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.
Command Line Uninstallation................................................................. 27
Uninstall SED Management................................................................. 27
Process.............................................................................................. 27
Deactivate the PBA............................................................................ 27
Uninstall SED Client.......................................................................... 28
Uninstall BitLocker Manager............................................................. 28
Command Line Uninstallation............................................................. 28

6 Data Security Uninstaller.................................................................. 29
Uninstall Endpoint Security Suite Enterprise..................................... 29

7 Provision a Tenant........................................................................... 34
Provision a Tenant............................................................................. 34

8 Configure Advanced Threat Prevention Agent Auto Update............ 38

9 Extract Child Installers.................................................................... 39

10 Configure Key Server...................................................................... 40
Services Panel - Add Domain Account User...................................... 40
Key Server Config File - Add User for Security Management Server Communication........................................ 41
Services Panel - Restart Key Server Service........................................ 41
Management Console - Add Forensic Administrator.......................... 42

11 Use the Administrative Download Utility (CMGAd)......................... 43
Use Forensic Mode........................................................................... 43
Use Admin Mode............................................................................. 45

12 Troubleshooting............................................................................. 47
All Clients - Troubleshooting............................................................. 47
All Clients - Protection Status............................................................. 47
Dell Encryption Troubleshooting (client and server).......................... 47
Activation on a Server Operating System........................................... 47
Encryption External Media and PCS Interactions............................... 50
Use WSScan.................................................................................... 51
Check Encryption Removal Agent Status.......................................... 54
Advanced Threat Prevention Troubleshooting.................................... 55
Find the Product Code with Windows PowerShell.............................. 55
Advanced Threat Prevention Provisioning and Agent Communication.. 55
BIOS Image Integrity Verification Process.......................................... 58
Dell ControlVault Drivers.................................................................. 59
Update Dell ControlVault Drivers and Firmware............................... 59

13 Glossary......................................................................................... 73
This guide details how to install and configure the application using the Endpoint Security Suite Enterprise master installer. This guide gives basic installation assistance. See the Advanced Installation Guide if you need information about installing the child installers, Security Management Server/Security Management Server Virtual configuration, or information beyond basic assistance with the Endpoint Security Suite Enterprise master installer.

All policy information and their descriptions are found in the AdminHelp.

**Before You Begin**

1. Install the Dell Server before deploying clients. Locate the correct guide as shown below, follow the instructions, and then return to this guide.

   - Security Management Server Installation and Migration Guide
   - Security Management Server Virtual Quick Start Guide and Installation Guide
   - Verify that polices are set as desired. Browse through the AdminHelp, available from the ? at the top right of the screen. The AdminHelp is page-level help designed to help you set and modify policy and understand your options with your Dell Server.
2 Provision a Tenant for Advanced Threat Prevention. A tenant must be provisioned in the Dell Server before Advanced Threat Prevention enforcement of policies becomes active.

3 Thoroughly read the Requirements chapter of this document.

4 Deploy clients to users.

**Using This Guide**

Use this guide in the following order.

- See Requirements for client prerequisites.
- Select one of the following:
  - Install Interactively Using the Master Installer
  - Install by Command Line Using the Master Installer

**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.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

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

All Clients

- IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.
- The user account performing the installation/upgrade/uninstallation must be a local or domain administrator user, which can be temporarily assigned by a deployment tool such as Microsoft SCCM. A non-administrator user that has elevated privileges is not supported.
- Back up all important data before beginning installation/uninstallation.
- Do not make changes to the computer, including inserting or removing external (USB) drives during installation.
- Administrators should ensure all necessary ports are available.
- Be sure to periodically check dell.com/support for the most current documentation and Technical Advisories.
- The Dell Data Security line of products does not support Windows Insider Preview releases.

Prerequisites

- The master installer installs these components if not already installed on the target computer.

Prerequisite

- Visual C++ 2012 Update 4 or later Redistributable Package (x86 and x64)
- Visual C++ 2015 Update 3 or later Redistributable Package (x86 and x64)

- To verify the version of Microsoft .Net installed, follow these instructions on the computer targeted for installation. See these instructions to install Microsoft .Net Framework 4.5.2.
- If installing Encryption in FIPS mode, Microsoft .Net Framework 4.6 is required.

Hardware

- The following table details the minimum supported computer hardware.

Hardware

- Intel Pentium or AMD Processor
- 500 MB available disk space
- 2 GB RAM

NOTE: Additional free disk space is required to encrypt files on the endpoint. Size varies based on enabled policies and drive capacity.
Localization

- Dell Encryption, SED management, PBA advanced authentication, Advanced Threat Prevention, and BitLocker Manager are multilingual user interface compliant and are localized in the following languages. Advanced Threat Prevention data displayed in the Management Console is English only.

<table>
<thead>
<tr>
<th>Language Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN - English</td>
</tr>
<tr>
<td>ES - Spanish</td>
</tr>
<tr>
<td>FR - French</td>
</tr>
</tbody>
</table>

Encryption

- The client computer must have network connectivity to activate.
- Turn off sleep mode during the initial encryption sweep to prevent an unattended computer from going to sleep. Encryption cannot occur on a sleeping computer (nor can decryption).
- Encryption does not support dual boot configurations since it is possible to encrypt system files of the other operating system, which would interfere with its operation.
- Encryption is validated against industry-leading antivirus providers. Hard-coded exclusions are in place for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. Encryption has also been tested with Microsoft Enhanced Mitigation Experience Toolkit.
- If your organization uses an anti-virus provider that is not listed, see KB article SLN288353 or Contact Dell ProSupport for help.
- Dell Encryption utilizes Intel's encryption instruction sets, Integrated Performance Primitives (IPP). For more information, see this kb.
- In-place operating system re-install is not supported. To re-install the operating system, perform a backup of the target computer, wipe the computer, install the operating system, then recover the encrypted data following established recovery procedures.
- The Secured Windows Hibernation File and Prevent Unsecured Hibernation policies are not supported in UEFI mode.
- Deferred activation allows the Active Directory user account used during activation to be independent of the account used to login to the endpoint. Instead of the network provider capturing the authentication information, the user instead manually specifies the Active Directory-based account when prompted. Once the credentials are entered, the authentication information is securely sent to the Dell Server which validates it against the configured Active Directory domains. For more information, see KB article SLN306341.
- Following Windows 10 feature upgrade, a restart is required to finalize Dell Encryption. The following message displays in the notification area after Windows 10 feature upgrades:

![Dell Encryption Restart Required](image)

Operating Systems

- The following table details supported operating systems.

<table>
<thead>
<tr>
<th>Windows Operating Systems (32- and 64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 7 SP1: Enterprise, Professional, Ultimate</td>
</tr>
</tbody>
</table>
Windows Operating Systems (32- and 64-bit)

- Windows Embedded Standard 7 with Application Compatibility template
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)
- VMware Workstation 12.5 and higher
- **Deferred Activation** includes support for all of the above

Encryption External Media

Operating Systems

- External media must have approximately 55MB available plus open space on the media that is equal to the largest file to be encrypted to host Encryption External Media.
- The following table details the operating systems supported when accessing media protected by Encryption External Media:

<table>
<thead>
<tr>
<th>Windows Operating Systems Supported to Access Encrypted Media (32- and 64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 7 SP1: Enterprise, Professional, Ultimate</td>
</tr>
<tr>
<td>- Windows Embedded Standard 7 with Application Compatibility template</td>
</tr>
<tr>
<td>- Windows 8.1: Enterprise, Pro</td>
</tr>
<tr>
<td>- Windows Embedded 8.1 Industry Enterprise</td>
</tr>
<tr>
<td>- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mac Operating Systems Supported to Access Encrypted Media (64-bit kernels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- macOS Sierra 10.12.6</td>
</tr>
<tr>
<td>- macOS High Sierra 10.13.5 - 10.13.6</td>
</tr>
</tbody>
</table>

Full Disk Encryption

Full Disk Encryption can **only** be installed through command line interface (CLI). Should you wish to install Full Disk Encryption, download the Endpoint Security Suite Enterprise Advanced Installation Guide for instructions.

- Full Disk Encryption requires activation against a Dell Server running v9.8.2 or later.
- Full Disk Encryption is not currently supported within virtualized host computers.
- Full Disk encryptions of multi-drive configurations are not supported.
- Third-party credential providers will not function with FDE features installed and all third-party credential providers will be disabled when the PBA is enabled.
- The client computer must have network connectivity or access code to activate.
- The computer must have a wired network connection for a smartcard user to log in through pre-boot authentication for the first time.
- Operating system Feature updates are not supported with Full Disk Encryption.
- A wired connection is required for the PBA to communicate with the Dell Server.
- An SED cannot be present on the target computer.
- Full Disk Encryption utilizes Intel's encryption instruction sets, Integrated Performance Primitives (IPP). For more information, see this kb.
- Full Disk Encryption is not supported with BitLocker or BitLocker Manager. Do not install Full Disk Encryption on a computer on which BitLocker or BitLocker Manager is installed.
- Dell recommends Intel Rapid Storage Technology Driver v15.2.0.0 or later, with NVMe drives.
• Any NVMe drive that is being leveraged for PBA:
  – The BIOS’ SATA operation must be set to RAID ON, as Dell’s PBA management does not support AHCI on NVMe drives.
  – The BIOS’s boot mode must be UEFI and Legacy option ROMs must be disabled.

