Dell Data Security

Endpoint Security Suite Pro Basic Installation Guide v1.8

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.

Endpoint Security Suite Pro Basic Installation Guide

2017 - 08

Rev. A01

Contents

1

Introduction

This guide details how to install and configure the application using the Endpoint Security Suite Pro 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 Pro master installer.

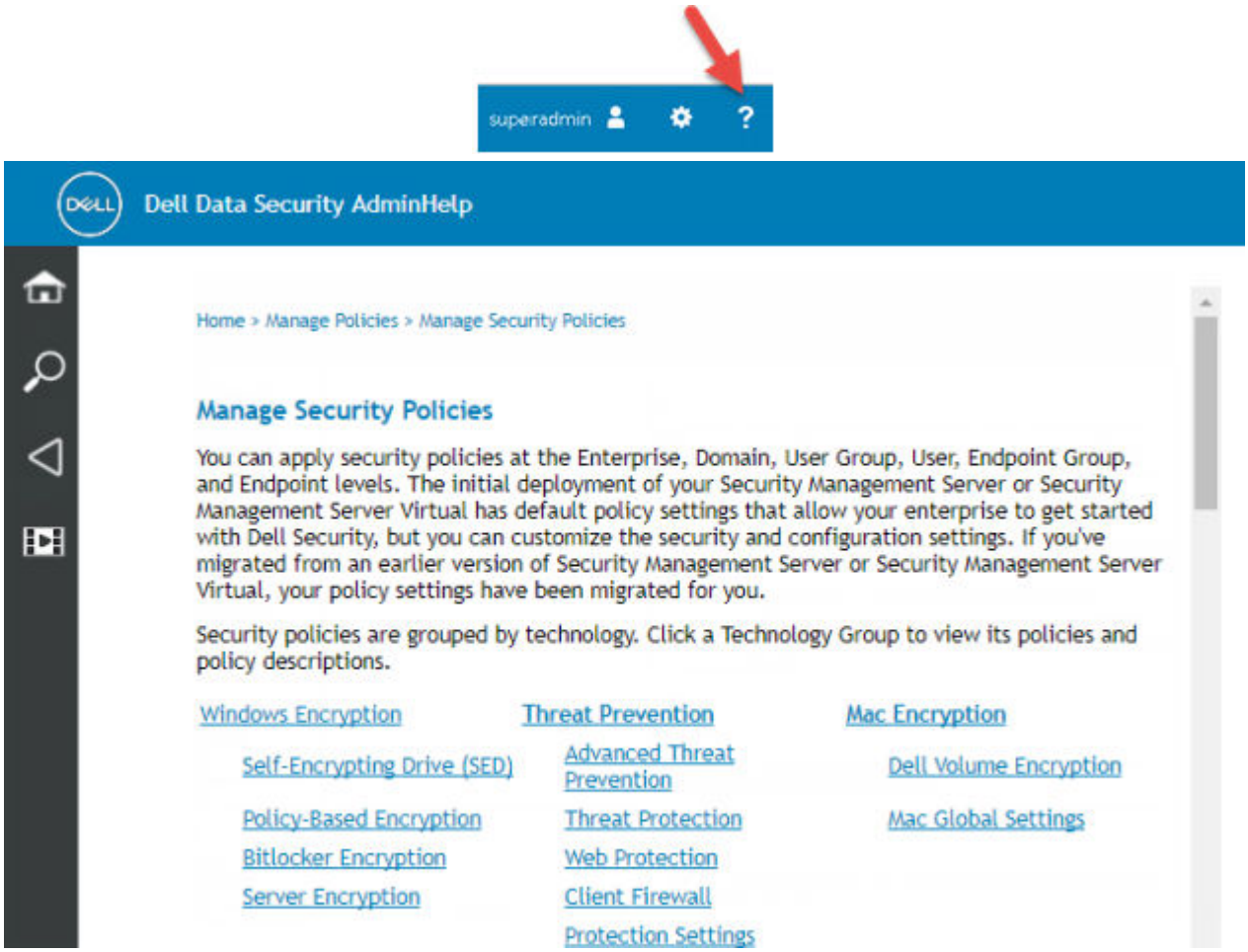
All policy information, and their descriptions are found in the AdminHelp.

Before You Begin

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

- *Dell Security Management Server Installation and Migration Guide*
- *Dell 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 far right of the screen. The AdminHelp is page-level help designed to help you set and modify policy and understand your options with your Security Management Server/Security Management Server Virtual.



2 Thoroughly read the Requirements chapter of this document.

3 Deploy clients to end 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

    or
  - 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 Code available when you call.

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

2

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 SMS or Dell KACE. 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.
- Ensure that outbound port 443 is available to communicate with the Security Management Server/Security Management Server Virtual if your master installer clients will be entitled using Dell Digital Delivery (DDD). The entitlement functionality will not work if port 443 is blocked (for any reason). DDD is not used if installing using the child installers.
- Be sure to periodically check www.dell.com/support for the most current documentation and Technical Advisories.

All Clients - Prerequisites

- Microsoft .Net Framework 4.5.2 (or later) is required for the Endpoint Security Suite Pro master installer and child installer clients. The installer *does not* install the Microsoft .Net Framework component.

  All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5.2 (or later). However, if you are not installing on Dell hardware or are upgrading the client on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version **prior to installing the client** to prevent installation/upgrade failures. To verify the version of Microsoft .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. To install Microsoft .Net Framework 4.5.2, go to https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Drivers and firmware for ControlVault, fingerprint readers and smart cards (as shown below) are not included in the Endpoint Security Suite Pro master installer or child installer executable files. The drivers and firmware must be kept up-to-date, and can be downloaded from http://www.dell.com/support and selecting your computer model. Download the appropriate drivers and firmware based on your authentication hardware.
  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

All Clients - Hardware

- The following table details supported computer hardware.

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

All Clients - Localization

- The Encryption, Threat Protection, and BitLocker Manager clients are Multilingual User Interface (MUI) compliant and are localized in the following languages.

Language Support

- EN - English
- ES - Spanish
- FR - French
- IT - Italian
- DE - German
- JA - Japanese
- KO - Korean
- PT-BR - Portuguese, Brazilian
- PT-PT - Portuguese, Portugal (Iberian)

Encryption Client

- 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).
- The Encryption client 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.
- The Encryption client has been tested and is compatible with McAfee, the Symantec client, Kaspersky, and MalwareBytes. Hard-coded exclusions are in place in for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. The Encryption client has also been tested with the Microsoft Enhanced Mitigation Experience Toolkit.

  If your organization uses an anti-virus provider that is not listed, see http://www.dell.com/support/article/us/en/19/SLN288353/ or Contact Dell ProSupport for help.
- 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.

Encryption Client Prerequisites

- The master installer installs the following prerequisites if not already installed on the 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)

Encryption Client Operating Systems

- The following table details supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template (hardware encryption is not supported)
- Windows 8: Enterprise, Pro

Windows Operating Systems (32- and 64-bit)

- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (hardware encryption is not supported)
- Windows 10: Education, Enterprise, Pro through Creators Update (Redstone 2)
- VMware Workstation 5.5 and higher

> **NOTE:**
> When using UEFI mode, the Secure Hibernation policy is not supported.

Encryption Client Operating Systems with Deferred Activation

- 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 http://www.dell.com/support/article/us/en/19/sln306341.
- The following table details supported operating systems with deferred activation.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Home Basic, Home Premium, Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template (hardware encryption is not supported)
- Windows 8: Home Basic, Home Premium, Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (hardware encryption is not supported)
- Windows 10: Home Basic, Home Premium, Education, Enterprise, Pro through Creators Update (Redstone 2)
- VMware Workstation 5.5 and higher

Encryption External Media Operating Systems

- The following table details the operating systems supported when accessing media protected by Encryption External Media.

> **NOTE:**
> 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.

> **NOTE:**
> Windows XP is supported when using Encryption External Media Explorer only.

