer can be used normally.

Activation as Administrator

The Client Tool offers the administrator new methods for activating the client software on a Mac computer and examining the client software. Two methods of activation are available:

- Activation using administrator credentials
- Temporary activation that emulates the user without leaving footprints on that computer.

Both methods can be used directly through a shell, or in a script.

NOTE:

Do not activate the client software on more than five computers with the same network account. Serious security vulnerabilities and degraded performance of your Dell Server could result.

Prerequisites

- The Encryption client for Mac must be installed on the remote computer.
- Do not activate through the client user interface prior to attempting to activate from a remote location.

Activate

Use this command to activate the client as administrator.

Example:

client -a *username@domain.com password admin admin*

Activate Temporarily

Use this command to activate the client without leaving footprints on the computer.

1. Open a shell or use a script to activate the client software:

   client *-at username@domain.com password*

2. Use the Client Tool to retrieve information about the client software, its policies, disk status, user account and more. For more information about the Client Tool, see Client Tool.

   NOTE:

   After activation, information about the client software, including policies, disk status, and user information, is also available in System Preferences in the Dell Encryption Enterprise preferences.

Encryption Client Reference

About Optional Firmware Password Protection

NOTE:

More recent Mac computers do not support Firmware Password Protection. Firmware Password Protection is supported for the following models:

- iMac10.*
- iMac11.*
- Macmini4.*

- MacBook7.*
- MacBookAir2.*
- MacBookPro7.*
- MacPro5.*
- XServe3.*

For example, iMac10.1, iMac11.1 and iMac11.2 support Optional Firmware Password Protection (as indicated by the *), but iMac12.1 or later does not.

NOTE:

When the FirmwarePasswordMode key option is set to **Optional**, it only disables client enforcement of firmware password protection. It does **not** remove any existing firmware password protection. You can remove any existing firmware password using the Mac OS X Firmware Password Utility.

If you intend to use Boot Camp (see How to Enable Mac OS X Boot Camp for instructions) on encrypted Mac computers, you **must** configure the client to **not** use firmware password protection.

Mac computers use firmware password protection to enhance access security of the computer. On Mac computers, by default, the protection is turned *OFF*. During client installation, whether a new installation or an upgrade from an earlier client version, you have the ability to edit the existing com.dell.ddp.plist file to allow the *FirmwarePasswordMode* key to be set to either *Required* or *Optional*. The *Required* option is the default setting that enforces firmware password protection, while the *Optional* setting causes the firmware password to not be enforced. Following the installation or upgrade, the client evaluates the modified installer com.dell.ddp.plist file during restart.

NOTE:

To prevent users from changing the computer's security posture, the client does not accept changes to the FirmwarePasswordMode key after installing the client software.

You can change the value of this key after installation or upgrade by initiating a disk decryption process, and then re-enabling encryption.

For Mac OS X firmware password protection to be **required**, follow normal client installation/upgrade procedures outlined in Install/Upgrade the Encryption Client for Mac.

Using Boot Camp

Mac OS X Boot Camp Support

NOTE:

When using Boot Camp, Dell Encryption Enterprise does not encrypt the Windows operating system. Also, if two or more bootable macOS partitions exist on the device, Encryption Enterprise encrypts only the primary volume.

Boot Camp is a utility included with Mac OS X that assists you in installing Windows on Mac computers in a dual-boot configuration. Boot Camp is supported with the following Windows operating systems:

- Windows 7 and 7 Home Premium, Professional, and Ultimate (64-bit)
- Windows 8.1 and 8.1 Pro (64-bit)

NOTE:

Windows 7 is Boot Camp 4 or 5.1. Windows 8.1 and higher is Boot Camp 5.1 only.

To use Endpoint Security Suite Enterprise for Windows in Boot Camp on a computer with Endpoint Security Suite Enterprise for Mac, the system volume must be encrypted through the Encryption client for Mac with FileVault2. See the Command Line Installation/Upgrade for instructions.

NOTE:

If your Windows partition is a candidate for Encryption External Media, be sure to allowlist it or it will be encrypted. See Copy allowlist rule.

NOTE:

You must ensure Windows is installed before deploying client policies enabling encryption. After the client begins the encryption process, it disallows disk partition operations required by Boot Camp.

Recovery of Endpoint Security Suite Enterprise for Windows on Boot Camp

To recover Endpoint Security Suite Enterprise for Windows running in a Boot Camp volume, you must also create a Boot Camp volume on an external drive.

Prerequisites

- An external bootable drive
- The Device ID/Unique ID of the computer targeted for recovery. In most cases, you can find the computer targeted for recovery in the Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Device ID/Unique ID is "John Doe's MacBook.Z4291LK58RH".

Process

1. On an external drive, create a Boot Camp volume.

   The steps are similar to creating a Boot Camp volume on your local system. See http://www.apple.com/support/bootcamp/.

2. From the Management Console, copy the recovery bundle to one of these:
   - Bootable USB drive

     or

   - FAT partition on the external Boot Camp volume
3. Shut down the computer with the Boot Camp volume to be recovered.
4. Connect the external drive to the computer.

   This drive contains the Boot Camp volume created in step 1.

5. To boot the computer from the external Boot Camp drive, do one of these:
   - Simultaneously press and hold the **Command-R** keys before the Power-On/Self-Test chime and during the computer boot-up.

     or

   - For earlier versions of Apple, press the **Option** key while you power on the computer.

     The *Mac OS X Utilities* dialog displays.
6. Select the Boot Camp volume (Windows) that is on the external drive.
7. In the USB drive or FAT partition, right-click the recovery bundle (from step 2) and select **Run as Administrator**.
8. Click **Yes.**
9. On the Dell Encryption Enterprise dialog, select an option:
   - *My system fails to boot* - If the user cannot boot into the system, select the first option

     or

   - *My system does not allow me to access encrypted data* - If the user cannot access some encrypted files when logging into the system, select the second option.
10. Click **Next.**

    The Backup and Recovery Information screen displays.

11. Click **Next.**
12. Select the Boot Camp volume to be recovered.

    NOTE:

    This is **not** the external Boot Camp volume.
13. Click **Next.**
14. Enter the password associated with this file.
15. Click **Next.**
16. Click **Recover.**
17. Click **Finish**.

18. When prompted to reboot, click **Yes.**
19. The system reboots, and you can log into Windows.

How to Retrieve a Firmware Password

Even if the client computer is configured for firmware password enforcement, it may not be needed for recovery. If the computer to recover is bootable, set the boot target in the Startup Disk system preferences pane.

In the case where the firmware password is needed to accomplish recovery (if the computer is not bootable and firmware password protection is enforced), follow the steps below.

To retrieve a firmware password, you must first retrieve the recovery bundle containing the disk's encryption keys.

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click **Populations > Endpoints**
3. Search for the device to recover.
4. Click the device name to open the Endpoint Detail page.
5. Click the **Details & Actions** tab.
6. Under *Shield Detail*, click the **Device Recovery Keys** link.
7. To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download**, and click **Save**.
8. Open the recovery bundle to retrieve the firmware password for the computer targeted for recovery. The firmware password is located within the string tags after the **FirmwarePassword** key.