• Any non-NVMe drive that is being leveraged for PBA:
  – The BIOS’ SATA operation must be set to AHCI, as Dell’s PBA management does not support RAID with non-NVMe drives.
  – RAID ON is not supported because access to read and write RAID-related data (at a sector that is not available on a locked non-NVMe drive) is not accessible at start-up, and cannot wait to read this data until after the user is logged on.
  – The operating system will crash when switched from RAID ON > AHCI if the AHCI controller drivers are not pre-installed. For instructions on how to switch from RAID > AHCI (or vice versa), see KB article SLN306460.

• Full Disk Encryption management does not support dual boot configurations since it is possible to encrypt system files of the other operating system, which would interfere with its operation.

• In-place operating system re-install is not supported. To re-install the operating system, perform a backup of the target computer, wipe the computer, install the operating system, then recover the encrypted data following established recovery procedures.

  **NOTE:** A password is required with pre-boot authentication. Dell recommends a minimum password setting compliant with internal security policies.

  **NOTE:** When PBA is used, the Sync All Users policy should be enabled if a computer has multiple users. Additionally, all users must have passwords. Zero-length password users will be locked out of the computer following activation.

  **NOTE:** Full Disk Encryption must be configured with Encryption Algorithm set to AES-256 and Encryption Mode set to CBC.

### Hardware

• The following table details supported hardware.

<table>
<thead>
<tr>
<th>Optional Embedded Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>– TPM 1.2 or 2.0</td>
</tr>
</tbody>
</table>

### Full Disk Encryption Client Operating Systems

• The following table details supported operating systems.

<table>
<thead>
<tr>
<th>Windows Operating Systems (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Windows 7 SP1: Enterprise, Professional, Ultimate (Legacy boot mode required)</td>
</tr>
</tbody>
</table>

### Advanced Threat Prevention

• To complete Advanced Threat Prevention installation when the Dell Server managing the client is running in Connected mode (default), the computer must have network connectivity. However, network connectivity is **not** required for Advanced Threat Prevention installation when the managing Dell Server is running in Disconnected mode.

• To provision a tenant for Advanced Threat Prevention, the Dell Server must have Internet connectivity.

• The optional Client Firewall and Web Protection features should **not** be installed on client computers that are managed by Dell Server running in Disconnected mode.
• Other vendors’ antivirus, antimalware, and antispyware applications may conflict with the Advanced Threat Prevention client. If possible, uninstall these applications. Conflicting software does not include Windows Defender. Firewall applications are allowed.

If uninstalling other antivirus, antimalware, and antispyware applications is not possible, you must add exclusions to Advanced Threat Prevention in the Dell Server and also to the other applications. For instructions on how to add exclusions to Advanced Threat Prevention in the Dell Server, see KB article SLN300970. For a list of exclusions to add to the other antivirus applications, see KB article SLN301562.

Operating Systems

• The following table details supported operating systems.

<table>
<thead>
<tr>
<th>Windows Operating Systems (32- and 64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 7 SP1: Enterprise, Professional, Ultimate</td>
</tr>
<tr>
<td>- Windows Embedded Standard 7</td>
</tr>
<tr>
<td>- Windows 8.1: Enterprise, Pro</td>
</tr>
</tbody>
</table>

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 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.

<table>
<thead>
<tr>
<th>Use</th>
<th>Application Protocol</th>
<th>Transport Protocol</th>
<th>Port Number</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Communication</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>Allow all https traffic to *.cylance.com</td>
<td>Outbound</td>
</tr>
</tbody>
</table>

For detailed information regarding the URLs being used, see KB article SLN303898.

BIOS Image Integrity Verification

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

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

Dell Computer Models supported with BIOS Image Integrity Verification

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
### Dell Computer Models supported with BIOS Image Integrity Verification

- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- Precision Workstation 3620
- Precision Workstation 7510
- Precision Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

### Client Firewall and Web Protection

- To successfully install Client Firewall and Web Protection, the computer must have network connectivity.
- Uninstall other vendors' anti-virus, anti-malware, anti-spyware, and firewall applications before installing the Client Firewall and Web Protection clients to prevent installation failures. Conflicting software does not include Windows Defender and Endpoint Security Suite Enterprise.
- The Web Protection feature is supported with the following browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Web Protection Support</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Yes</td>
<td>All Modern Versions</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Yes</td>
<td>Microsoft Edge is supported with Endpoint Security Suite Enterprise v10.1 and later</td>
</tr>
<tr>
<td>Microsoft Internet Explorer 11</td>
<td>Yes</td>
<td>All Modern Versions</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Yes</td>
<td>− Firefox 56 and later is supported with Endpoint Security Suite Enterprise v10.0 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>− Firefox 51 is supported with Endpoint Security Suite Enterprise v1.8 and later</td>
</tr>
</tbody>
</table>

### Ports

- To ensure that Client Firewall and Web Protection receives the most current Client Firewall and Web Protection updates, ports 443 and 80 must be available for the client to communicate with the various destination servers. If the ports are blocked for any reason, anti-virus signature updates (DAT files) cannot be downloaded, so computers may not have the most current protection. Ensure that client computers can access the URLs, as follows.

<table>
<thead>
<tr>
<th>Use</th>
<th>Application Protocol</th>
<th>Transport Protocol</th>
<th>Port Number</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation Service</td>
<td>SSL</td>
<td>TCP</td>
<td>443</td>
<td>tunnel.web.trustedsource.org</td>
<td>Outbound</td>
</tr>
<tr>
<td>Reputation Service Feedback</td>
<td>SSL</td>
<td>TCP</td>
<td>443</td>
<td>gtifeedback.trustedsource.org</td>
<td>Outbound</td>
</tr>
<tr>
<td>URL Reputation Database Update</td>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>list.smartfilter.com</td>
<td>Outbound</td>
</tr>
<tr>
<td>URL Reputation Lookup</td>
<td>SSL</td>
<td>TCP</td>
<td>443</td>
<td>tunnel.web.trustedsource.org</td>
<td>Outbound</td>
</tr>
</tbody>
</table>
Operating Systems

- The following table details supported operating systems.

**Windows Operating Systems (32- and 64-bit)**
- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version through v1607 - v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)

SED

- The computer must have a wired network connection to successfully install SED management.
- The computer must have a wired network connection for a smartcard user to log in through pre-boot authentication for the first time.
- Third-party credential providers will not function with SED Management installed and all third-party credential providers will be disabled when the PBA is enabled.
- IPv6 is not supported.
- SED Manager is not supported with multi-drive configurations.
- SED Manager is not currently supported within virtualized host computers.
- Dell Encryption utilizes Intel's encryption instruction sets, Integrated Performance Primitives (IPP). For more information, see KB article SLN301500.
- Be prepared to shut down and restart the computer after you apply policies and are ready to begin enforcing them.
- Computers equipped with self-encrypting drives cannot be used with HCA cards. Incompatibilities exist that prevent the provisioning of the HCA. Dell does not sell computers with self-encrypting drives that support the HCA module. This unsupported configuration would be an after-market configuration.
- If the computer targeted for encryption is equipped with a self-encrypting drive, ensure that the Active Directory option, User Must Change Password at Next Logon, is disabled. Pre-boot authentication does not support this Active Directory option.
- Dell recommends that you do not change the authentication method after the PBA has been activated. If you must switch to a different authentication method, you must either:
  - Remove all the users from the PBA.
  or
  - Deactivate the PBA, change the authentication method, and then re-activate the PBA.

**IMPORTANT:**
Due to the nature of RAID and SEDs, SED management does not support RAID. The issue with RAID=On with SEDs is that RAID requires access to the disk to read and write RAID-related data at a high sector not available on a locked SED from start and cannot wait to read this data until after the user is logged on. Change the SATA operation in the BIOS from RAID=On to AHCI to resolve the issue. If the operating system does not have the AHCI controller drivers pre-installed, the operating system will crash when switched from RAID=On to AHCI.