Windows Operating Systems Supported to Access Encryption External Media-Protected Media (32- and 64-bit)

- Windows 7 SP0-SP1: Home Basic, Home Premium, Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template (hardware encryption is not supported)
- Windows 8: Home Basic, Home Premium, Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (hardware encryption is not supported)
- Windows 10: Home Basic, Home Premium, Education, Enterprise, Pro through Creators Update (Redstone 2)

Mac Operating Systems Supported to Access Encryption External Media-Protected Media (64-bit kernels)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.5 and 10.12.6

Threat Protection Client

- The Threat Protection clients cannot be installed without the Encryption client being detected on the computer. Installation will fail if attempted.
- To successfully install Threat Protection, the computer must have network connectivity.
- Uninstall other vendors' anti-virus, anti-malware, anti-spyware, and firewall applications before installing the Threat Protection clients to prevent installation failures. Conflicting software does not include Windows Defender and Endpoint Security Suite Pro.
- The Web Protection feature is supported with Internet Explorer only.

Threat Protection Client Operating Systems

- The following table details supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro through Creators Update (Redstone 1)

Threat Protection Client Ports

- To ensure that Threat Protection clients receive the most current Threat 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.

Use	Application Protocol	Transport Protocol	Port Number	Destination	Direction	Notes
Anti-virus Updates	HTTP	TCP	443/fallback 80	vs.mcafeeasap.com	Outbound	
Anti-virus Engine/ Signature Updates	SSL	TCP	443	vs.mcafeeasap.com	Outbound	
Anti-Spam Engine	HTTP	TCP	443	vs.mcafeeasap.com	Outbound	
Anti-Spam Rules and Streaming Updates	HTTP	TCP	80	vs.mcafeeasap.com	Outbound	Packet types: X-SU3X-SU3-Component-Name X-SU3-Component-Type X-SU3-Status
Reputation Service	SSL	TCP	443	tunnel.web.trustedsource.org	Outbound	

Use	Application Protocol	Transport Protocol	Port Number	Destination	Direction	Notes
Reputation Service Feedback	SSL	TCP	443	gtifeedback.trustedsource.org	Outbound	
Quarantine Manager	HTTP HTTPS	TCP	80 443	Your Security Management Server/Security Management Server Virtual	Bi-directional	
URL Reputation Database Update	HTTP	TCP	80	list.smartfilter.com	Outbound	
URL Reputation Lookup	SSL	TCP	443	tunnel.web.trustedsource.org	Outbound	

SED Client

- The computer must have a wired network connection to successfully install SED management.
- IPv6 is not supported.
- 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. Preboot 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 blue screen when switched from *RAID=On* to *AHCI*.
- Configuration of self-encrypting drives for Dell's SED management differ between NVMe and non-NVMe (SATA) drives, as follows.
  - Any NVMe drive that is being leveraged as an SED – The BIOS' SATA operation must be set to RAID ON, as Dell's SED management does not support AHCI on NVMe drives.
  - Any NVMe drive that is being leveraged as an SED – The BIOS's boot mode must be UEFI and Legacy option ROMs must be disabled.
  - Any non-NVMe drive that is being leveraged as an SED – The BIOS' SATA operation must be set to AHCI, as Dell's 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 http://www.dell.com/support/article/us/en/19/SLN306460.

  Supported OPAL compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite/drivers. Dell recommends Intel Rapid Storage Technology Driver version 15.2.0.0 or later, with NVMe drives.

- SED Management is not supported with Server Encryption.

SED Client Prerequisites

- The Endpoint Security Suite Pro master installer installs the following prerequisites if not already installed on the computer.

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

SED Client Hardware

SED Client International Keyboards

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

International Keyboard Support - UEFI
• DE-CH - Swiss German • DE-FR - Swiss French

International Keyboard Support - Non-UEFI
• AR - Arabic (using Latin letters) • DE-CH - Swiss German • DE-FR - Swiss French

SED Client Localization

The SED and Advanced Authentication clients are Multilingual User Interface (MUI) compliant and are localized the following languages. UEFI Mode and Preboot Authentication are supported in the following languages **except** Russian, Traditional Chinese, or Simplified Chinese.

Language Support	
• EN - English	• KO - Korean
• FR - French	• ZH-CN - Chinese, Simplified
• IT - Italian	• ZH-TW - Chinese, Traditional/Taiwan
• DE - German	• PT-BR - Portuguese, Brazilian
• ES - Spanish	• PT-PT - Portuguese, Portugal (Iberian)

Language Support

- JA - Japanese
- RU - Russian

SED Client Operating Systems

- The following table details the supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional (supported with Legacy Boot mode but not UEFI)

  NOTE:
  Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.

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

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro through Creators Update (Redstone 2)

Advanced Authentication Client

- When using Advanced Authentication, users will be securing access to the computer using advanced authentication credentials that are managed and enrolled using Advanced Authentication. Advanced Authentication will be the primary manager of the authentication credentials for Windows Sign-in, including Windows password, fingerprint, and smart cards. Picture password, PIN, and fingerprint credentials enrolled using the Microsoft Operating System will not be recognized at Windows Sign-in.

  To continue using the Microsoft Operating System to manage user credentials, do not install Advanced Authentication or uninstall it.

Advanced Authentication Client Hardware

- The following table details supported authentication hardware.

Fingerprint and Smart Card Readers

- Validity VFS495 in Secure Mode
- ControlVault Swipe Reader
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Authentec Eikon and Eikon To Go USB Readers

Contactless Cards

- Contactless Cards using Contactless Card Readers built-in to specified Dell laptops

Smart Cards

- PKCS #11 Smart Cards using the ActivIdentity client

  NOTE:
  The ActivIdentity client is not pre-loaded and must be installed separately.

- CSP Cards

Smart Cards

- Common Access Cards (CACs)
- Class B/SIPR Net Cards

Advanced Authentication Client Operating Systems

Windows Operating Systems

- The following table details supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro through Creators Update (Redstone 2)

ⓘ | **NOTE: UEFI mode is not supported on Windows 7.**

BitLocker Manager Client

- 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.
- 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 will take ownership of the TPM and will not require a reboot. However, if a TPM ownership already exists, BitLocker Manager will begin the encryption setup process (no restart is required). The point is that the TPM must be "owned" and enabled.

BitLocker Manager Client Prerequisites

- The Endpoint Security Suite Pro master installer installs the following prerequisites if not already installed on the computer.

Prerequisites

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

BitLocker Manager Client Operating Systems

- The following table details supported operating systems.

Windows Operating Systems

- Windows 7 SP0-SP1: Enterprise, Ultimate (32- and 64-bit)
- Windows 8: Enterprise (64-bit)
- Windows 8.1: Enterprise Edition, Pro Edition (64-bit)
- Windows 10: Education, Enterprise, Pro through Creators Update (Redstone 2)
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-bit)
- Windows Server 2012

Windows Operating Systems

- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64-bit)
- Windows Server 2016

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 Pro master installer log files are located at **C:\ProgramData\Dell\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 feature of the Encryption client. 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 Pro Help* to learn how to use the features of Advanced Authentication and Threat Protection. 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 system tray 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

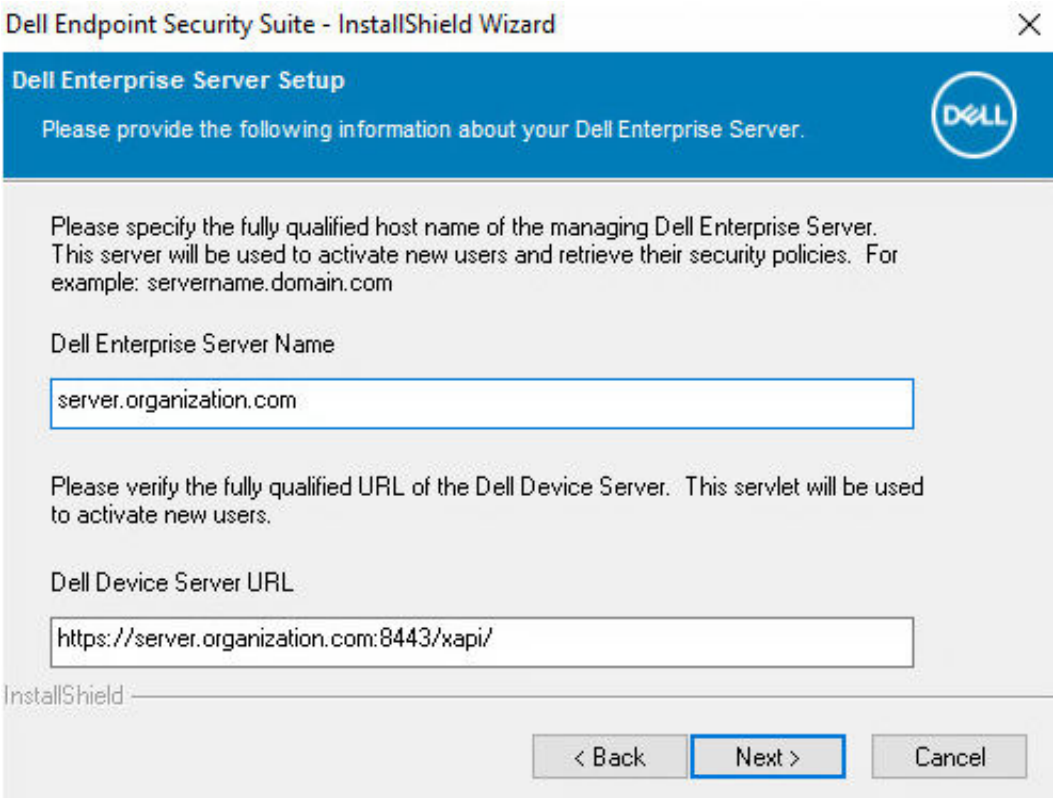
- The Endpoint Security Suite Pro master installer can be located at:
  - **From Your Dell FTP Account** - Locate the installation bundle at Endpoint-Security-Suite-Pro_Ent-1.x.x.xxx.zip
- Use these instructions to install Endpoint Security Suite Pro interactively using the Endpoint Security Suite Pro 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 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 the **Enterprise Server Name** field, enter the fully qualified host name of the Security Management Server/Security Management Server Virtual that will manage the target user, such as server.organization.com.