   For example:

   <key>FirmwarePassword</key>

   <string>Bo$vun8WDn</string>

Client Tool

The Client Tool is a shell command that runs on a Mac endpoint. It is used to activate the client from a remote location or to run a script through a remote management utility. As administrator, you can activate a client and do the following:

- Activate as administrator
- Activate temporarily
- Retrieve information from the Mac client

To use the Client Tool manually, open a ssh session and enter the desired command on the command line.

Example:

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Enter **client** alone to display the usage instructions.

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/client

Table 1. Client Tool Commands

Command	Purpose	Syntax	Results
Activate	Activates a Mac client with the Dell Server but without going through the user interface. To activate, a valid domain user name and password must be entered.	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword **domainAccount** is the account used to activate via the client tool. **localAccount** is optional and is the current user if none is specified. The activation command has this format:	0 = Success 2 = Activation failed, and reason for failure 6 = User not found

Table 1. Client Tool Commands (continued)

Command	Purpose	Syntax	Results
	With the client tool you can activate a different local user than the one logged in and associate the domain credentials with that user.	client -a <user to activate*> <domainUser> <domainPassword> If you use the *No Auth User List* policy to create classes of users that do not get activated to the Dell Server, optionally, you can use the client tool to specify a different local account than the one logged in. See No Auth User List policy in step 3.	
Activate temporarily	Activates a Mac client without leaving a footprint.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Disk	Request the status of the disk	-d	Disk status displays, including the disk's ID, encryption status, and policies If empty braces are returned, it means no disks are encrypted.
FileVault Change Recovery	Cycle recovery keys for FileVault volumes	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile **NOTE:** deviceId must be a Logical Volume UUID or resolved to exactly one LVUUID. Often, a mount point or devnode works.	0 = Success 7= LVUUID not found 10 = Credential failure 11 = Escrow failed
Policy	Request the policies of the Mac client	-p	Policies display
Server	Polls the Dell Server for updated policies on behalf of the Mac client **NOTE:** The poll can take several minutes to complete.	-s	0 = Success Any other value indicates that either the Dell Server or Mac client software was busy or not responding.
Test	Test the Mac client's activation status	-t localAccount*	0 (domainAccount) = Success 1 = Not activated 6 = User not found
User	Request user information	-u localAccount*	The user's account information displays:

Table 1. Client Tool Commands (continued)

Command	Purpose	Syntax	Results
			0 (account information) = Success 6 = User not found
Version	Request the Mac client's version	-v	The version of the Mac client displays: Example: 8.x.x.xxxx

* The account running the Client Tool is used for the localAccount unless another is specified.

The Plist Option

The -plist option prints the results of the command with which it is combined. It follows the command and must appear prior to its arguments to make the results print as a plist.

Examples

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

To retrieve the policies from the client and print them.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

To temporarily activate the client and print the result.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -s ; echo$?**

To poll the Dell Server for updated policies on behalf of the client and display them on-screen.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

To retrieve the client's disk status and prints it.

Global Return Codes

No error 0

Parameter error 4

Unrecognized command 5

Socket timed out 8

Internal error 9

4

Tasks

Topics:

- Install Advanced Threat Prevention for Mac
- Verify the Advanced Threat Prevention Installation
- Collect Log Files for Endpoint Security Suite Enterprise
- View Advanced Threat Prevention Details
- Provision a Tenant
- Configure Advanced Threat Prevention Agent Auto Update
- Advanced Threat Prevention Troubleshooting

Install Advanced Threat Prevention for Mac

This section guides you through the Advanced Threat Prevention installation.

There are two methods to install Advanced Threat Prevention.

- Interactive Installation - This method is the easiest to install. However, this method does not allow any customizations.
- Command Line Installation - This is an advanced installation/upgrade method that should only be used by administrators experienced with command line syntax.

Prerequisites

Dell recommends that IT best practices are followed during the deployment of client software. This includes, but is not limited to, controlled test environments for initial tests and staggered deployments to users.

Before beginning this process, ensure the following prerequisites are met:

- Ensure that the Dell Server and its components are already installed.

  If you have not yet installed the Dell Server, follow the instructions in the appropriate guide below.

  Security Management Server Installation and Migration Guide

  Security Management Server Virtual Quick Start Guide and Installation Guide

- Ensure that you have the Dell Server hostname and port. Both are needed for client software installation.
- Ensure that the target computer has network connectivity to the Dell Server.
- If a client's server certificate is missing or is self-signed, you must disable the SSL certificate trust on the client side only.

Interactive Installation for Advanced Threat Prevention

This section guides you through the Advanced Threat Prevention for Mac installation process.

Interactive installation is the easiest method to install or upgrade the client software package. However, this method does not allow any customizations.

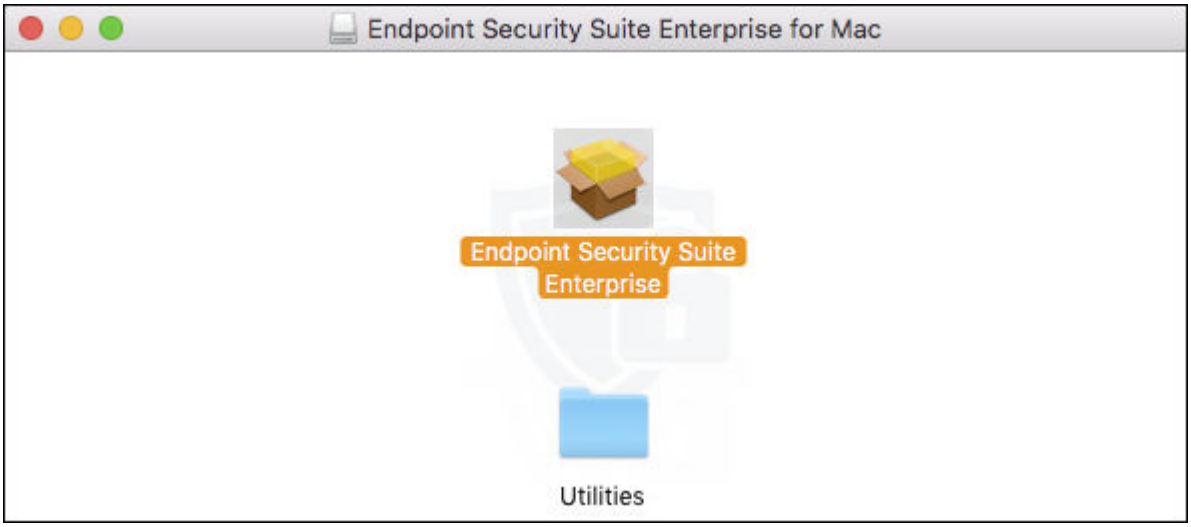
To install the client software, follow the steps below. You must have an administrator account to perform these steps.