- Configuration of self-encrypting drives for SED management differ between NVMe and non-NVMe (SATA) drives, as follows.
  - Any NVMe drive that is being leveraged for SED:
    - The BIOS’ SATA operation must be set to RAID ON, as SED management does not support AHCI on NVMe drives.
    - The BIOS's boot mode must be UEFI and Legacy option ROMs must be disabled.
  - Any non-NVMe drive that is being leveraged for SED:
    - The BIOS’ SATA operation must be set to AHCI, as SED management does not support RAID with non-NVMe drives.
    - RAID ON is not supported because access to read and write RAID-related data (at a sector that is not available on a locked non-NVMe drive) is not accessible at start-up, and cannot wait to read this data until after the user is logged on.
The operating system will crash when switched from RAID ON > AHCI if the AHCI controller drivers are not pre-installed. For instructions on how to switch from RAID > AHCI (or vice versa), see KB article SLN306460.

Supported OPAL compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at www.dell.com/support. Dell recommends Intel Rapid Storage Technology Driver version 15.2.0.0 or later, with NVMe drives.

**NOTE:** The Intel Rapid Storage Technology Drivers are platform dependent. You can find your system’s driver at the link above based on your computer model.

- SED management is not supported with Encryption on server operating systems or Advanced Threat Prevention on a server operating system.

**NOTE:** A password is required with pre-boot authentication. Dell recommends a minimum password setting compliant with internal security policies.

**NOTE:** When PBA is used, the Sync All Users policy should be enabled if a computer has multiple users. Additionally, all users must have passwords. Zero-length password users will be locked out of the computer following activation.

### Hardware

### International Keyboards

The following table lists international keyboards supported with Pre-boot Authentication on UEFI and non-UEFI computers.

#### International Keyboard Support - UEFI

<table>
<thead>
<tr>
<th>Keyboard Code</th>
<th>Language Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-FR</td>
<td>(French Swiss)</td>
</tr>
<tr>
<td>DE-CH</td>
<td>(German Swiss)</td>
</tr>
<tr>
<td>EN-US</td>
<td>English (American English)</td>
</tr>
<tr>
<td>EN-GB</td>
<td>English (British English)</td>
</tr>
<tr>
<td>EN-CA</td>
<td>English (Canadian English)</td>
</tr>
</tbody>
</table>

#### International Keyboard Support - Non-UEFI

<table>
<thead>
<tr>
<th>Keyboard Code</th>
<th>Language Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AR</td>
<td>Arabic (using Latin letters)</td>
</tr>
<tr>
<td>DE-FR</td>
<td>(French Swiss)</td>
</tr>
<tr>
<td>DE-CH</td>
<td>(German Swiss)</td>
</tr>
<tr>
<td>EN-US</td>
<td>English (American English)</td>
</tr>
<tr>
<td>EN-GB</td>
<td>English (British English)</td>
</tr>
<tr>
<td>EN-CA</td>
<td>English (Canadian English)</td>
</tr>
</tbody>
</table>

### Localization

SED management is a multilingual user interface compliant and is localized the following languages. UEFI mode and PBA advanced authentication are supported in the following languages:

#### Language Support

<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN</td>
<td>English</td>
</tr>
<tr>
<td>FR</td>
<td>French</td>
</tr>
<tr>
<td>IT</td>
<td>Italian</td>
</tr>
<tr>
<td>DE</td>
<td>German</td>
</tr>
<tr>
<td>ES</td>
<td>Spanish</td>
</tr>
<tr>
<td>JA</td>
<td>Japanese</td>
</tr>
<tr>
<td>KO</td>
<td>Korean</td>
</tr>
<tr>
<td>PT-BR</td>
<td>Portuguese, Brazilian</td>
</tr>
<tr>
<td>PT-PT</td>
<td>Portuguese, Portugal (Iberian)</td>
</tr>
</tbody>
</table>
Operating Systems

- The following table details the supported operating systems.

<table>
<thead>
<tr>
<th>Windows Operating Systems (32- and 64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate (supported with Legacy Boot mode but not UEFI)</td>
</tr>
<tr>
<td>- Windows 8.1: Enterprise, Pro</td>
</tr>
<tr>
<td>- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)</td>
</tr>
</tbody>
</table>

**NOTE:** NVMe self-encrypting drives are not supported with Windows 7.

BitLocker Manager

- Consider reviewing Microsoft BitLocker requirements if BitLocker is not yet deployed in your environment.
- Ensure that the PBA partition is already set up. If BitLocker Manager is installed before the PBA partition is set up, BitLocker cannot be enabled and BitLocker Manager will not be operational.
- A Dell Server is required to use BitLocker Manager.
- Ensure a signing certificate is available within the database. For more information, see KB article SLN307028.
- The keyboard, mouse, and video components must be directly connected to the computer. Do not use a KVM switch to manage peripherals as the KVM switch can interfere with the computer's ability to properly identify hardware.
- Turn on and enable the TPM. BitLocker Manager takes ownership of the TPM and does not require a reboot. However, if a TPM ownership already exists, BitLocker Manager begins the encryption setup process (no restart is required). The point is that the TPM must be owned and enabled.
- BitLocker Manager is not supported with Encryption of server operating systems or Advanced Threat Prevention on a server operating system.

Hardware

- The following table details supported hardware.

<table>
<thead>
<tr>
<th>Optional Embedded Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>- TPM 1.2 or 2.0</td>
</tr>
</tbody>
</table>

Operating Systems

- The following table details supported operating systems.

<table>
<thead>
<tr>
<th>Windows Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 7 SP0-SP1: Enterprise, Ultimate (32- and 64-bit)</td>
</tr>
<tr>
<td>- Windows 10: Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)</td>
</tr>
</tbody>
</table>
Windows updates KB3133977 and KB3125574 must not be installed if installing BitLocker Manager on Windows 7.
Install Using the Master Installer

- Command line switches and parameters are case-sensitive.
- To install using non-default ports, use the child installers instead of the master installer.
- Endpoint Security Suite Enterprise master installer log files are located at C:\ProgramData\Del\Dell Data Protection\Installer.
- Instruct users to see the following document and help files for application assistance:
  - See the Dell Encrypt Help to learn how to use the features of Encryption. Access the help from <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help.
  - See the Encryption External Media Help to learn how the features of Encryption External Media. Access the help from <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS.
  - See the Endpoint Security Suite Enterprise Help to learn how to use the features of Advanced Threat Prevention. Access the help from <Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help.
- Users should update their policies by right-clicking the Dell Encryption icon in the notification area and selecting Check for Policy Updates after installation completes.
- The master installer installs the entire suite of products. There are two methods to install using the master installer. Choose one of the following.
  - Install Interactively Using the Master Installer
  or
  - Install by Command Line Using the Master Installer

Install Interactively Using the Master Installer

- The Endpoint Security Suite Enterprise master installer can be located at:
  - From Your Dell FTP Account - Locate the installation bundle at Endpoint-Security-Suite-Ent-1.x.x.xxx.zip.
- Use these instructions to install or update Dell Endpoint Security Suite Enterprise interactively using the Endpoint Security Suite Enterprise master installer. This method can be used to install the suite of products on one computer at a time.

1. Locate DDSSuite.exe in the Dell installation media. Copy it to the local computer.
2. Double-click DDSSuite.exe to launch the installer. This may take several minutes.
3. Click Next in the Welcome dialog.
4. Read the license agreement, accept the terms, and click Next.
5. In On-Prem Dell Management Server Name, enter the fully qualified hostname of the Dell Server to manage the target user, such as server.organization.com.
   In Dell Device Server URL, enter the URL of the Dell Server with which the client will communicate.

   The format is https://server.organization.com:8443/xapi/ (including trailing forward slash).

   Click Next.
6 Click **Next** to install the product in the default location of `C:\Program Files\Dell\Dell Data Protection`. Dell recommends installing in the default location only, as problems may arise when installing in other locations.

7 Select the components to be installed.

   - **Security Framework** installs the underlying security framework.
   - **Encryption** installs the Encryption client, the component that enforces security policy, whether a computer is connected to the network, disconnected from the network, lost, or stolen.
   - **Threat Protection** installs the Threat Protection clients, which are malware and antivirus protection to scan for viruses, spyware, and unwanted programs, client firewall to monitor communication between the computer and resources on the network and the Internet, and web filtering to display safety ratings or block access to websites during online browsing.
   - **BitLocker Manager** installs the BitLocker Manager client, designed to enhance the security of BitLocker deployments by simplifying and reducing the cost of ownership through centralized management of BitLocker encryption policies.
   - **Advanced Threat Prevention** installs the Advanced Threat Prevention client, which is next-generation antivirus protection that uses algorithmic science and machine learning to identify, classify, and prevent both known and unknown cyberthreats from executing or harming endpoints.
   - **Web Protection and Firewall** installs the optional features, Web Protection and Firewall. The Client Firewall checks all incoming and outgoing traffic against its list of rules. Web Protection monitors web browsing and downloads to identify threats and enforce action set by policy when a threat is detected, based on ratings for websites.

Click **Next** when your selections are complete.
Click **Install** to begin the installation. Installation takes several minutes.