   In the **Device Server URL** field, enter the URL of the Device Server (Security 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 and Advanced Authentication, the advanced authentication client that manages multiple authentication methods, including PBA and credentials such as fingerprints and passwords.

Advanced Authentication installs the files and services required for Advanced Authentication.

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.

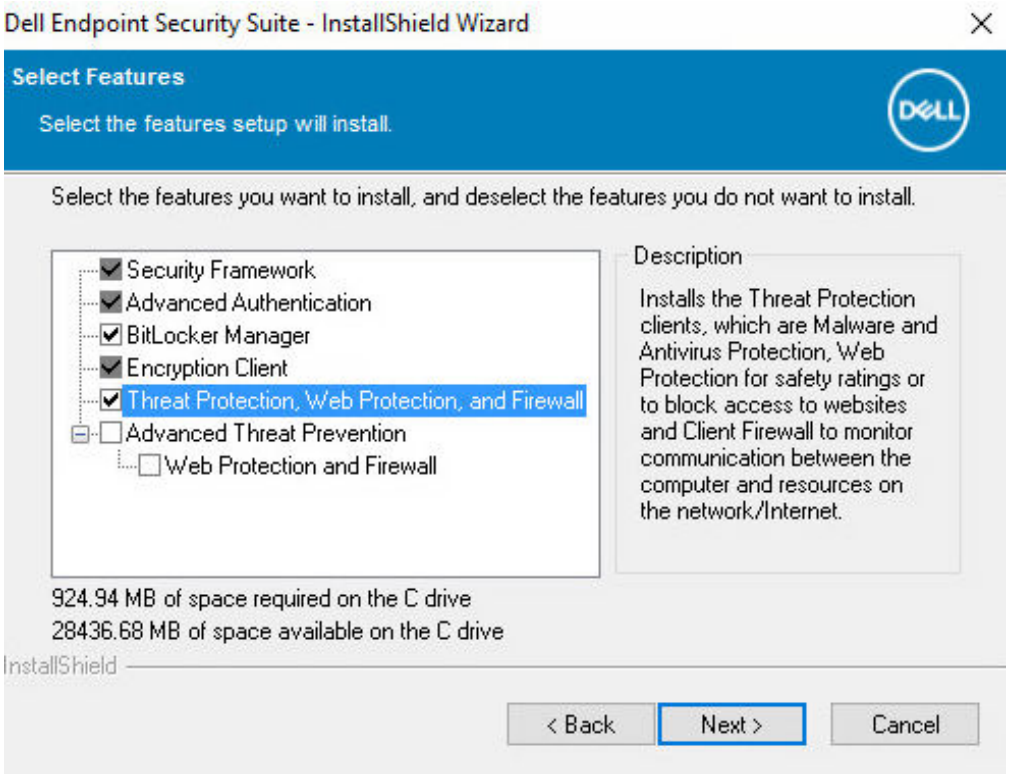
BitLocker Manager installs the BitLocker Manager client, designed to enhance the security of BitLocker deployments by simplifying and reducing the cost of ownership through centralized management of BitLocker encryption policies.

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.

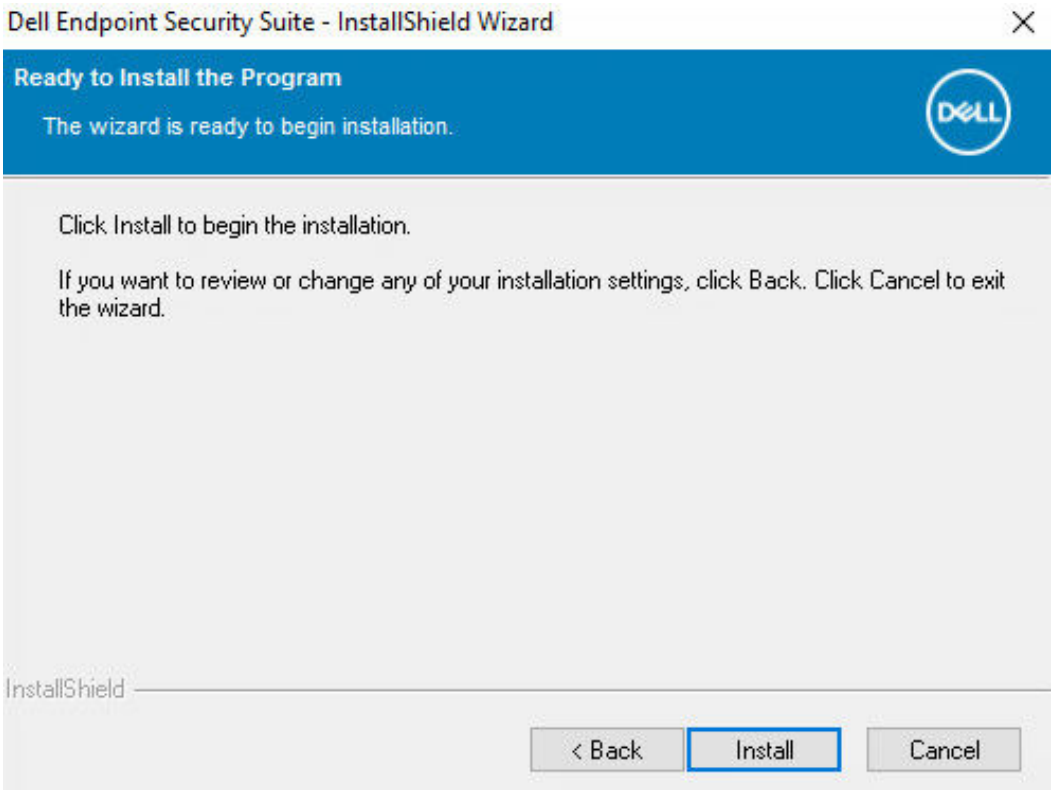
NOTE: Threat Protection and Advanced Threat Prevention cannot reside on the same computer. The installer automatically prevents the selection of both components. Should you wish to install Advanced Threat Prevention, download the Endpoint Security Suite Enterprise *Advanced Installation Guide* for instructions.

NOTE: If the installer detects a Windows version later than Anniversary Update (Redstone 1), the Threat Protection option does not display.