NOTE:

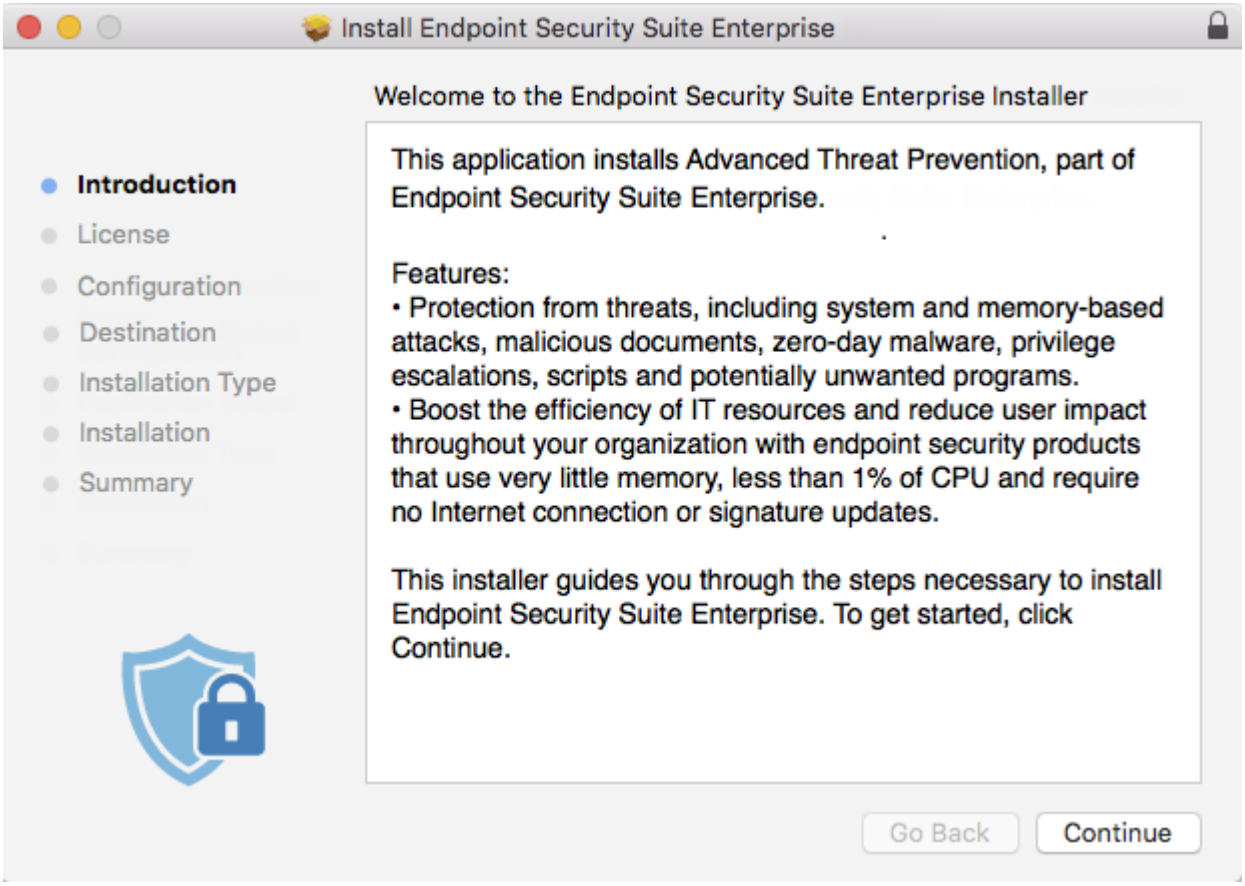
Before you begin, save the user's work and close other applications.

1. From the Dell installation media, mount the **Endpoint-Security-Suite-Enterprise-<version>.dmg** file.

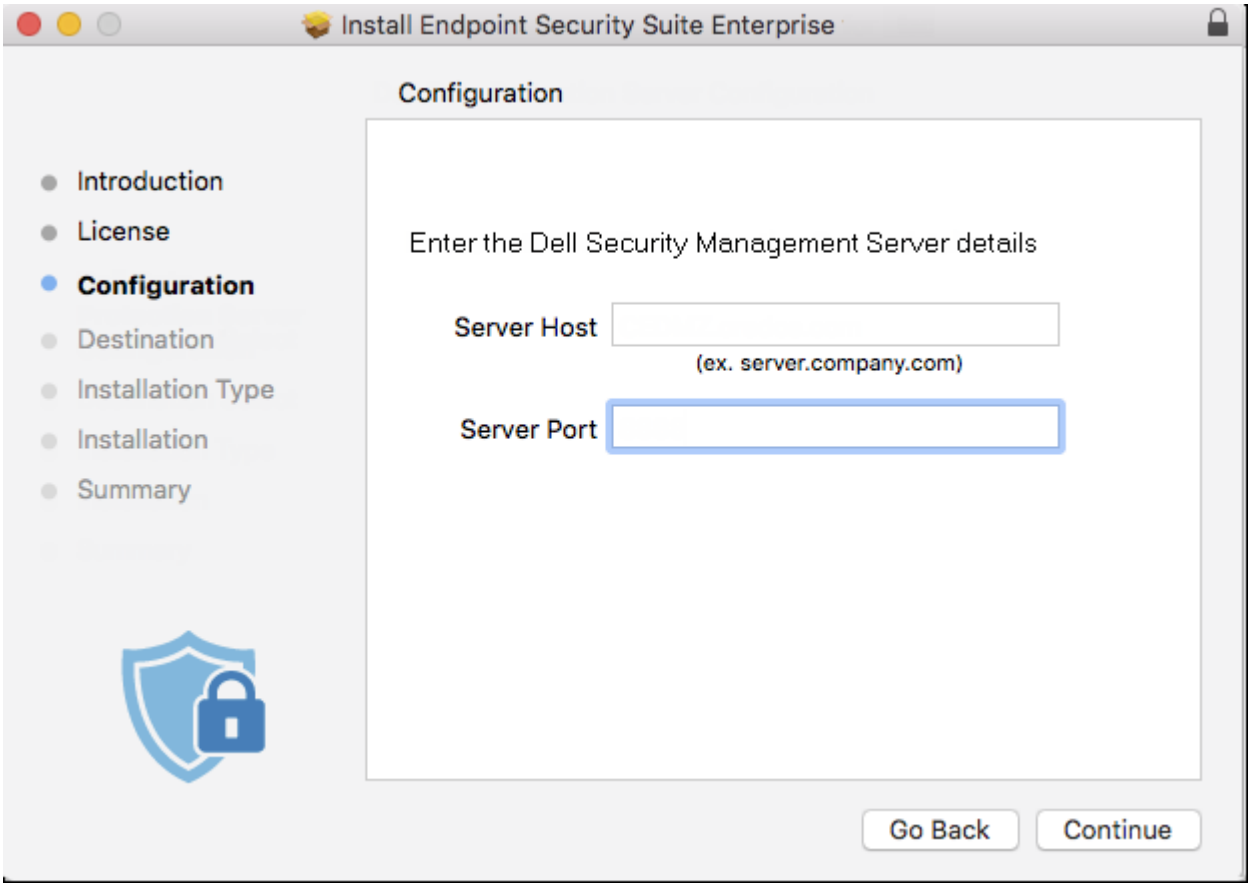
   Endpoint Security Suite Enterprise for Mac package opens.



2. Double-click the **Endpoint Security Suite Enterprise** package installer. The following message displays: *This package runs a program to determine if the software can be installed.*
3. Click **Continue**.
4. Read the Welcome text and click **Continue**.



5. Review the license agreement, click **Continue**, and then click **Agree** to accept the terms of the license agreement.
6. In the *Server Host* field, enter the fully qualified hostname of the Dell Server to manage the target user, such as server.organization.com.