Select **Yes, I want to restart my computer now** and click **Finish**.
Install by Command Line Using the Master Installer

- The switches must be specified first in a command line installation. Other parameters go inside an argument that is passed to the /v switch.

**Switches**

- The following table describes the switches that can be used with the Endpoint Security Suite Enterprise master installer.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-y -gm2</td>
<td>Pre-extraction of Endpoint Security Suite Enterprise master installer. The -y and -gm2 switches must be used together. Do not separate the switches.</td>
</tr>
<tr>
<td>/S</td>
<td>Silent installation</td>
</tr>
<tr>
<td>/z</td>
<td>Pass variables to the .msi inside the DDSSuite.exe</td>
</tr>
</tbody>
</table>

**Parameters**

- The following table describes the parameters that can be used with the Endpoint Security Suite Enterprise master installer. The Endpoint Security Suite Enterprise master installer cannot exclude individual components but can receive commands to specify which components should be installed.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUPPRESSREBOOT</td>
<td>Suppresses the automatic reboot after the installation completes. Can be used in SILENT mode.</td>
</tr>
<tr>
<td>SERVER</td>
<td>Specifies the URL of the Dell Server.</td>
</tr>
<tr>
<td>InstallPath</td>
<td>Specifies the path for the installation. Can be used in SILENT mode.</td>
</tr>
<tr>
<td>FEATURES</td>
<td>Specifies the components that can be installed in SILENT mode.</td>
</tr>
<tr>
<td>ATP</td>
<td>Advanced Threat Prevention only</td>
</tr>
<tr>
<td>DE-ATP</td>
<td>Advanced Threat Prevention and Encryption. This is the default installation option if the FEATURES parameter is not specified</td>
</tr>
<tr>
<td>DE</td>
<td>Drive Encryption client only</td>
</tr>
<tr>
<td>BLM</td>
<td>BitLocker Manager</td>
</tr>
<tr>
<td>SED</td>
<td>SED management (Encryption Management Agent/Manager, PBA/GPE Drivers)(Available only when installed on a workstation operating system)</td>
</tr>
<tr>
<td>ATP-WEBFIREWALL</td>
<td>Advanced Threat Prevention with Client Firewall and Web Protection</td>
</tr>
<tr>
<td>DE-ATP-WEBFIREWALL</td>
<td>Encryption and Advanced Threat Prevention with Client Firewall and Web Protection</td>
</tr>
</tbody>
</table>

**NOTE:** For upgrades from Encryption Enterprise or from pre-v1.4 Endpoint Security Suite Enterprise, ATP-WEBFIREWALL or DE-ATP-WEBFIREWALL *must* be specified in order to install Client Firewall and Web Protection. Do not specify ATP-WEBFIREWALL or DE-ATP-WEBFIREWALL when installing a client to be managed by Dell Server running in Disconnected mode.

BLM_ONLY=1 Must be used when using FEATURES=BLM in the command line to exclude the SED management plugin.

**Example Command Line**

- Command line parameters are case-sensitive.
- (On a workstation operating system) This example installs all components using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of `C:\Program Files\Dell\Dell Data Protection\` and configures it to use the specified Dell Server.

  ```cmd
  "DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com""
  ```

- (On a workstation operating system) This example installs Advanced Threat Prevention and Encryption *only* using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of `C:\Program Files\Dell\Dell Data Protection\` and configures it to use the specified Dell Server.

  ```cmd
  "DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=DE-ATP""
  ```

- (On a workstation operating system) This example installs Advanced Threat Prevention, Encryption, and SED management using the Endpoint Security Suite Enterprise master installer on standard ports, silently, with a suppressed reboot, in the default location of `C:\Program Files\Dell\Dell Data Protection\` and configures it to use the specified Dell Server.

  ```cmd
  "DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=ATP-SED, SUPPRESSREBOOT=1""
  ```

- (On a workstation operating system) This example installs Advanced Threat Prevention, Encryption, Web Protection, and Client Firewall using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of `C:\Program Files\Dell\Dell Data Protection\` and configures it to use the specified Dell Server.

  ```cmd
  "DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL""
  ```
(On a server operating system) This example installs Advanced Threat Prevention and Encryption, only using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of \Program Files\Dell\Dell Data Protection\, and configures it to use the specified Dell Server.

"DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=DE-ATP\"

(On a server operating system) This example installs Advanced Threat Prevention, Encryption, Web Protection, and Client Firewall using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of \Program Files\Dell\Dell Data Protection\.

"DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREFWALL\"

(On a server operating system) This example installs Advanced Threat Prevention, only using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of \Program Files\Dell\Dell Data Protection\, and configures it to use the specified Dell Server.

"DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=ATP\"

(On a server operating system) This example installs Encryption, only using the Endpoint Security Suite Enterprise master installer on standard ports, silently, in the default location of \Program Files\Dell\Dell Data Protection\, and configures it to use the specified Dell Server.

"DDSSuite.exe" -y -gm2 /S /z""SERVER=server.organization.com, FEATURES=DE\"
Uninstall the Master Installer

- Dell recommends using the Data Security Uninstaller to remove the Data Security suite.
- Each component must be uninstalled separately, followed by uninstallation of the Endpoint Security Suite Enterprise master installer. The clients must be uninstalled in a **specific order to prevent uninstallation failures**.
- Follow the instructions in Extract the Child Installers from the Master Installer to obtain child installers.
- Ensure that the same version of Endpoint Security Suite Enterprise master installer (and thereby clients) is used for uninstallation as installation.
- This chapter refers you to other chapters that contain detailed instructions of how to uninstall the child installers. This chapter explains the last step only, uninstalling the master installer.
- Uninstall the clients in the following order.
  a. Uninstall Encryption Client.
  c. Uninstall SED Client (this uninstalls the Dell Encryption Management Agent, which cannot be uninstalled until Advanced Threat Prevention is uninstalled).
  d. Uninstall BitLocker Manager Client
- Proceed to Uninstall the Master Installer.

Uninstall the Endpoint Security Suite Enterprise Master Installer

Now that all of the individual clients have been uninstalled, the master installer can be uninstalled.

Command Line Uninstallation

- The following example silently uninstalls the Endpoint Security Suite Enterprise master installer.

  "DDSSuite.exe" -y -gm2 /S /x

  Reboot the computer when finished.
Uninstall Using the Child Installers

- Dell recommends using the Data Security Uninstaller to remove the Data Security suite.
- To uninstall each client individually, the child executable files must first be extracted from the Endpoint Security Suite Enterprise master installer, as shown in Extract the Child Installers from the Master Installer. Alternatively, run an administrative installation to extract the .msi.
- Ensure that the same versions of client are used for uninstallation as installation.
- Command line switches and parameters are case-sensitive.
- Be sure to enclose a value that contains one or more special characters, such as a blank space in the command line, in escaped quotation marks. Command line parameters are case-sensitive.
- Use these installers to uninstall the clients using a scripted installation, batch files, or any other push technology available to your organization.
- Log files - Windows creates unique child installer uninstallation log files for the logged in user at %temp%, located at C:\Users \<UserName>\AppData\Local\Temp.

If you decide to add separate a log file when you run the installer, ensure that the log file has a unique name, as child installer log files do not append. The standard .msi command can be used be create a log file by using /l:C:\<any directory>\<any log file name>.log. Dell does not recommend using "/l*v" (verbose logging) in a command line uninstallation, as the username/password is recorded in the log file.

- All child installers use the same basic .msi switches and display options, except where noted, for command line uninstallations. The switches must be specified first. The /v switch is required and takes an argument. Other parameters go inside an argument that is passed to the /v switch.

Display options can be specified at the end of the argument passed to the /v switch to achieve the expected behavior. Do not use both /q and /qn in the same command line. Only use ! and - after /qb.

### Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/v</td>
<td>Pass variables to the .msi inside the setup.exe. The content must always be enclosed in plain-text quotes.</td>
</tr>
<tr>
<td>/s</td>
<td>Silent mode</td>
</tr>
<tr>
<td>/x</td>
<td>Uninstall mode</td>
</tr>
<tr>
<td>/a</td>
<td>Administrative install (copies all files inside the .msi)</td>
</tr>
</tbody>
</table>

**NOTE:**

With /v, the Microsoft default options are available. For a list of options, see https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

### Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/q</td>
<td>No Progress dialog, restarts itself after process completion</td>
</tr>
<tr>
<td>/qb</td>
<td>Progress dialog with Cancel button, prompts for restart</td>
</tr>
<tr>
<td>/qb-</td>
<td>Progress dialog with Cancel button, restarts itself after process completion</td>
</tr>
<tr>
<td>Option</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/qb!</td>
<td>Progress dialog without Cancel button, prompts for restart</td>
</tr>
<tr>
<td>/qb!-</td>
<td>Progress dialog without Cancel button, restarts itself after process completion</td>
</tr>
<tr>
<td>/qn</td>
<td>No user interface</td>
</tr>
</tbody>
</table>

**Uninstall Encryption and Encryption on Server Operating System**

- To reduce decryption time, run the Windows Disk Cleanup Wizard to remove temporary files and other unneeded data.
- Plan to decrypt overnight, if possible.
- Turn off sleep mode to prevent an unattended computer from going to sleep. Decryption cannot occur on a sleeping computer.
- Shut down all processes and applications to minimize decryption failures because of locked files.
- Once the uninstall is complete and decryption is in progress, disable all network connectivity. Otherwise, new policies may be acquired that re-enable encryption.
- Follow your existing process for decrypting data, such as issuing a policy update.
- Encryption and Encryption External Media update the Dell Server to change the status to Unprotected at the beginning of a client uninstall process. However, in the event that the client cannot contact the Dell Server, regardless of the reason, the status cannot be updated. In this case, you will need to manually Remove Endpoint in the Management Console. If your organization uses this workflow for compliance purposes, Dell recommends that you verify that Unprotected has been set as expected, either in the Management Console or Managed Reports.