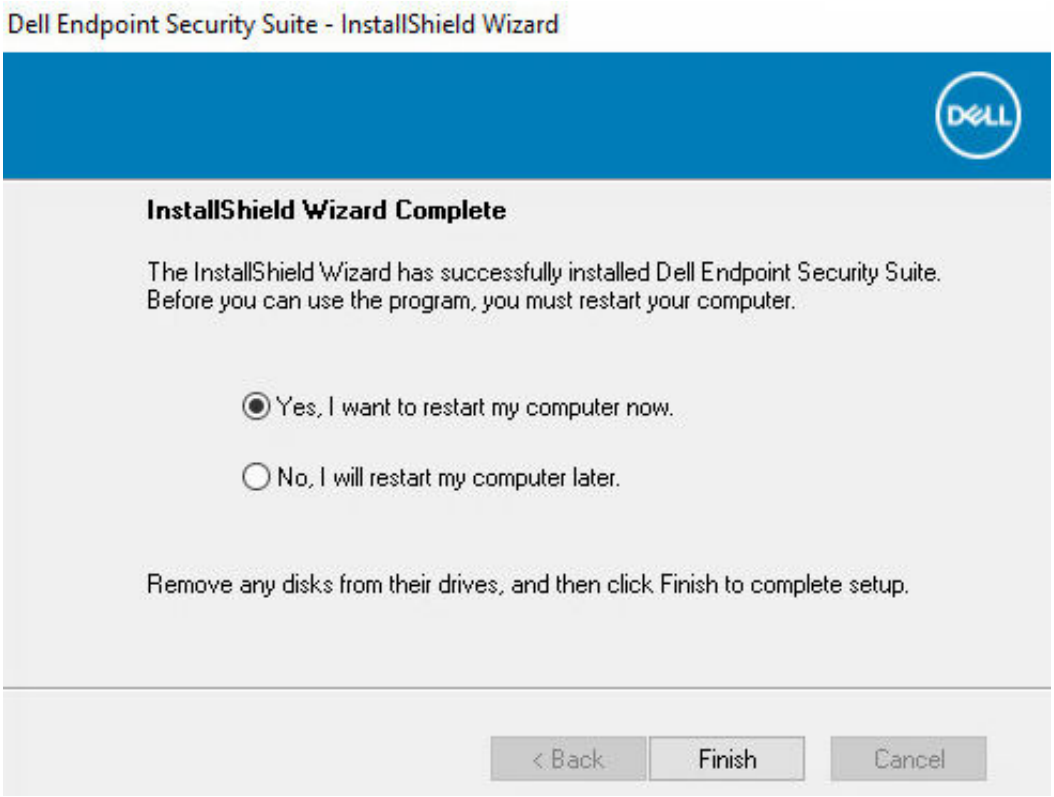
Click **Next** when your selections are complete.



8 Click **Install** to begin the installation. Installation will take several minutes.



9 Select **Yes, I want to restart my computer now** and click **Finish**.



Installation is complete.

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 Pro master installer.

> **NOTE: If you attempt to install the optional Threat Protection features on a Windows 10 Anniversary Update (Redstone 2) or later, an incompatibility warning displays.**

Switch	Description
-y -gm2	Pre-extraction of Endpoint Security Suite Pro master installer. The -y and -gm2 switches must be used together. Do not separate the switches.
/S	Silent installation
/z	Pass variables to the .msi inside the DDSSuite.exe

Parameters

- The following table describes the parameters that can be used with the Endpoint Security Suite Pro master installer. The Endpoint Security Suite Pro master installer cannot exclude individual components but can receive commands to specify which components should be installed.

Parameter	Description
SUPPRESSREBOOT	Suppresses the automatic reboot after the installation completes. Can be used in SILENT mode.
SERVER	Specifies the URL of the Security Management Server/Security Management Server Virtual.
InstallPath	Specifies the path for the installation. Can be used in SILENT mode.
FEATURES	Specifies the components that can be installed in SILENT mode. DE-TP = Threat Protection and Encryption DE = Drive Encryption (Encryption client) BLM = BitLocker Manager SED = SED Management (EMAgent/Manager, PBA/GPE Drivers)
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.
- This example installs all components using the Endpoint Security Suite Pro 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 Security Management Server/Security Management Server Virtual.

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

- This example installs Threat Protection and Encryption ***only*** using the Endpoint Security Suite Pro 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 Security Management Server/Security Management Server Virtual.

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

- This example installs Threat Protection, Encryption, and SED Management using the Endpoint Security Suite Pro 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 Security Management Server/Security Management Server Virtual.

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

-

4

Uninstall Using the Endpoint Security Suite Pro Master Installer

- Each component must be uninstalled separately, followed by uninstallation of the Endpoint Security Suite Pro 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 Pro 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 Threat Protection Clients.
  b Uninstall Encryption Client.
  c Uninstall SED and Advanced Authentication Clients.
  d Uninstall BitLocker Manager Client.
- Proceed to Uninstall the Master Installer.

Uninstall the Endpoint Security Suite Pro 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 Pro master installer.

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

  Reboot the computer when finished.

Uninstall Using the Child Installers

- To uninstall each client individually, the child executable files must first be extracted from the Endpoint Security Suite Pro 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.

Switch	Meaning
/v	Pass variables to the .msi inside the setup.exe. The content must always be enclosed in plain-text quotes.
/s	Silent mode
/x	Uninstall mode
/a	Administrative install (will copy all files inside the .msi)

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.

Option	Meaning
/q	No Progress dialog, restarts itself after process completion
/qb	Progress dialog with **Cancel** button, prompts for restart
/qb-	Progress dialog with **Cancel** button, restarts itself after process completion
/qb!	Progress dialog without **Cancel** button, prompts for restart

Option	Meaning
/qb!-	Progress dialog without **Cancel** button, restarts itself after process completion
/qn	No user interface

Uninstall Threat Protection Clients

Command Line Uninstallation

- Once extracted from the Endpoint Security Suite Pro master installer, the Threat Protection client installer can be located at **C:\extracted\Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi.**
- Go to Add/Remove Programs in the Control Panel and uninstall the following components in this order.
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Threat Prevention
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Then:
- The following example uninstalls the Threat Protection client .

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

Uninstall Encryption Client

- 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.
- Windows Encryption clients update the Security Management Server/Security Management Server Virtual to change the status to *Unprotected* at the beginning of a Encryption client uninstall process. However, in the event that the client cannot contact the Security Management Server/Security Management Server Virtual, regardless of the reason, the status cannot be updated. In this case, you will need to manually *Remove Endpoint* in the Remote 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 Remote Management Console or Compliance Reporter.

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 Pro master installer, the Encryption client installer can be located at **C:\extracted \Encryption\DDPE_XXbit_setup.exe**.
- The following table details the parameters available for the uninstallation.

Parameter	Selection
CMG_DECRYPT	Property for selecting the type of Encryption Removal Agent installation: 3 - Use LSARecovery bundle 2 - Use previously downloaded forensics key material 1 - Download keys from the Dell Server 0 - Do not install Encryption Removal Agent
CMGSILENTMODE	Property for silent uninstallation: 1 - Silent 0 - Not Silent
Required Properties	
DA_SERVER	FQHN for the Security Management Server hosting the negotiate session.
DA_PORT	Port on the Security Management Server for request (default is 8050).
SVCPN	Username in UPN format that the Key Server Service is logged on as on the Security Management Server.
DA_RUNAS	Username in SAM compatible format under whose context the key fetch request will be made. This user must be in the Key Server list in the Security Management Server.
DA_RUNASPWD	Password for the runas user.
FORENSIC_ADMIN	The Forensic Administrator account on the Dell Server, which can be used for forensic requests for uninstalls or keys.
FORENSIC_ADMIN_PWD	The password for the Forensic Administrator account.
Optional Properties	
SVCLOGONUN	Username in UPN format for Encryption Removal Agent Service log on as parameter.
SVCLOGONPWD	Password for log on as user.

- The following example silently uninstalls the Encryption client 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 the Encryption client and downloads the encryptions 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 Remote 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.

NOTE:

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 SED and Advanced Authentication Clients

- Network connection to the Security Management Server/Security Management Server Virtual is required for PBA deactivation.

Process

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

Deactivate the PBA

1. As a Dell administrator, log in to the Remote Management Console.
2. In the left pane, click **Protect & Manage** > **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 **Details** icon of the desired computer.

7 Click **Security Policies** on the top menu.

8 Select **Self-Encrypting Drives**.from the **Policy Category** drop-down menu.

9 Expand the **SED Administration** area and change the **Enable SED Management** and **Activate PBA** policies from *True* to ***False***.

10 Click **Save**.

11 In the left pane, click **Actions** > **Commit Policies**.

12 Click **Apply Changes**.

Wait for the policy to propagate from the Security Management Server/Security Management Server Virtual to the computer targeted for deactivation.

Uninstall the SED and Authentication clients after the PBA is deactivated.

Uninstall SED Client and Advanced Authentication Clients

Command Line Uninstallation

- Once extracted from the master installer, the SED client installer can be located at C:\extracted\Advanced Authentication\<x64/x86>\setup.exe.
  - The following example silently uninstalls the Advanced Authentication client.