7. In the *Server Port* field, enter **8888** and click **Continue**.
   Once a connection is established, the connectivity indicator changes from red to green.
   NOTE:
   The port is the Core Server service port, which is configurable. The default port number is 8888.
8. In the Installation screen, click **Install**.
9. When prompted, enter the administrator account credentials (required by the Mac OS X Installer application), then click **Install Software**.
10. When installation is complete, click **Close**.
    The Advanced Threat Prevention client for Mac is installed.
11. Close the package.
12. See Verify the Advanced Threat Prevention Installation.

If the system is not registered to the Dell Server, see the logs to determine if you have a valid certificate on your Dell Server. See Disable SSL Trust Certificate for Advanced Threat Prevention.

Interactive Uninstall of the Advanced Threat Prevention Client

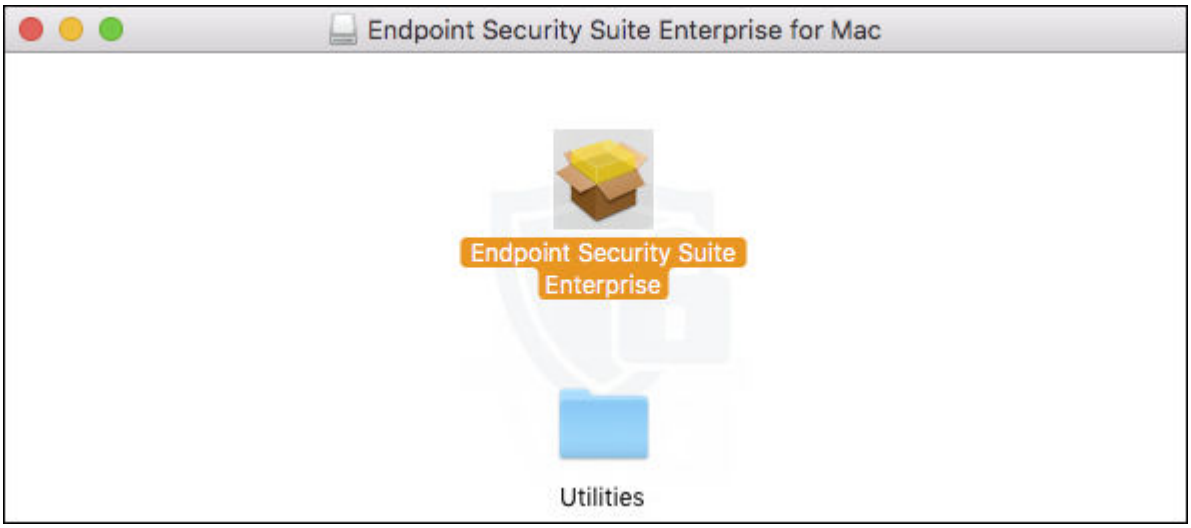
The client software may be uninstalled by running the **Uninstall Endpoint Security Suite Enterprise** application. To uninstall the client software, follow the steps below.

1. Mount the Endpoint-Security-Suite-Enterprise-<version>.dmg file.
2. In the Utilities folder, launch the **Uninstall Endpoint Security Suite Enterprise** application.
3. Click **Uninstall**.
4. When prompted, enter the administrator account credentials (required by the Mac OS X Installer application), then click **OK**.
   Messages display the status of the uninstallation.
5. At the success confirmation, click **OK**.
   Advanced Threat Prevention for Mac is now uninstalled, and the computer can be used normally.

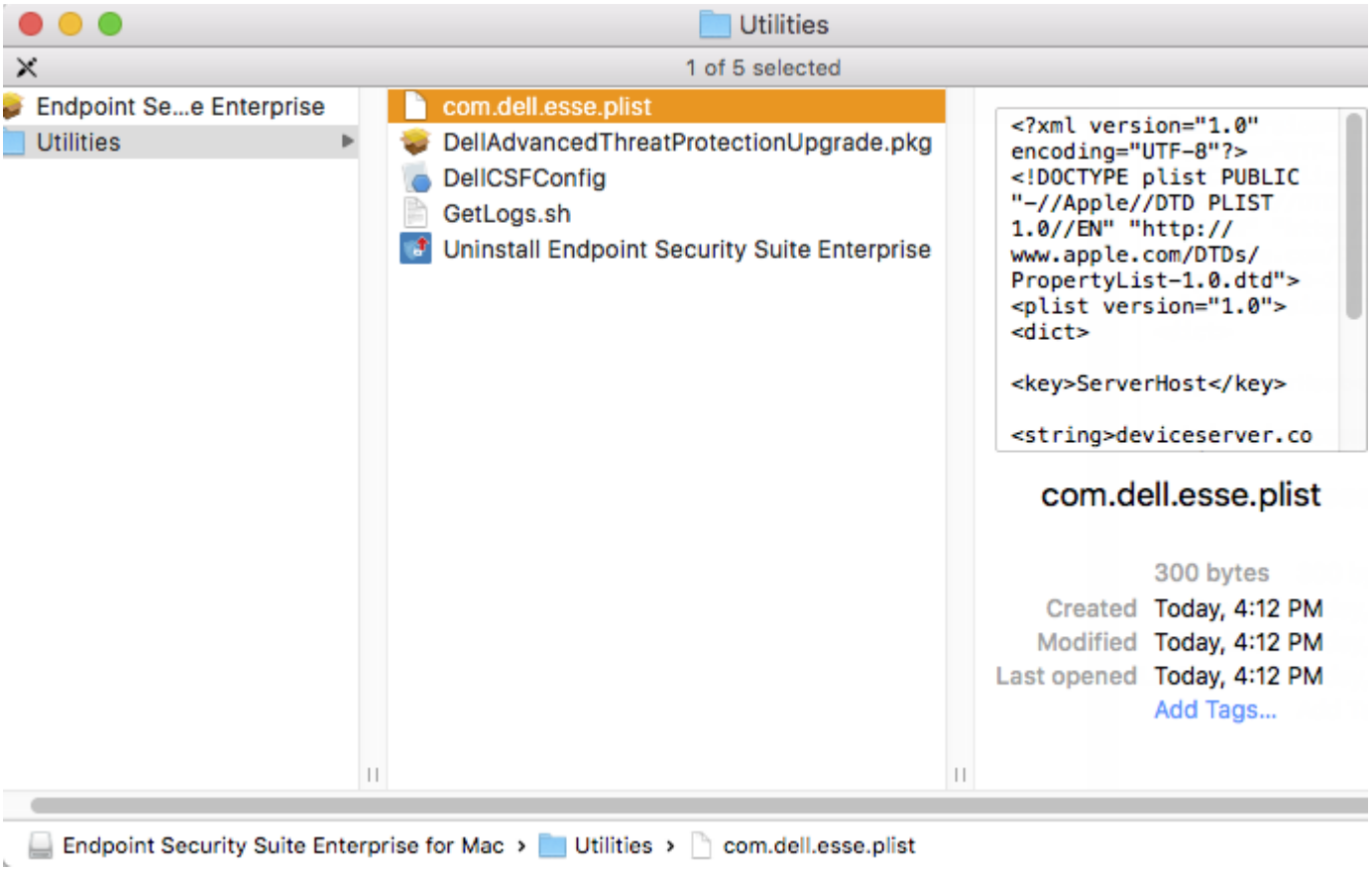
Command Line Installation for Advanced Threat Prevention

To install the Advanced Threat Prevention client using the command line, follow the steps below.