**Process**

- The Key Server (and Security Management Server) must be configured prior to uninstallation if using the Encryption Removal Agent's Download Keys from Server option. See Configure Key Server for Uninstallation of Encryption Client Activated Against Security Management Server for instructions. No prior action is needed if the client to uninstall is activated against a Security Management Server Virtual, as Security Management Server Virtual does not use the Key Server.
- You must use the Dell Administrative Utility (CMGAd) prior launching the Encryption Removal Agent if using the Encryption Removal Agent's Import Keys from a file option. This utility is used to obtain the encryption key bundle. See Use the Administrative Download Utility (CMGAd) for instructions. The utility can be located in the Dell installation media.

**Command Line Uninstallation**

- Once extracted from the Endpoint Security Suite Enterprise master installer, the Encryption installer can be located at C:\extracted\Encryption\DDPE_XXbit_setup.exe.
- The following table details the parameters available for the uninstallation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMG_DECRYPT</td>
<td>Property for selecting the type of Encryption Removal Agent installation:</td>
</tr>
<tr>
<td></td>
<td>3 - Use LSARecovery bundle</td>
</tr>
<tr>
<td></td>
<td>2 - Use previously downloaded forensics key material</td>
</tr>
<tr>
<td></td>
<td>1 - Download keys from the Dell Server</td>
</tr>
<tr>
<td></td>
<td>0 - Do not install Encryption Removal Agent</td>
</tr>
<tr>
<td>CMGSILENTMODE</td>
<td>Property for silent uninstallation:</td>
</tr>
</tbody>
</table>
### Required Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA_SERVER</td>
<td>FQHN for the Security Management Server hosting the negotiate session.</td>
</tr>
<tr>
<td>DA_PORT</td>
<td>Port on the Security Management Server for request (default is 8050).</td>
</tr>
<tr>
<td>SVCPN</td>
<td>User name in UPN format that the Key Server service is logged on as on the Security Management Server.</td>
</tr>
<tr>
<td>DA_RUNAS</td>
<td>User name in SAM compatible format under whose context the key fetch request is made. This user must be in the Key Server list in the Security Management Server.</td>
</tr>
<tr>
<td>DA_RUNASPWD</td>
<td>Password for the runas user.</td>
</tr>
<tr>
<td>FORENSIC_ADMIN</td>
<td>The forensic administrator account on the Dell Server, which can be used for forensic requests for uninstalls or keys.</td>
</tr>
<tr>
<td>FORENSIC_ADMIN_PWD</td>
<td>The password for the forensic administrator account.</td>
</tr>
</tbody>
</table>

### Optional Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVCLOGONUN</td>
<td>User name in UPN format for Encryption Removal Agent service log on as parameter.</td>
</tr>
<tr>
<td>SVCLOGONPWD</td>
<td>Password for log on as user.</td>
</tr>
</tbody>
</table>

The following example silently uninstalls Encryption and downloads the encryption keys from the Security Management Server.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 DA_SERVER=server.organization.com DA_PORT=8050 SVCPN=administrator@organization.com DA_RUNAS=domain\username DA_RUNASPWD=password /qn"
```

MSI Command:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050" SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

Reboot the computer when finished.

The following example silently uninstalls Encryption and downloads the encryption keys using a forensic administrator account.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
```

MSI Command:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1 FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit REBOOT=REALLYSUPPRESS
```

Reboot the computer when finished.
IMPORTANT:
Dell recommends the following actions when using a forensic administrator password on the command line:

1. Create a forensic administrator account in the Management Console for the purpose of performing the silent uninstallation.
2. Use a temporary password for that account that is unique to that account and time period.
3. After the silent uninstallation has been completed, remove the temporary account from the list of administrators or change its password.

Some older clients may require escape characters of \\ around the values of parameters. For example:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050" SVCPN="administrator@organization.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn"
```

Uninstall Advanced Threat Prevention

Command Line Uninstallation

- The following example uninstalls the Advanced Threat Prevention client. This command must be run from an administrative command prompt.

```
wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
```

Shut down and restart the computer, then uninstall the Dell Encryption Management Agent component.

- IMPORTANT: If you installed the SED client or activated pre-boot authentication, follow the uninstallation instructions in Uninstall SED Client.

The following example uninstalls only the Dell Encryption Management Agent component and not the SED client.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

Uninstall SED Management

- Network connection to the Dell Server is required for PBA deactivation.

Process

- Deactivate the PBA, which removes all PBA data from the computer and unlocks the SED keys.
- Uninstall SED management.

Deactivate the PBA

1. As a Dell administrator, log in to the Management Console.
2. In the left pane, click Populations > Endpoints.
3. Select the appropriate Endpoint Type.
4. Select Show > Visible, Hidden, or All.
5. If you know the Hostname of the computer, enter it in the Hostname field (wildcards are supported). You may leave the field blank to display all computers. Click Search.

If you do not know the Hostname, scroll through the list to locate the computer.

A computer or list of computers displays based on your search filter.

6. Select the hostname of the desired computer.
7 Click **Security Policies** on the top menu.
8 Select **Self-Encrypting Drives** from the **Policy Category** page.
9 Change the **Self-Encrypting Drive (SED)** and policy from **On** to **Off**.
10 Click **Save**.
11 In the left pane, click the **Commit Policies** banner.
12 Click **Commit Policies**.

Wait for the policy to propagate from the Dell Server to the computer targeted for deactivation.

Uninstall SED management and PBA Advanced Authentication after the PBA is deactivated.

**Uninstall SED Client**

**Command Line Uninstallation**

- Once extracted from the master installer, the SED management installer can be located at `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - The following example silently uninstalls SED management.

  `EMAgent_XXbit_setup.exe /x /s /v" /qn"

  Shut down and restart the computer when finished.

**Uninstall BitLocker Manager**

**Command Line Uninstallation**

- Once extracted from the Endpoint Security Suite Enterprise master installer, the BitLocker Manager installer can be located at `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- The following example silently uninstalls BitLocker Manager.

  `EMAgent_XXbit_setup.exe /x /s /v" /qn"

  Reboot the computer when finished.
Data Security Uninstaller

Uninstall Endpoint Security Suite Enterprise

Dell provides the Data Security Uninstaller as a master uninstaller. This utility gathers the currently installed products and removes them in the appropriate order.

**NOTE:** When uninstalling FDE, Dell recommends restarting the computer after FDE deactivation is complete to prevent computer hibernation issues.

This Data Security Uninstaller is available in: C:\Program Files (x86)\Dell\Dell Data Protection

For more information or to use command line interface (CLI), see KB article SLN307791.

Logs are generated in C:\ProgramData\Dell\Dell Data Protection\ for all of the components that are removed.

To run the utility, open the containing folder, right-click DataSecurityUninstaller.exe, and select Run as administrator.

Click Next.
 Optionally clear any application from removal and click **Next**.

Required dependencies are automatically selected or cleared.
To remove applications without installing the Encryption Removal Agent, choose **Do not install Encryption Removal Agent** and select **Next**.

Select **Encryption Removal Agent - Download Keys from Server**.

Select **Encryption Removal Agent - Import Keys from a File**.

Select **Do not install Encryption Removal Agent**.
Enter the fully qualified credentials of a forensic administrator and select Next:

Device Server URL: example@dds.com
Forensics Administrator: forensicadmin@dds.com
Password: ********
Machine ID: 

Select Remove to begin the uninstall.

Click Finish to complete removal and reboot the computer. Reboot machine after clicking finished is selected by default.
Uninstallation and removal is complete.
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.
The guided set up begins once the licenses are imported. Click Next to begin.

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.
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**.
The master installer is not a master uninstaller. Each client must be uninstalled individually, followed by uninstallation of the master installer. Use this process to extract the clients from the master installer so that they can be used for uninstallation.