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

    Shut down and restart the computer when finished.
- Once extracted from the master installer, the SED client installer can be located at C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe.
  - The following example silently uninstalls the SED client.

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

    Shut down and restart the computer when finished.

Uninstall BitLocker Manager Client

Command Line Uninstallation

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

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

Reboot the computer when finished.

Extract the Child Installers from the Endpoint Security Suite Pro Master Installer

- 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.

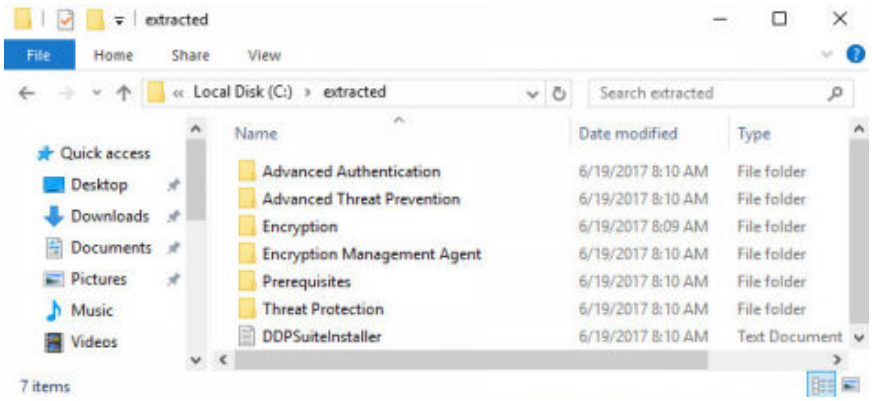
1 From the Dell installation media, copy the **DDSSuite.exe** file to the local computer.

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\.**



7

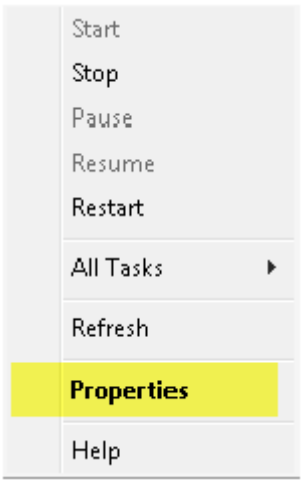
Configure Key Server for Uninstallation of Encryption Client Activated Against Security Management Server

- 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 will need 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**.

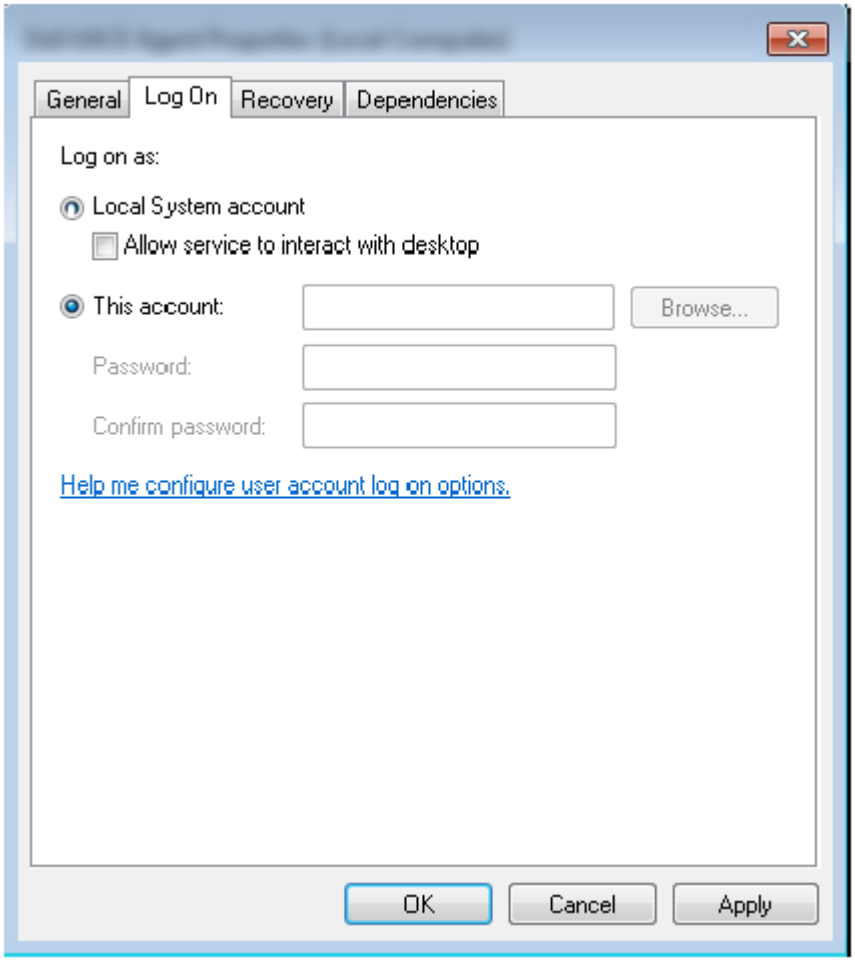


3 Select the Log On tab and select the **This account:** option.

In the *This account:* field, 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.

Remote Management Console - Add Forensic Administrator

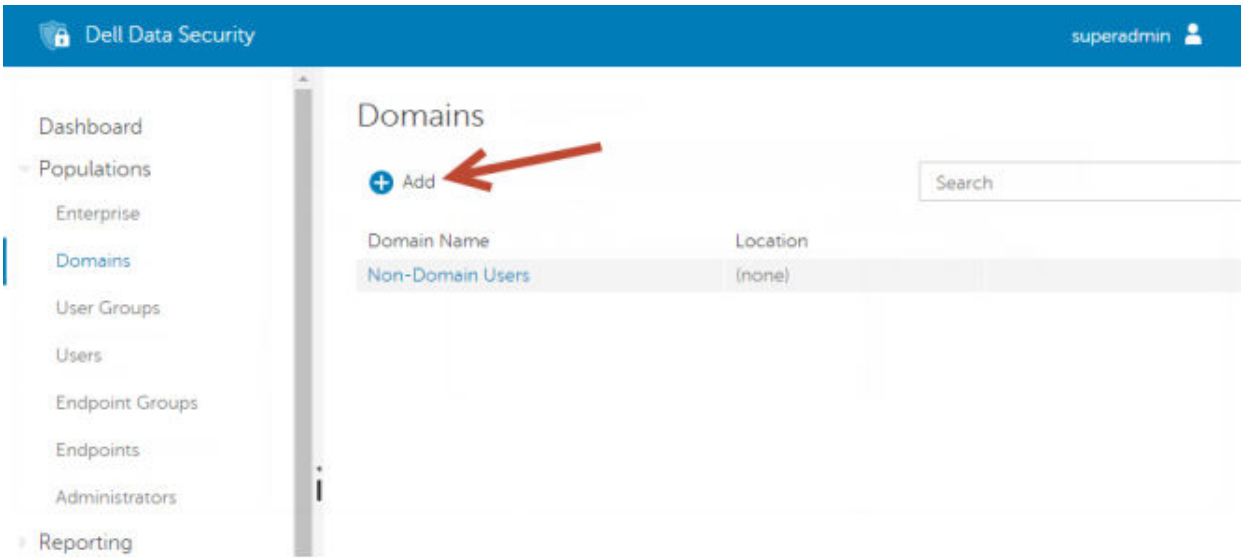
1 If needed, log on to the Remote Management Console.

2 Click **Populations** > **Domains**.

3 Select the appropriate Domain.

4 Click the **Key Server** tab.

5 In the Account field, add the user that will be performing 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 username 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.