1. From the Dell installation media, mount the Endpoint-Security-Suite-Enterprise-<version>.dmg file. The Endpoint Security Suite Enterprise for Mac package opens.



2. From the Utilities folder, copy the **com.dell.esse.plist** file to the local drive.



3. Open the .plist file.
4. Edit the placeholder values with the fully qualified hostname of the Dell Server to manage the target user, such as server.organization.com, and port number **8888**:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
  <key>ServerHost</key>
  <string>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <array>
</dict>
</plist>
```

NOTE:

The port is the Core Server service port, which is configurable. The default port number is 8888.

5. Save and close the file.
6. For each targeted computer, copy the **Endpoint Security Suite Enterprise for Mac** package installer to a temporary folder and the modified **com.dell.esse.plist** file to **/Library/Preferences**.
7. If prompted, enter your credentials.
8. Launch a Terminal window.
9. Perform a command line installation of the package using the **installer** command:
   sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /

   NOTE:

   The -pkg path is the path to the .pkg installer found in the .dmg file.
10. Press **Enter**.
11. See Verify the ESSE Advanced Threat Prevention Installation.

Command Line Uninstall of Advanced Threat Prevention for Mac

To uninstall the Advanced Threat Prevention client using the command line, follow the steps below.

1. Launch a Terminal window.
2. Perform a command line uninstallation of the package using the **uninstaller** command:
   sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui

   NOTE: Be sure that the --noui switch is included at the end of the command.
3. Press **Enter**.
   Advanced Threat Prevention for Mac is now uninstalled, and the computer can be used normally.

Troubleshooting Advanced Threat Prevention for Mac

Disable SSL Trust Certificate or Policy Check for Advanced Threat Prevention

If a client's server certificate is missing or is self-signed, you must disable the SSL certificate trust on the client side only.

If you run self-signed certificates throughout your environment, disable PolicyCheck.

If you have self-signed certificates within your environment and you have not imported the certificate into the keychain on your Macs, set both DisableCertTrust and DisablePolicyCheck to False.

1. On the client, launch a Terminal window.
2. Enter the path to the DellCSFConfig.app:

   ```
   cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
   ```

3. Run the DellCSFConfig.app:

   ```
   sudo DellCSFConfig.app/Contents/MacOS/DellCSFConfig
   ```

   The following displays with default settings:

```
Current Settings:
ServerHost = deviceserver.company.com
ServerPort = 8888
DisableCertTrust = False
DisablePolicyCheck = False
DumpXmlInventory = False
DumpPolicies = False
```

4. Type **-help** to list the options.
5. To disable SSL Certificate Trust on the client, change `DisableCertTrust` to **True**.
6. To disable the Policy Signing Check on the client, change `DisablePolicyCheck` to **True**.

Add XML Inventory and Policy Changes to the Logs Folder

To add the inventory.xml or policies.xml files to the Logs folder:

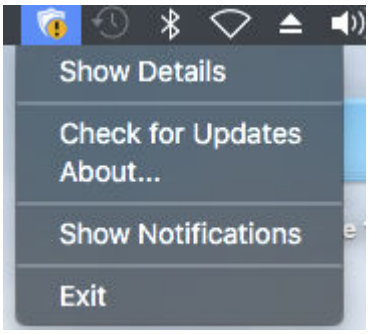
1. Run the DellCSFConfig.app as described above.
2. Change DumpXmlInventory to **True**.
3. Change DumpPolicies to **True**.

   Policy files are dumped only if a policy change has occurred.
4. To view inventory.xml and policies.xml log files, go to **/Library/Application\ Support/Dell/Dell\ Data\ Protection/**.

Verify the Advanced Threat Prevention Installation

Optionally, you can verify the installation.

1. Confirm that the Advanced Threat Prevention icon has a green badge  in the command bar.
2. If an exclamation mark displays on the icon, right click and select **Show Details**. It may indicate that you are not registered.

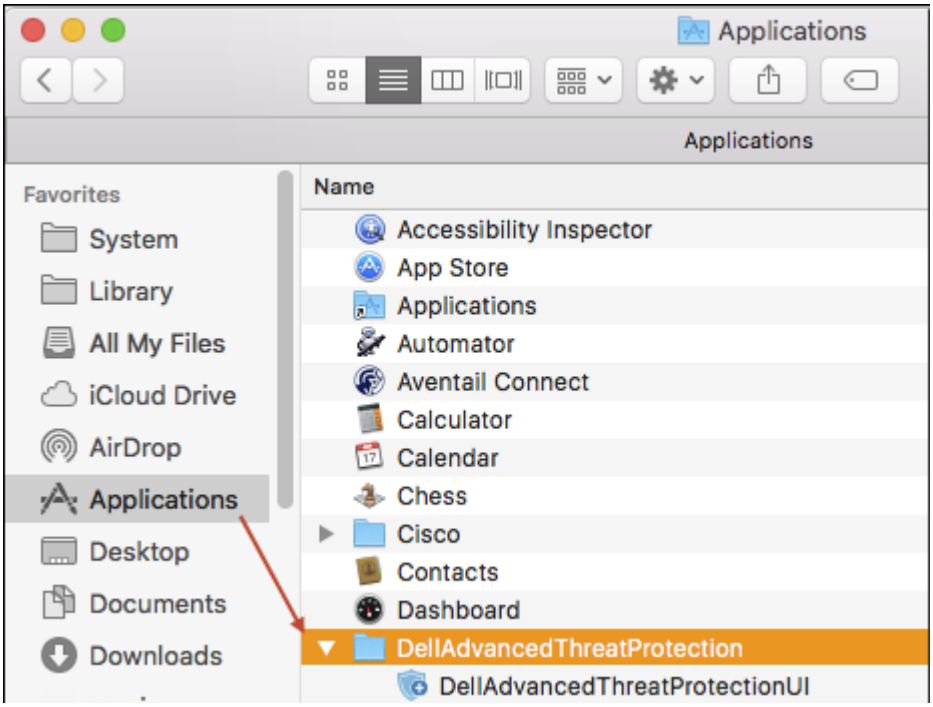


Check for Updates - Checks for Advanced Threat Prevention engine updates, not Dell Server policy updates.

About - Includes the following:

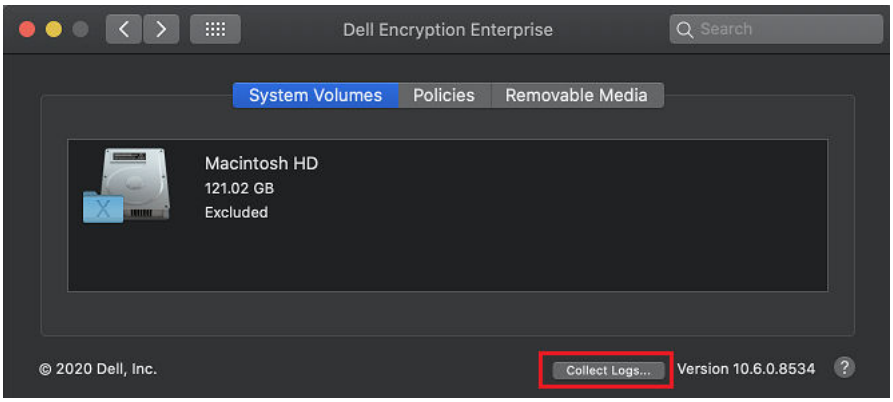
- Verison
- Policy - [online] indicates Server-based policy and [offline] indicates Airgap or offline-based policy
- Serial # - Use this when contacting support. This is the unique identifier of the installation.

3. In /Applications, the Advanced Threat Prevention folder is created.



Collect Log Files for Endpoint Security Suite Enterprise

In *System Preferences* > *Dell Encryption Enterprise* > *System Volumes*, a *Collect Logs* button at the bottom right allows an administrator to pre-generate logs for support. This action may impact performance while logs are collected.