1. From the Dell installation media, copy the `DDSSuite.exe` file to the local computer.
2. Open a command prompt in the same location as the `DDSSuite.exe` file and enter:

   ```
   DDSSuite.exe /z""EXTRACT_INSTALLERS=C:\extracted\"
   ```

The extraction path cannot exceed 63 characters.

The extracted child installers are located at `C:\extracted\`. 

![Image of extracted folders with extracted files]
Configure Key Server

- This section explains how to configure components for use with Kerberos Authentication/Authorization when using an Security Management Server. The Security Management Server Virtual does not use the Key Server.
- If Kerberos Authentication/Authorization is to be used, then the server that contains the Key Server component needs to be part of the affected domain.
- Because the Security Management Server Virtual does not use the Key Server, typical uninstallation is affected. When an Encryption client that is activated against a Security Management Server Virtual is uninstalled, standard forensic key retrieval through the Security Server is used, instead of the Key Server's Kerberos method. See Command Line Uninstallation for more information.

Services Panel - Add Domain Account User

1. On the Security Management Server, navigate to the services panel (Start > Run > services.msc > OK).
2. Right-click Key Server and select Properties.

   
   ![Services Panel - Add Domain Account User]

3. Select the Log On tab and select the This account: option.

   In This account:, add the domain account user. This domain user must have at least local administrator rights to the Key Server folder (must be able to write to the Key Server config file, as well as the ability to write to the log.txt file).

   Enter and confirm the password for the domain user.

   Click OK.
4. Restart the Key Server service (leave the services panel open for further operation).
5. Navigate to `<Key Server install dir> log.txt` to verify that the service started properly.

**Key Server Config File - Add User for Security Management Server Communication**

1. Navigate to `<Key Server install dir>`.
2. Open `Credant.KeyServer.exe.config` with a text editor.
3. Go to `<add key="user" value="superadmin" />` and change the "superadmin" value to the name of the appropriate user (you may also leave as "superadmin").
4. Go to `<add key="epw" value="<encrypted value of the password>" />` and change "epw" to "password". Then change "<encrypted value of the password>" to the password of the user from Step 3. This password is re-encrypted when the Security Management Server restarts.

If using "superadmin" in Step 3, and the superadmin password is not "changeit", it must be changed here. Save and close the file.

**Services Panel - Restart Key Server Service**

1. Go back to the services panel (Start > Run > services.msc > OK).
2. Restart the Key Server service.
3. Navigate to `<Key Server install dir> log.txt` to verify that the service started properly.
4. Close the services panel.
Management Console - Add Forensic Administrator

1. As a Dell administrator, log in to the Management Console.
2. Click **Populations > Domains**.
3. Select the appropriate Domain.
4. Click the **Key Server** tab.
5. In Account, add the user to perform the administrator activities. The format is DOMAIN\Username. Click **Add Account**.
6. Click **Users** in the left menu. In the search box, search for the user name added in Step 5. Click **Search**.
7. Once the correct user is located, click the **Admin** tab.
8. Select **Forensic Administrator** and click **Update**.

The components are now configured for Kerberos Authentication/Authorization.
Use the Administrative Download Utility (CMGAd)

- This utility allows the download of a key material bundle for use on a computer that is not connected to a Dell Server.
- This utility uses one of the following methods to download a key material bundle, depending on the command line parameter passed to the application:
  - Forensic Mode - Used if -f is passed on the command line or if no command line parameter is used.
  - Admin Mode - Used if -a is passed on the command line.

Log files can be located at C:\ProgramData\CmgAdmin.log

Use Forensic Mode

1. Double-click cmgad.exe to launch the utility or open a command prompt where CMGAd is located and type cmgad.exe -f (or cmgad.exe).
2. Enter the following information (some fields may be pre-populated).
   - Device Server URL: Fully qualified Security Server (Device Server) URL. The format is https://securityserver.domain.com:8443/xapi/.
   - Dell Admin: Name of the administrator with forensic administrator credentials, such as jdoe (Enabled in the Management Console)
   - Password: Forensic administrator password
   - MCID: Machine ID, such as machineID.domain.com
   - DCID: First eight digits of the 16-digit Shield ID

   **TIP:**
   Specifying either the MCID or DCID is usually sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information used by this utility.

Click Next.
3 In **Passphrase**, enter a passphrase to protect the download file. The passphrase must be at least eight characters long, and contain at least one alphabetic and one numeric character. Confirm the passphrase. Either accept the default name and location of where the file will be saved or click ... to select another location. Click **Next**.

A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

4 Click **Finish** when complete.
Use Admin Mode

The Security Management Server Virtual does not use the Key Server, so Admin mode cannot be used to obtain a key bundle from a Security Management Server Virtual. Use Forensic mode to obtain the key bundle if the client is activated against a Security Management Server Virtual.

1. Open a command prompt where CMGAd is located and type `cmgad.exe -a`.
2. Enter the following information (some fields may be pre-populated).
   - **Server**: Fully qualified hostname of the Key Server, such as `keyserver.domain.com`
   - **Port Number**: The default port is 8050
   - **Server Account**: The domain user the Key Server is running as. The format is `DOMAIN\Username`. The domain user running the utility must be authorized to perform the download from the Key Server
   - **MCID**: Machine ID, such as `machineID.domain.com`
   - **DCID**: First eight digits of the 16-digit Shield ID

   **TIP:**
   Specifying either the MCID or DCID is usually sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information used by this utility.

   Click **Next**.

3. In **Passphrase:** type a passphrase to protect the download file. The passphrase must be at least eight characters long, and contain at least one alphabetic and one numeric character.
   - Confirm the passphrase.
   - Either accept the default name and location of where the file will be saved or click ... to select another location.

   Click **Next**.
A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

4 Click **Finish** when complete.
Troubleshooting

All Clients - Troubleshooting

- **Endpoint Security Suite Enterprise master Suite installer log files** are located at `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows creates unique **child installer installation log files** for the logged in user at `%temp%`, located at `C:\Users\<UserName>\AppData\Local\Temp`.
- Windows creates log files for client prerequisites, such as Visual C++, for the logged in user at `%temp%`, located at `C:\Users\<UserName>\AppData\Local\Temp`. For example, `C:\Users\<UserName>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log`.
- Follow the instructions at http://msdn.microsoft.com to verify the version of Microsoft .Net that is installed on the computer targeted for installation.
  
- See this document if the computer targeted for installation has (or has had in the past) Dell Access installed. Dell Access is not compatible with this suite of products.

All Clients - Protection Status

A new method for deriving a device's protected status has been implemented in the Dell Server v9.8.2. Previously, the Endpoint Protected Status area in the Management Console's dashboard would only denote the state of Encryption per device.

As of Dell Server v9.8.2, Protected status is now denoted if any of the following criteria have been met:

- Advanced Threat Prevention is installed and enabled.
- Web Protection or Client Firewall is installed and either Web Protection or Client Firewall's policy is enabled.
- Dell Data Guardian is installed and enabled.
- Self-Encrypting Drive Management is installed, enabled, and the PBA is enabled.
- BitLocker Manager is installed, enabled, and encryption has completed.
- Dell Encryption (Mac) is installed and enabled, and Encrypt Using FileVault for Mac has been enforced.
- Dell Encryption (Windows) is installed, enabled, Policy-Based Encryption has been set for the endpoint, and device sweeps are completed.

Dell Encryption Troubleshooting (client and server)

Activation on a Server Operating System

When Encryption is installed on a server operating system, activation requires two phases of activation: initial activation and device activation.

Troubleshooting Initial Activation

Initial activation fails when:

- A valid UPN cannot be constructed using the supplied credentials.
- The credentials are not found in the enterprise vault.
The credentials used to activate are not domain administrator's credentials.

**Error Message: Unknown user name or bad password**

The user name or password does not match.

Possible Solution: Try to log in again, ensuring that you type the user name and password exactly.

**Error Message: Activation failed because the user account does not have domain administrator rights.**

The credentials used to activate do not have domain administrator rights, or the administrator's user name was not in UPN format.

Possible Solution: In the Activation dialog, enter credentials in UPN format for a domain administrator.

**Error Messages: A connection with the server could not be established.**

or

The operation timed out.

Server Encryption could not communicate with port 8449 over HTTPS to the Dell Server.

**Possible Solutions**

- Connect directly to your network and try to activate again.
- If connected by VPN, try connecting directly to the network and try again to activate.
- Check the Dell Server URL to ensure it matches the URL supplied by the administrator. The URL and other data that the user entered into the installer are stored in the registry. Check the accuracy of the data under [HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon\CMGShield] and [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Disconnect the server from the network. Restart the server and reconnect to the network.