8

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 an Security Management Server/Security Management Server Virtual.
- This utility uses one of the following methods to download a key 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 the Administrative Download Utility in 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 (enabled in the Remote Management Console), such as jdoe

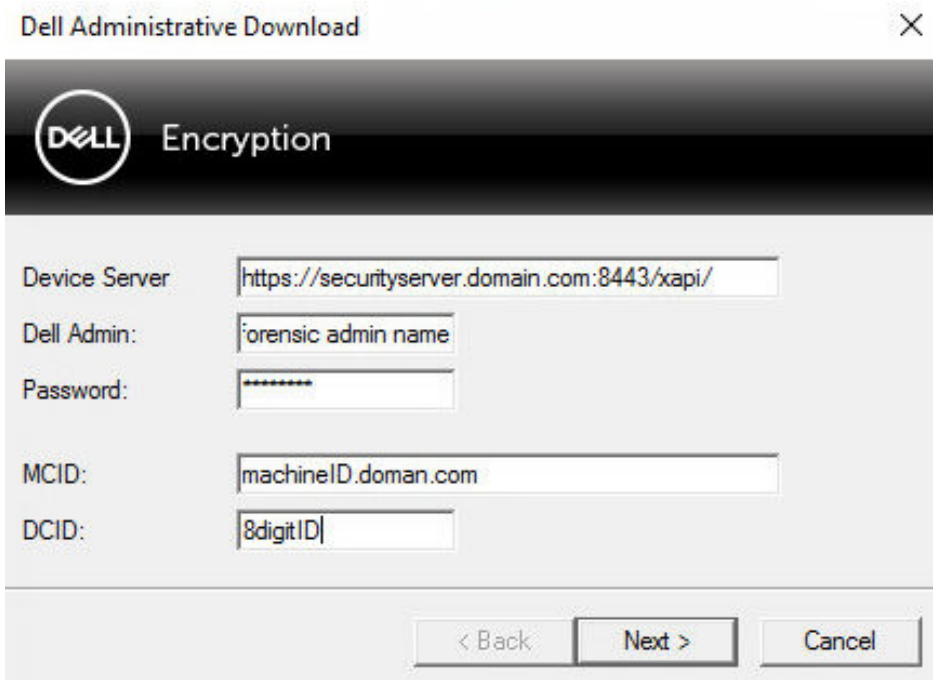
Password: Forensic administrator password

MCID: Machine ID, such as machineID.domain.com

DCID: First eight digits of the 16-digit Shield ID

> **TIP:**
> Usually, specifying either the MCID *or* DCID are sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information about the client and client computer.

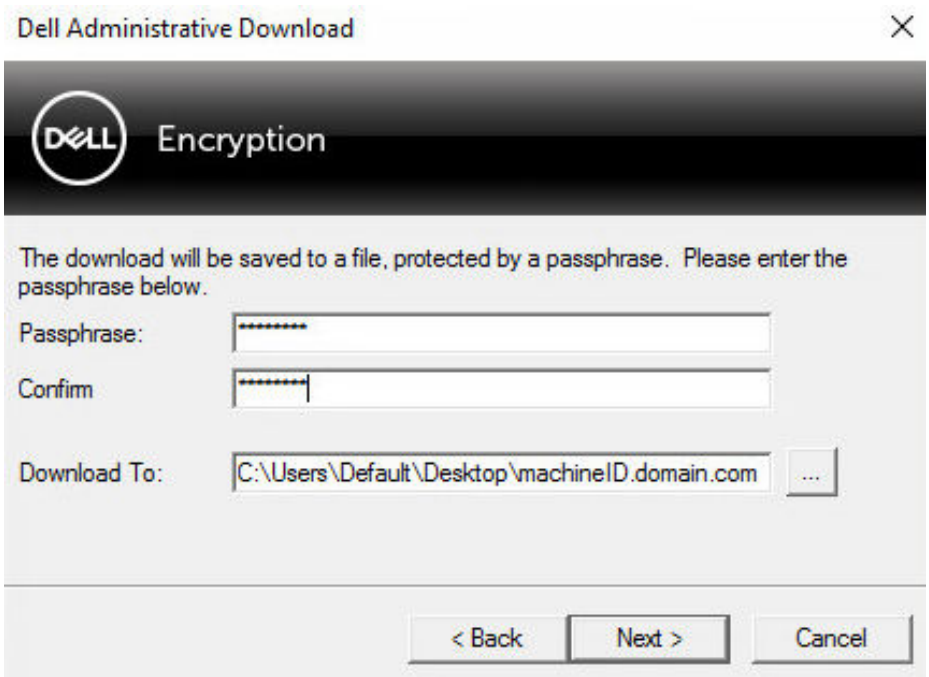
Click **Next**.



3 In the Passphrase: field, 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 to or click ... to select a different location.

Click **Next**.



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

4 Click **Finish** when complete.

Use the Administrative Download Utility in 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

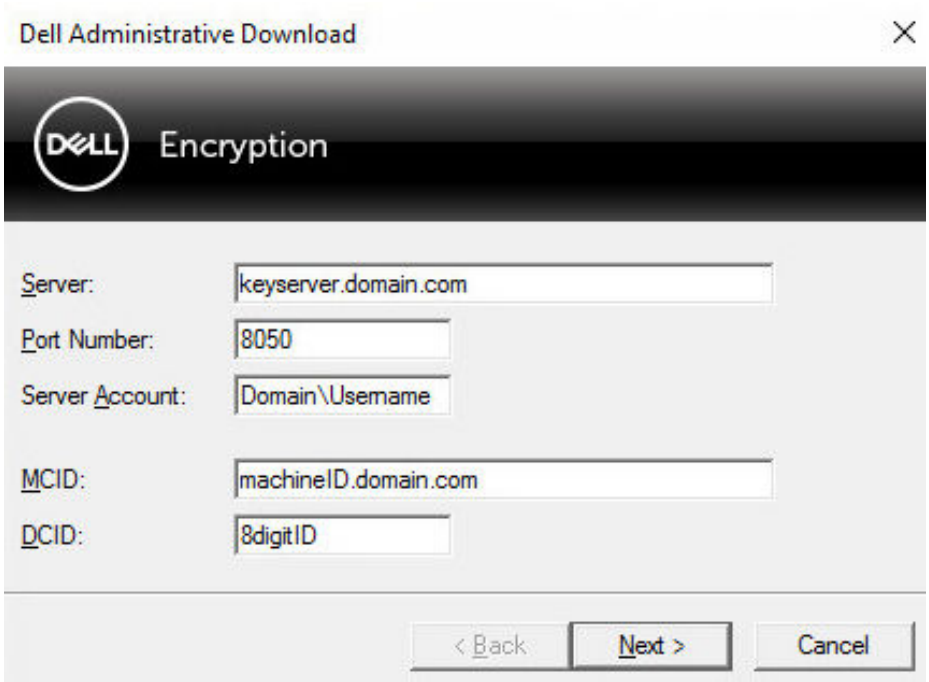
Server Account: The domain user the Key Server is running as. The format is domain\username. The domain user running the utility must be authorized to perform the download from the Key Server

MCID: Machine ID, such as machineID.domain.com

DCID: First eight digits of the 16-digit Shield ID

> **TIP:**
> Usually, specifying either the MCID *or* DCID are sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information about the client and client computer.

Click **Next**.

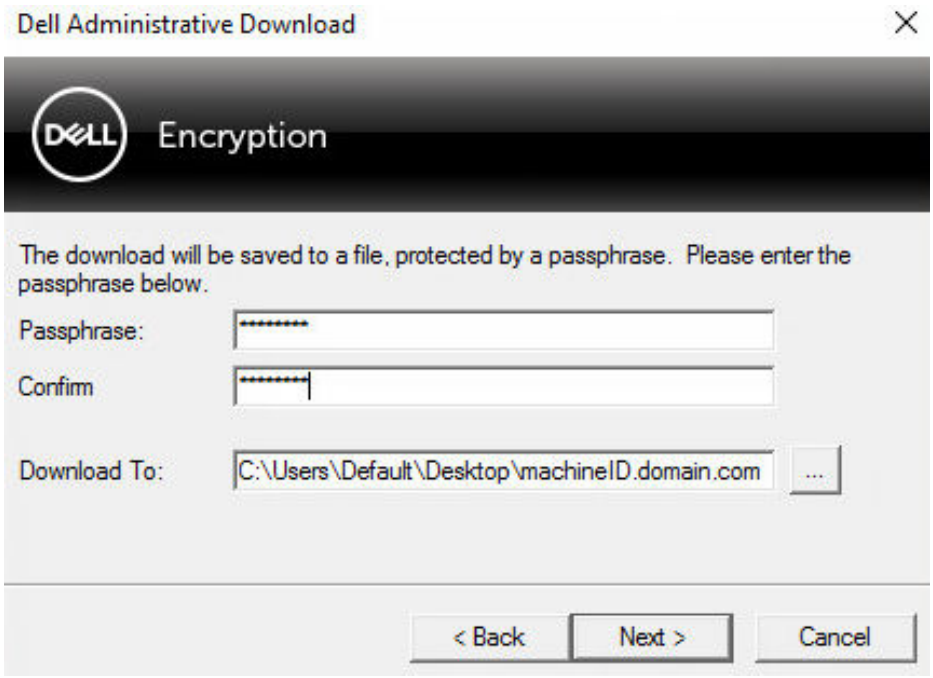


3 In the Passphrase: field, type a passphrase to protect the download file. The passphrase must be at least eight characters long, and contain at least one alphabetic and one numeric character.