DellLogs.zip contains the logs for Mac Encryption Enterprise and Advanced Threat Prevention. For information about how to collect the logs, see http://www.dell.com/support/article/us/en/19/SLN303924.

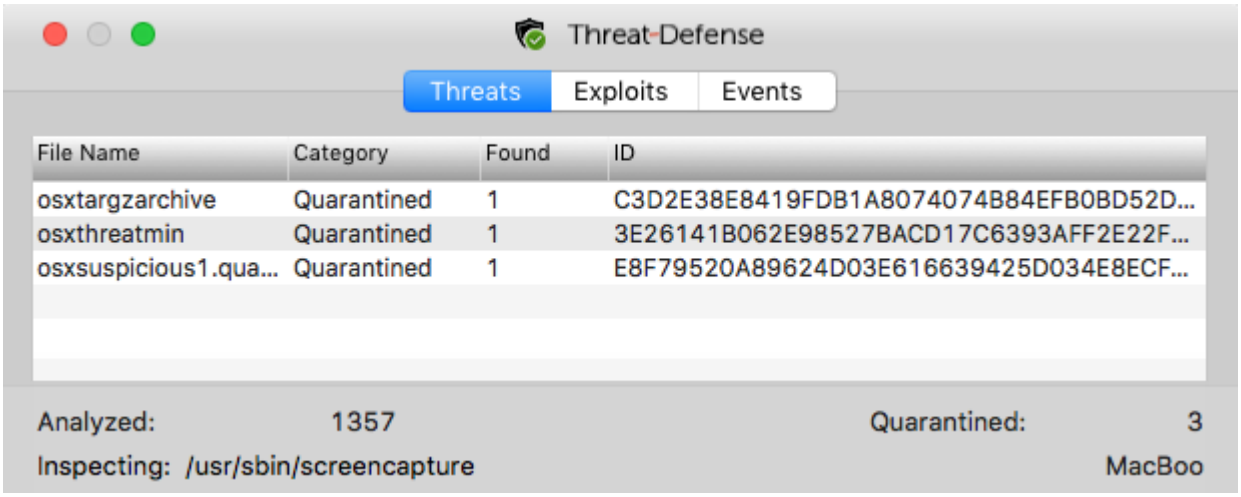
View Advanced Threat Prevention Details

After the Advanced Threat Prevention client is installed on an endpoint computer, it is recognized by the Dell Server as an agent.

Right-click the Advanced Threat Prevention icon  in the command bar, and select **Show Details**. The Advanced Threat Prevention Details screen has the following tabs.

Threats tab

The Threats tab displays all threats discovered on the device and the action taken. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.



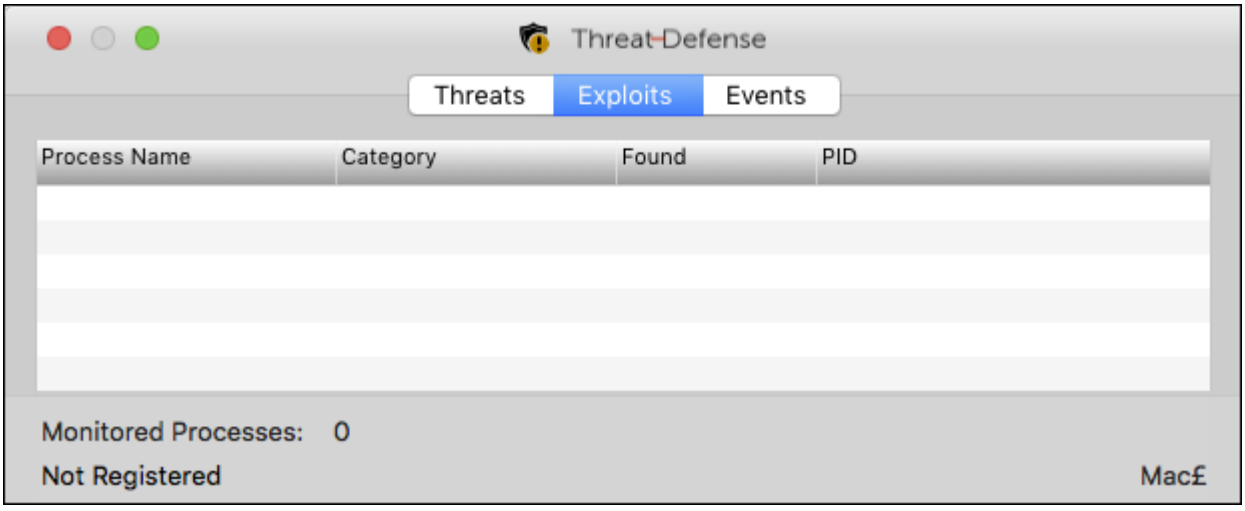
The Category column can include the following.

- **Unsafe** - A suspicious file that is likely to be malware
- **Abnormal** - A suspicious file that may be malware
- **Quarantined** - A file that is moved from its original location, stored in the Quarantine folder, and prevented from executing on the device.
- **Waived** - A file allowed to execute on the device.
- **Cleared** - A file that has been cleared within the organization. Cleared files include files that are Waived, added to the Safe list, and deleted from the Quarantine folder on the device.

For more information about Advanced Threat Prevention threat classifications, see *AdminHelp*, available in the Management Console.

Exploits tab

The Exploits tab lists exploits, which are considered threats.



Dell Server policies determine the action taken when an exploit is detected:

- **Ignore** - No action is taken against identified memory violations.
- **Alert** - The memory violation is recorded and reported to the Dell Server.
- **Block** - The process call is blocked if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run.

- **Terminate** - The process call is blocked if an application attempts to call a memory violation process. The application that made the call is terminated.