**Error Message: Activation failed because the Server is unable to support this request.**

**Possible Solutions**

- Server Encryption cannot be activated against a legacy server; the Dell Server version must be version 9.1 or higher. If necessary, upgrade your Dell Server to version 9.1 or higher.
- Check the Dell Server URL to ensure it matches the URL supplied by the administrator. The URL and other data that the user entered into the installer are stored in the registry.
- Check the accuracy of the data under [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] and [HKLM \Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

**Initial Activation Process**

The following diagram illustrates a successful initial activation.

The initial activation process of Encryption of server operating systems requires a live user to access the server. The user can be of any type: domain or non-domain, remote-desktop-connected or interactive user, but the user must have access to domain administrator credentials.
The Activation dialog displays when one of two workflows occur:

- A new (unmanaged) user logs on to the computer.
- When a new user right-clicks the Encryption icon in the notification area and selects Activate Dell Encryption.

The initial activation process is as follows:

1. The user logs in.
2. Upon detection of a new (unmanaged) user, the Activate dialog displays. The user clicks Cancel.
3. The user opens the Server Encryption About box to confirm that it is running in Server mode.
4. The user right-clicks the Encryption icon in the notification area and selects Activate Dell Encryption.
5. The user enters domain administrator credentials in the Activate dialog.

### NOTE:
The requirement for domain administrator credentials is a safety measure that prevents Encryption of server operating systems from being rolled out to unsupported server environments. To disable the requirement for domain administrator credentials, see Before You Begin.

6. Dell Server checks for the credentials in the enterprise vault (Active Directory or equivalent) to verify that the credentials are domain administrator credentials.
7. A UPN is constructed using the credentials.
8. With the UPN, the Dell Server creates a new user account for the virtual server user, and stores the credentials in the Dell Server's vault.

The **virtual server user account** is for the exclusive use of the Encryption client. It is used to authenticate with the server, to handle Common encryption keys, and to receive policy updates.

### NOTE:
Password and DPAPI authentication are disabled for this account so that only the virtual server user can access encryption keys on the computer. This account does not correspond to any other user account on the computer or on the domain.

9. When activation is successful, the user restarts the computer, which kicks off the second phase, authentication and device activation.

**Troubleshooting Authentication and Device Activation**

Device activation fails when:

- The initial activation failed.
- The connection to the server could not be established.
- The trust certificate could not be validated.

After activation, when the computer is restarted, Encryption for server operating systems automatically logs in as the virtual server user, requesting the Machine key from the Dell Server. This takes place even before any user can log in.

- Open the About dialog to confirm that Encryption for server operating systems is authenticated and in Server mode.
• If the Encryption client ID is red, encryption has not yet been activated.
• In the Management Console, the version of a server with Server Encryption installed is listed as Shield for Server.
• If the Machine key retrieval fails due to a network failure, Server Encryption registers for network notifications with the operating system.
• If the Machine key retrieval fails:
  – The virtual server user logon is still successful.
  – Set up the Retry Interval Upon network Failure policy to make key retrieval attempts on a timed interval.

For details on the Retry Interval Upon network Failure policy, refer to AdminHelp, available in the Management Console.

Authentication and Device Activation

The following diagram illustrates successful authentication and device activation.

1 When restarted after a successful initial activation, a computer with Server Encryption automatically authenticates using the virtual server user account and runs the Encryption client in Server mode.
2 The computer checks its device activation status with the Dell Server:
   • If the computer has not previously device-activated, the Dell Server assigns the computer an MCID, a DCID, and a trust certificate, and stores all of the information in the Dell Server’s vault.
   • If the computer had previously been device-activated, the Dell Server verifies the trust certificate.
3 After the Dell Server assigns the trust certificate to the server, the server can access its encryption keys.
4 Device activation is successful.

**NOTE:** When running in Server mode, the Encryption client must have access to the same certificate as was used for device activation to access the encryption keys.

Encryption External Media and PCS Interactions

To Ensure Media is Not Read-Only and the Port is Not Blocked

The EMS Access to unShielded Media policy interacts with the Port Control System - Class: Storage > Subclass Storage: External Drive Control policy. If you intend to set the EMS Access to unShielded Media policy to Full Access, ensure that the Subclass Storage: External Drive Control policy is also set to Full Access to ensure that the media is not set to read-only and the port is not blocked.

To Encrypt Data Written to CD/DVD
• Set Windows Media Encryption = On.
• Set EMS Exclude CD/DVD Encryption = not selected.
• Set Subclass Storage: Optical Drive Control = UDF Only.

Use WSScan

• WSScan allows you to ensure that all data is decrypted when uninstalling Encryption as well as view encryption status and identify unencrypted files that should be encrypted.
• Administrator privileges are required to run this utility.

**NOTE:** WSScan must be run in System Mode with the PsExec tool if a target file is owned by the system account.

Run WSScan

1. From the Dell installation media, copy WSScan.exe to the Windows computer to scan.
2. Launch a command line at the location above and enter `wsscan.exe` at the command prompt. WSScan launches.
3. Click Advanced.
4. Select the type of drive to scan: All Drives, Fixed Drives, Removable Drives, or CDROMs/DVDROMs.
5. Select the Encryption Report Type: Encrypted Files, Unencrypted Files, All Files, or Unencrypted Files in Violation:
   - **Encrypted Files** - To ensure that all data is decrypted when uninstalling Encryption. Follow your existing process for decrypting data, such as issuing a decryption policy update. After decrypting data, but before performing a restart in preparation for uninstall, run WSScan to ensure that all data is decrypted.
   - **Unencrypted Files** - To identify files that are not encrypted, with an indication of whether the files should be encrypted (Y/N).
   - **All Files** - To list all encrypted and unencrypted files, with an indication of whether the files should be encrypted (Y/N).
   - **Unencrypted Files in Violation** - To identify files that are not encrypted that should be encrypted.
6. Click Search.
Click **Advanced** to toggle the view to **Simple** to scan a particular folder.

Go to Scan Settings and enter the folder path in the **Search Path** field. If this field is used, the selection in the menu is ignored.

If you do not want to write WSScan output to a file, clear the **Output to File** check box.

Change the default path and file name in Path, if desired.

Select **Add to Existing File** if you do not want to overwrite any existing WSScan output files.

Choose the output format:

- Select Report Format for a report style list of scanned output. This is the default format.
- Select Value Delimited File for output that can be imported into a spreadsheet application. The default delimiter is ",", although it can be changed to up to 9 alphanumeric, space, or keyboard punctuation characters.
- Select the Quoted Values option to enclose each value in double quotation marks.
- Select Fixed Width File for non-delimited output containing a continuous line of fixed-length information about each encrypted file.

Click **Search**.

Click **Stop Searching** to stop your search. Click **Clear** to clear displayed messages.
WSScan Output

WSScan information about encrypted files contains the following information.

Example Output:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted

<table>
<thead>
<tr>
<th>Output</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/time stamp</td>
<td>The date and time the file was scanned.</td>
</tr>
<tr>
<td>Encryption type</td>
<td>The type of encryption used to encrypt the file.</td>
</tr>
<tr>
<td><strong>SysData</strong>: SDE key.</td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>User:</strong></td>
<td>User encryption key.</td>
</tr>
<tr>
<td><strong>Common:</strong></td>
<td>Common encryption key.</td>
</tr>
<tr>
<td>WSScan does not report files encrypted using Encrypt for Sharing.</td>
<td></td>
</tr>
<tr>
<td><strong>KCID</strong></td>
<td>The Key Computer ID.</td>
</tr>
<tr>
<td>As shown in the example above, &quot;7vdxrsb&quot;</td>
<td></td>
</tr>
<tr>
<td>If you are scanning a mapped network drive, the scanning report does not return a KCID.</td>
<td></td>
</tr>
<tr>
<td><strong>UCID</strong></td>
<td>The User ID.</td>
</tr>
<tr>
<td>As shown in the example above, &quot;<em>SDENCR</em>&quot;</td>
<td></td>
</tr>
<tr>
<td>The UCID is shared by all the users of that computer.</td>
<td></td>
</tr>
<tr>
<td><strong>File</strong></td>
<td>The path of the encrypted file.</td>
</tr>
<tr>
<td>As shown in the example above, &quot;c:\temp\Dell - test.log&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Algorithm</strong></td>
<td>The encryption algorithm being used to encrypt the file.</td>
</tr>
<tr>
<td>As shown in the example above, &quot;is still AES256 encrypted&quot;</td>
<td></td>
</tr>
<tr>
<td>RIJNDAEL 128</td>
<td></td>
</tr>
<tr>
<td>RIJNDAEL 256</td>
<td></td>
</tr>
<tr>
<td>AES-128</td>
<td></td>
</tr>
<tr>
<td>AES-256</td>
<td></td>
</tr>
<tr>
<td>3DES</td>
<td></td>
</tr>
</tbody>
</table>

**Check Encryption Removal Agent Status**

The Encryption Removal Agent displays its status in the description area of the services panel (Start > Run > services.msc > OK) as follows. Periodically refresh the service (highlight the service > right-click > Refresh) to update its status.