Confirm the passphrase.

Either accept the default name and location of where the file will be saved or click ... to select a different location.

Click **Next**.



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

4 Click **Finish** when complete.

9

Troubleshooting

All Clients - Troubleshooting

- **Endpoint Security Suite Pro master 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.

  Go to https://www.microsoft.com/en-us/download/details.aspx?id=30653to download the full version of Microsoft .Net Framework 4.5.2 or later.
- See *this document* if the computer targeted for installation has (or has had in the past) Dell Access installed. DDP|A 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 Security Management 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.

Protected status is now denoted if any of the following criteria have been met:

- Advanced Threat Prevention is installed and enabled.
- Dell Data Guardian is installed and enabled.
- Self-Encrypting Drive Management is installed, enabled, and the Pre-Boot Authentication (PBA) is enabled.
- BitLocker Manager is installed, enabled, and encryption has completed.
- Dell Encryption (Mac) is installed and enabled, and policy-based encryption has been enforced.
- Dell Encryption (Windows) is installed, enabled, Policy-Based Encryption has been set for the endpoint, and the most recent policy has been applied for the last logged on user.

Encryption Client Troubleshooting

Upgrade to the Windows 10 Creators Update

To upgrade to the Windows 10 Creators Update version, follow the instructions in the following article: http://www.dell.com/support/article/us/en/19/SLN298382.

Encryption External Media and PCS Interactions

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

The Encryption External Media Access to unShielded Media policy interacts with Port Control System - Storage Class: External Drive Control policy. If you intend to set the Encryption External Media Access to unShielded Media policy to *Full Access*, ensure that the Storage Class: 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

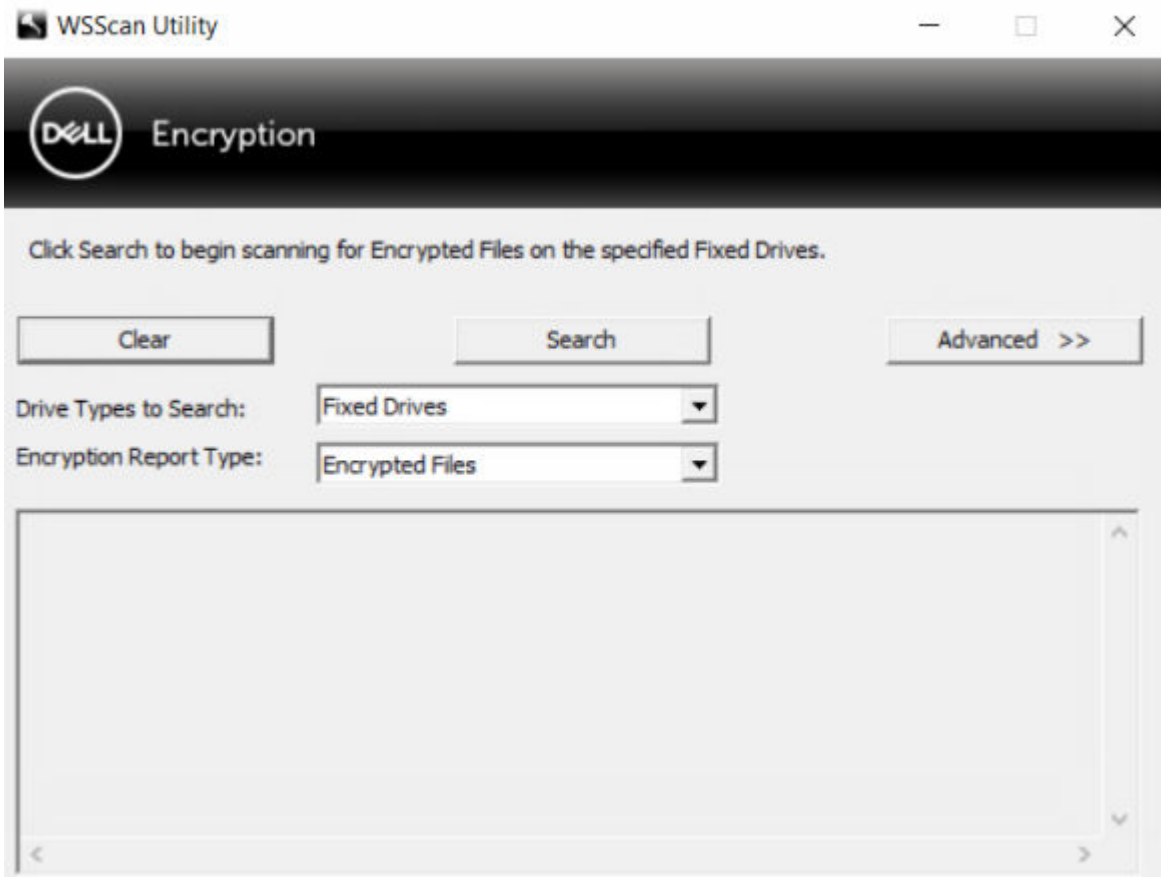
- Set Windows Media Encryption = On.
- Set EMS Exclude CD/DVD Encryption = not selected.
- Set Subclass Storage: Optical Drive Control = UDF Only.

Use WSScan

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

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 from the drop-down menu: *All Drives, Fixed Drives*, *Removable Drives*, or *CDROMs/ DVDROMs*.
5 Select the desired Encryption Report Type from the drop-down menu: *Encrypted Flles*, *Unencrypted Flles*, *All Flles*, or *Unencrypted Flles in Violation*:
   - *Encrypted Flles* - To ensure that all data is decrypted when uninstalling the Encryption client. 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 Flles* - To identify files that are not encrypted, with an indication of whether the files should be encrypted (Y/N).
   - *All Flles* - To list all encrypted and unencrypted files, with an indication of whether the files should be encrypted (Y/N).
   - *Unencrypted Flles in Violation* - To identify files that are not encrypted that should be encrypted.
6 Click **Search**.



OR

1 Click **Advanced** to toggle the view to **Simple** to scan a particular folder.

2 Go to Scan Settings and enter the folder path in the **Search Path** field. If this field is used, the selection in the drop-down box is ignored.