The following exploit types are detected:

- Stack Pivot
- Stack Protect
- Scanner Memory Search
- Malicious Payload

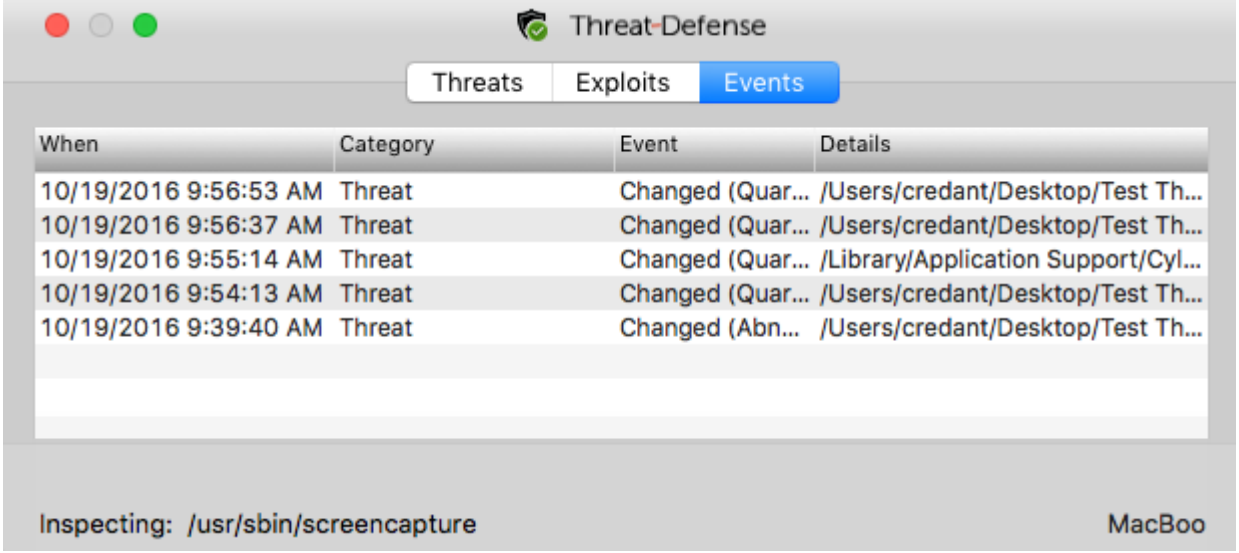
For more information about Exploit policies, see *AdminHelp*, available in the Management Console.

Events tab

NOTE:

An event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived.

The Events tab displays any threat events that occur on the device and displays them by event type as assigned by Advanced Threat Prevention. Data is removed when the system restarts.



Examples of event types include:

Threat Found

Threat Removed

Threat Quarantined

Threat Waived

Threat Changed

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**.

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

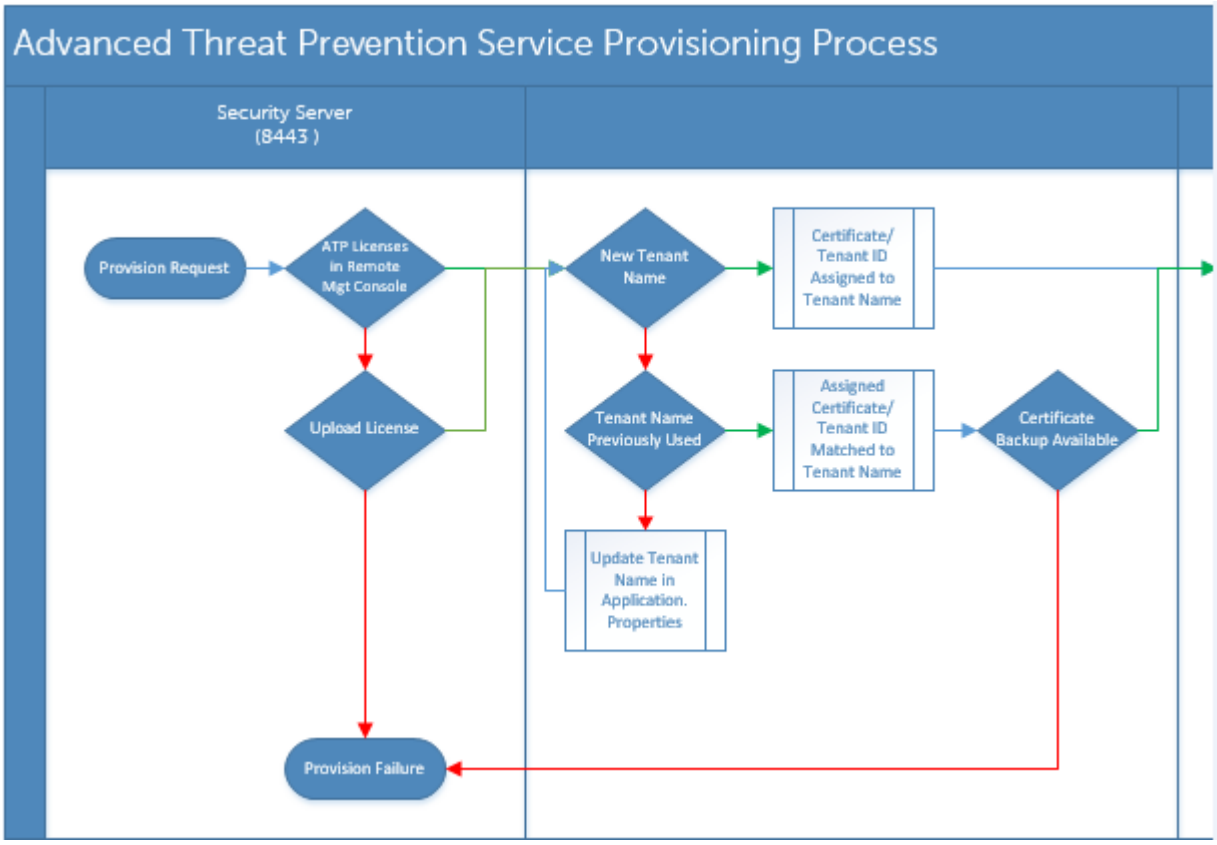
To stop receiving agent auto updates:

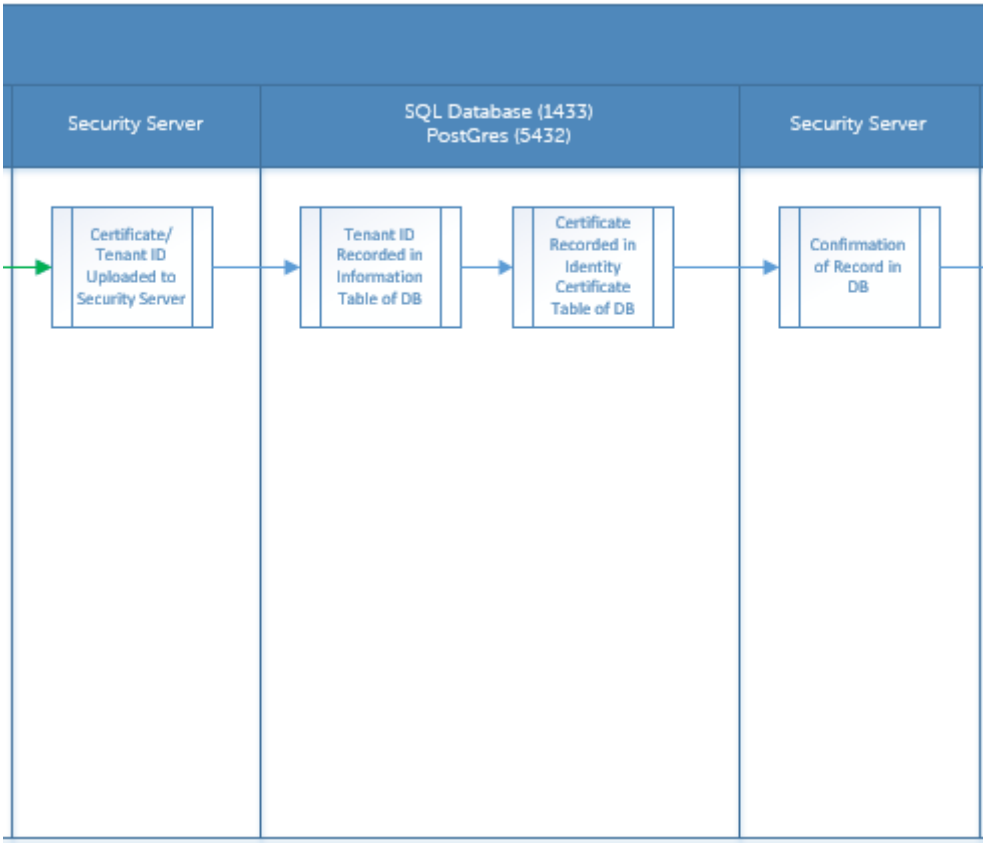
1. In the left pane of the Management Console, click **Management** > **Services Management**.
2. On the *Advance Threats* tab, under *Agent Auto Update*, click **Off** then click **Save Preferences**.

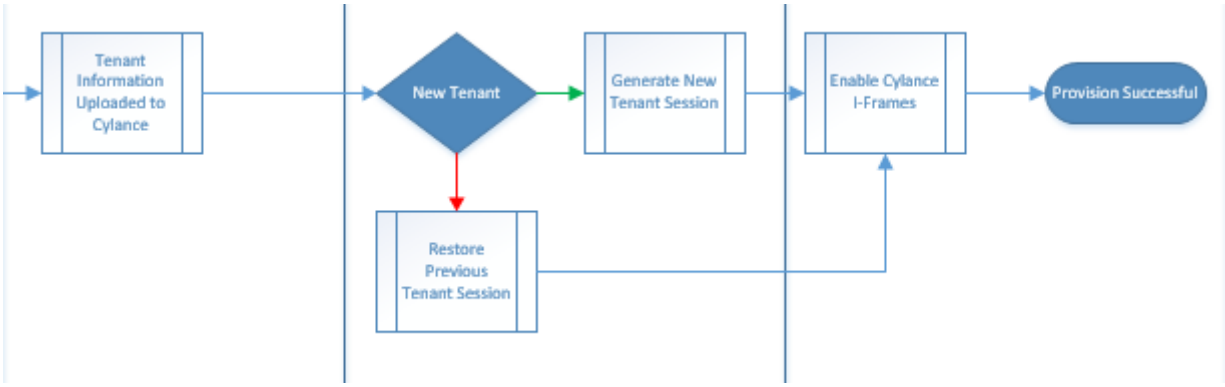
Advanced Threat Prevention Troubleshooting

Advanced Threat Prevention Provisioning and Agent Communication

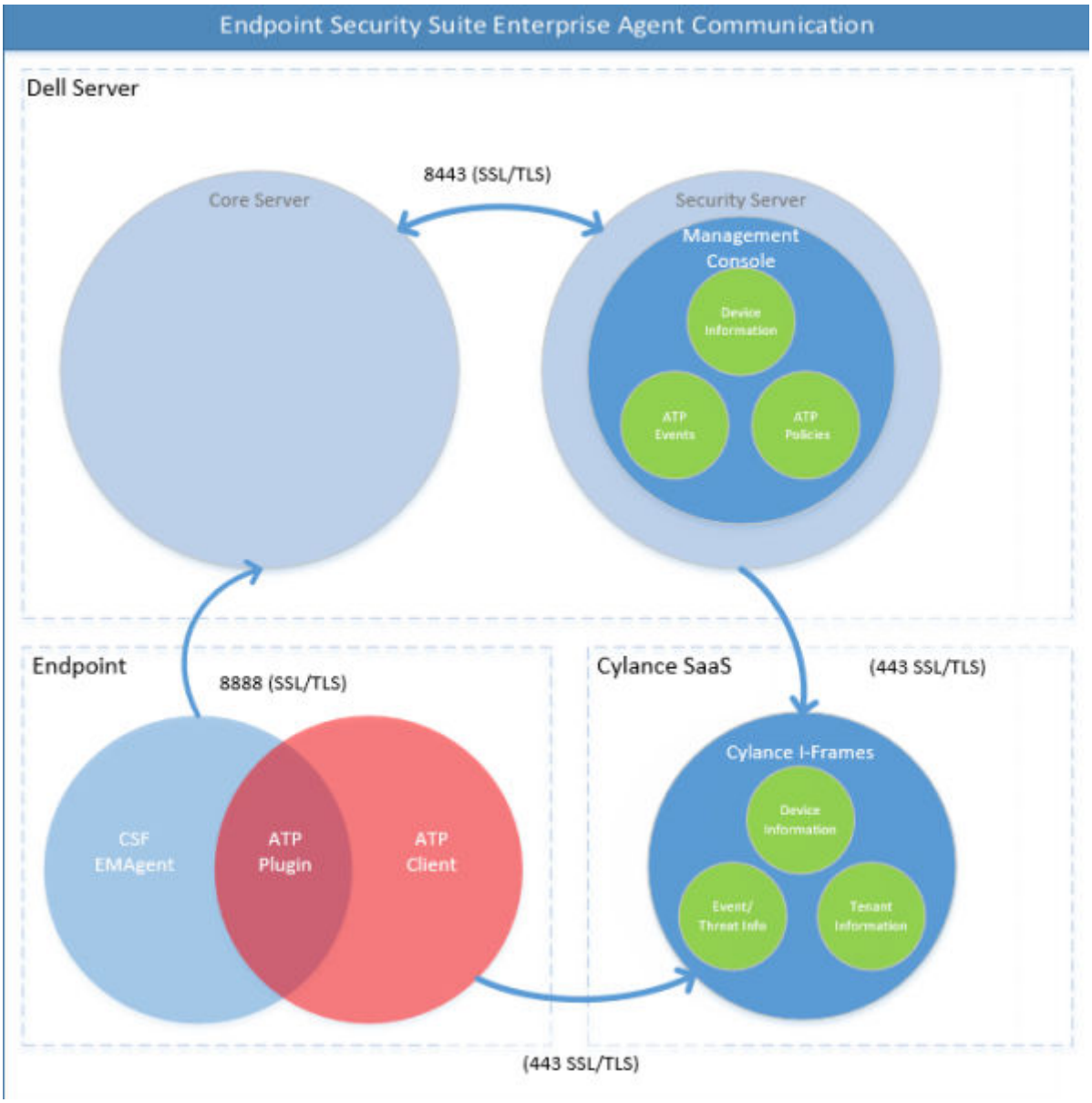
The following diagrams illustrate the Advanced Threat Prevention service provisioning process.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Tenant Name Previously Used
Certificate/ Tenant ID Assigned to Tenant Name
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB



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



5

Glossary

Security Server - Used for activations of Dell Encryption.

Policy Proxy - Used to distribute policies for client software.

Management Console - Dell Server's administrative console for the entire enterprise deployment.

Shield - Occasionally, you may see this name in the documentation and in the user interfaces. "Shield" is a name used to represent Dell Encryption.