- **Waiting for SDE Deactivation** - Encryption is still installed, is still configured, or both. Decryption does not start until Encryption is uninstalled.
- **Initial sweep** - The service is making an initial sweep, calculating the number of encrypted files and bytes. The initial sweep occurs one time.
- **Decryption sweep** - The service is decrypting files and possibly requesting to decrypt locked files.
- **Decrypt on Reboot (partial)** - The decryption sweep is complete and some locked files (but not all) are to be decrypted on the next restart.
- **Decrypt on Reboot** - The decryption sweep is complete and all locked files are to be decrypted on the next restart.
- **All files could not be decrypted** - The decryption sweep is complete, but all files could not be decrypted. This status means one of the following occurred:
  - The locked files could not be scheduled for decryption because they were too big, or an error occurred while making the request to unlock them.
  - An input/output error occurred while decrypting files.
  - The files could not be decrypted by policy.
  - The files are marked as should be encrypted.
An error occurred during the decryption sweep.

In all cases, a log file is created (if logging is configured) when LogVerbosity=2 (or higher) is set. To troubleshoot, set the log verbosity to 2 and restart the Encryption Removal Agent service to force another decryption sweep.

- **Complete** - The decryption sweep is complete. The service, the executable, the driver, and the driver executable are all scheduled for deletion on the next restart.

---

### Advanced Threat Prevention Troubleshooting

#### Find the Product Code with Windows PowerShell

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

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

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

---

### Advanced Threat Prevention Provisioning and Agent Communication

The following diagrams illustrate the Advanced Threat Prevention service provisioning process.
The following diagram illustrates the Advanced Threat Prevention agent communication process.
BIOS Image Integrity Verification Process

The following diagram illustrates the BIOS image integrity verification process. For a list of Dell computer models supported with BIOS image integrity verification, see Requirements - BIOS Image Integrity Verification.
Dell ControlVault Drivers

Update Dell ControlVault Drivers and Firmware

- Dell ControlVault drivers and firmware that are installed on Dell computers at the factory are outdated and should be updated by following this procedure, in this order.
- If an error message is received during client installation prompting you to exit the installer to update Dell ControlVault drivers, the message may be safely dismissed to continue with the installation of the client. The Dell ControlVault drivers (and firmware) can be updated after the client installation is complete.

Download Latest Drivers

1. Go to support.dell.com.

2. Select your computer model.
3 Select Drivers & Downloads.
4. Select the **Operating System** of the target computer.

5. Expand the **Security** category.
6 Download and save the Dell ControlVault Drivers.

7 Download and save the Dell ControlVault Firmware.
8 Copy the drivers and firmware to the target computers, if needed.

**Install Dell ControlVault Driver**

1 Navigate to the folder which you downloaded the driver installation file.

2 Double-click the Dell ControlVault driver to launch the self-extracting executable file.

<table>
<thead>
<tr>
<th>TIP:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be sure to install the driver first. The file name of the driver at the time of this document creation is ControlVault_Setup_2MYJC_A37_ZPE.exe.</td>
</tr>
</tbody>
</table>

3 Click **Continue** to begin.
4 Click **Ok** to unzip the driver files in the default location of `C:\Dell\Drivers\New Folder`.

5 Click **Yes** to allow the creation of a new folder.

6 Click **Ok** when the successfully unzipped message displays.

7 The folder which contains the files should display after extraction. If not, navigate to the folder to which you extracted the files. In this case, the folder is **JW22F**.
8 Double-click **CVHCI64.MSI** to launch the driver installer. [this example is **CVHCI64.MSI** in this example (CVHCI for a 32-bit computer)].

9 Click **Next** at the Welcome screen.

10 Click **Next** to install the drivers in the default location of **C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\**.
11 Select the **Complete** option and click **Next**.

12 Click **Install** to begin the installation of the drivers.
13 Optionally check the box to display the installer log file. Click **Finish** to exit the wizard.

**Verify Driver Installation**

- The Device Manager will have a Dell ControlVault device (and other devices) depending on the operating system and hardware configuration.

**Install Dell ControlVault Firmware**
1. Navigate to the folder which you downloaded the firmware installation file.

2. Double-click the Dell ControlVault firmware to launch the self-extracting executable file.

3. Click **Continue** to begin.

4. Click **Ok** to unzip the driver files in the default location of `C:\Dell\Drivers\<New Folder>`.

5. Click **Yes** to allow the creation of a new folder.
6 Click **Ok** when the successfully unzipped message displays.

![Image of successfully unzipped message]

7 The folder which contains the files should display after extraction. If not, navigate to the folder to which you extracted the files. Select the **firmware** folder.

![Image of firmware folder]

8 Double-click **ushupgrade.exe** to launch the firmware installer.

9 Click **Start** to begin the firmware upgrade.
**IMPORTANT:**

You may be asked to enter the administrator password if upgrading from an older version of firmware. Enter **Broadcom** as the password and click **Enter** if presented with this dialog.

Several status messages display.
This program will update the ControlVault firmware from 30.7.27.0 to 30.7.27.0.

Once started, do not interrupt process.

Going to stop Host Services.
   Credential Vault Host Control Service ... stopped.
   Credential Vault Host Storage ... stopped.

Going to stop Host and DCP tasks.

Checking current ControlVault status.
Found ControlVault Chip Type: 5882 B0 CustID 7
Going to update the SBI.
Going to clear SCD.
Going to reset ControlVault.
Waiting for ControlVault to come up (~5 seconds)

Going to update the BCM (~40 seconds)
10 Click **Restart** to complete the firmware upgrade.

The update of the Dell ControlVault drivers and firmware is complete.
Advanced Threat Prevention - The Advanced Threat Prevention product is next-generation antivirus protection that uses algorithmic science and machine learning to identify, classify, and prevent both known and unknown cyberthreats from executing or harming endpoints. The optional Client Firewall feature monitors communication between the computer and resources on the network and the Internet and intercepts potentially malicious communications. The optional Web Protection feature blocks unsafe websites and downloads from those websites during online browsing and searching, based on safety ratings and reports for websites.

BitLocker Manager - Windows BitLocker is designed to help protect Windows computers by encrypting both data and operating system files. To improve the security of BitLocker deployments and to simplify and reduce the cost of ownership, Dell provides a single, central management console that addresses many security concerns and offers an integrated approach to managing encryption across other non-BitLocker platforms, whether physical, virtual, or cloud-based. BitLocker Manager supports BitLocker encryption for operating systems, fixed drives, and BitLocker To Go. BitLocker Manager enables you to seamlessly integrate BitLocker into your existing encryption needs and to manage BitLocker with the minimum effort while streamlining security and compliance. BitLocker Manager provides integrated management for key recovery, policy management and enforcement, automated TPM management, FIPS compliance, and compliance reporting.

Deactivate - Deactivation occurs when SED management is turned OFF in the Management Console. Once the computer is deactivated, the PBA database is deleted and there is no longer any record of cached users.

Encryption External Media - This service within Encryption protects removable media and external storage devices.

Encryption External Media Access Code - This service allows for recovery of Encryption External Media protected devices where the user forgets their password and can no longer login. Completing this process allows the user to reset the password set on the media.

Encryption - On-device component that enforces security policies, whether an endpoint is connected to the network, disconnected from the network, lost, or stolen. Creating a trusted computing environment for endpoints, Encryption operates as a layer on top of the device operating system, and provides consistently-enforced authentication, encryption, and authorization to maximize the protection of sensitive information.

Endpoint - Depending on context, a computer, mobile device, or external media...

Encryption sweep - The process of scanning folders to be encrypted to ensure the contained files are in the proper encryption state. Ordinary file creation and rename operations do not trigger an encryption sweep. It is important to understand when an encryption sweep may happen and what may affect the resulting sweep times, as follows: - An encryption sweep occurs upon initial receipt of a policy that has encryption enabled. This can occur immediately after activation if your policy has encryption enabled. - If the Scan Workstation on Logon policy is enabled, folders specified for encryption are swept on each user logon. - A sweep can be re-triggered under certain subsequent policy changes. Any policy change related to the definition of the encryption folders, encryption algorithms, encryption key usage (common verses user), triggers a sweep. In addition, toggling between encryption enabled and disabled triggers an encryption sweep.

SED management - SED management provides a platform for securely managing self-encrypting drives. Although SEDs provide their own encryption, they lack a platform to manage their encryption and available policies. SED management is a central, scalable management component, which allows you to more effectively protect and manage your data. SED management ensures that you can administer your enterprise more quickly and easily.

Server user – A virtual user account created by Encryption for the purpose of handling encryption keys and policy updates on a server operating system. This user account does not correspond to any other user account on the computer or within the domain, and it has no user name and password that can be used physically. The account is assigned a unique UCID value in the Management Console.