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

4 Change the default path and filename in *Path*, if desired.

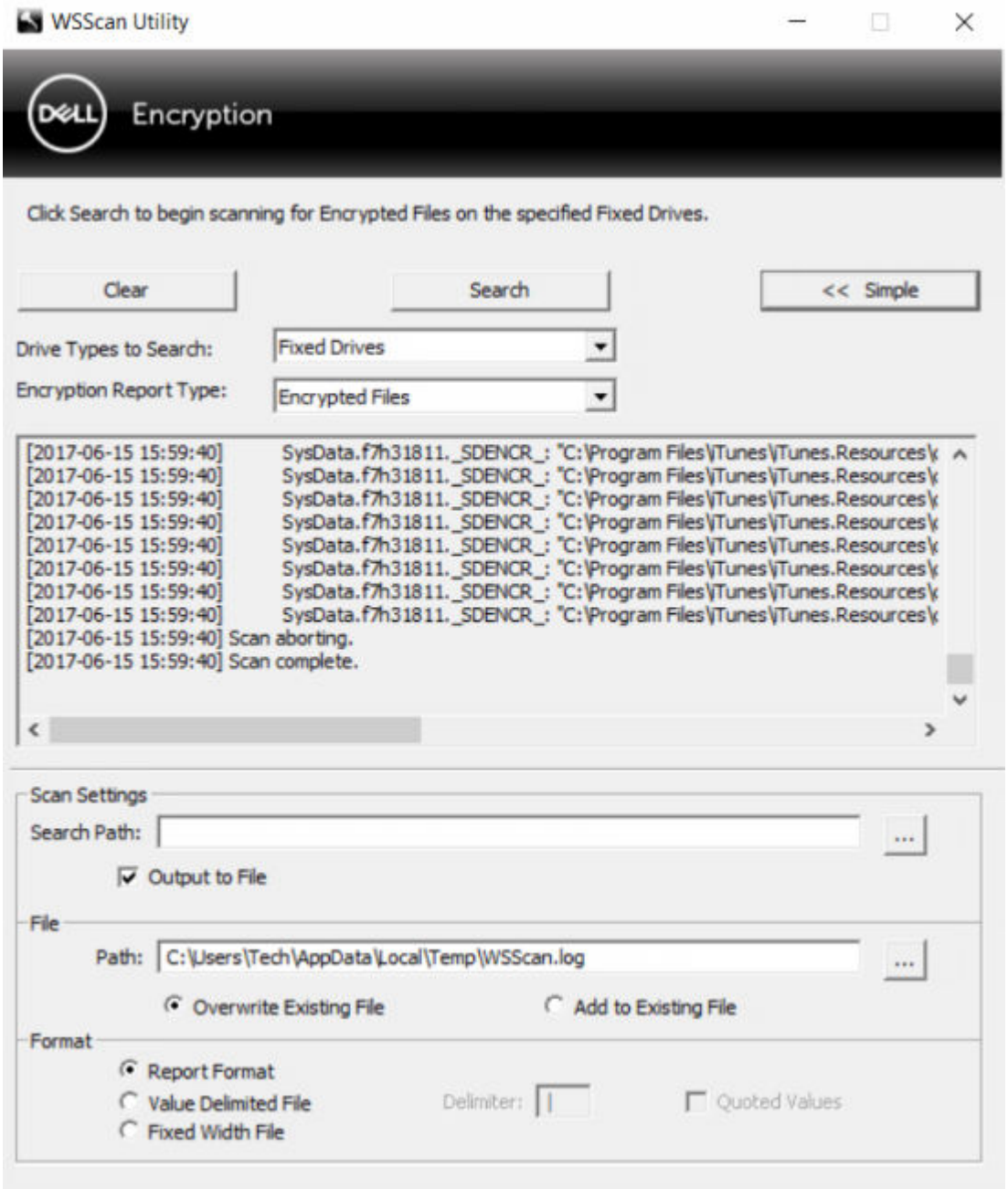
5 Select **Add to Existing File** if you do not want to overwrite any existing WSScan output files.

6 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.

7 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

Output	Meaning
Date/time stamp	The date and time the file was scanned.
Encryption type	The type of encryption used to encrypt the file. **SysData:** SDE Encryption Key.

Output	Meaning
	User: User Encryption Key. **Common:** Common Encryption Key. WSScan does not report files encrypted using Encrypt for Sharing.
KCID	The Key Computer ID. As shown in the example above, "**7vdlxrsb**" If you are scanning a mapped network drive, the scanning report does not return a KCID.
UCID	The User ID. As shown in the example above, "**_SDENCR_**" The UCID is shared by all the users of that computer.
File	The path of the encrypted file. As shown in the example above, "**c:\temp\Dell - test.log**"
Algorithm	The encryption algorithm being used to encrypt the file. As shown in the example above, "**is still AES256 encrypted**" RIJNDAEL 128 RIJNDAEL 256 AES 128 AES 256 3DES

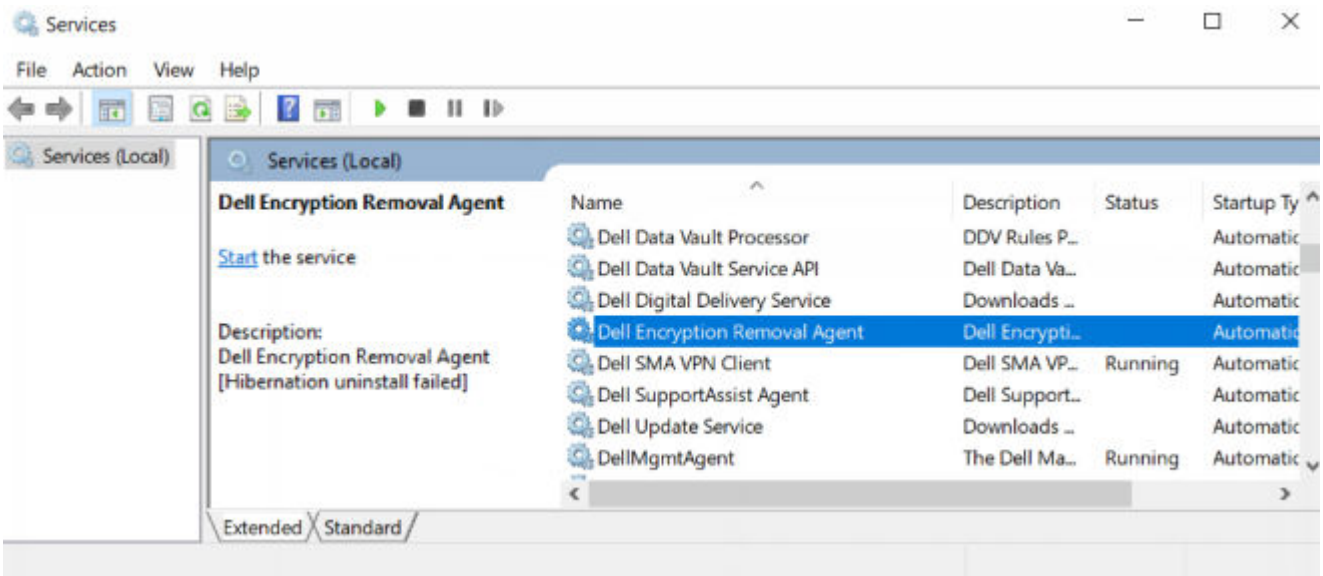
Check Encryption Removal Agent Status

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** - The Encryption client is still installed, is still configured, or both. Decryption does not start until the Encryption client 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.



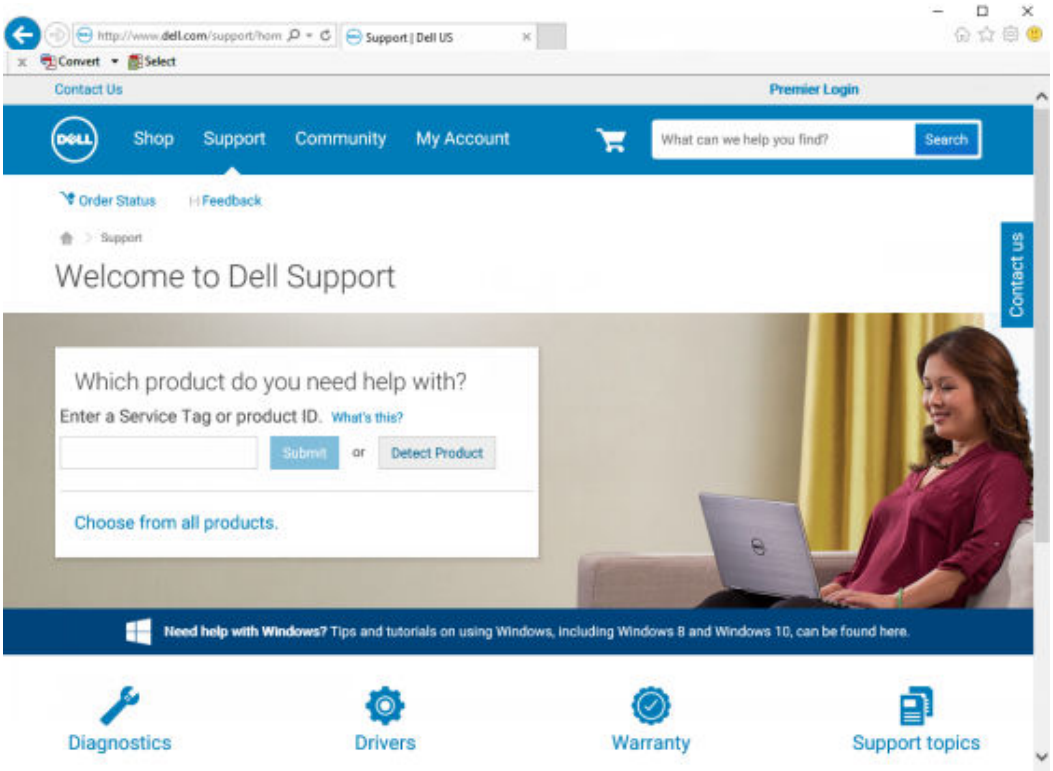
Dell ControlVault Drivers

Update Dell ControlVault Drivers and Firmware

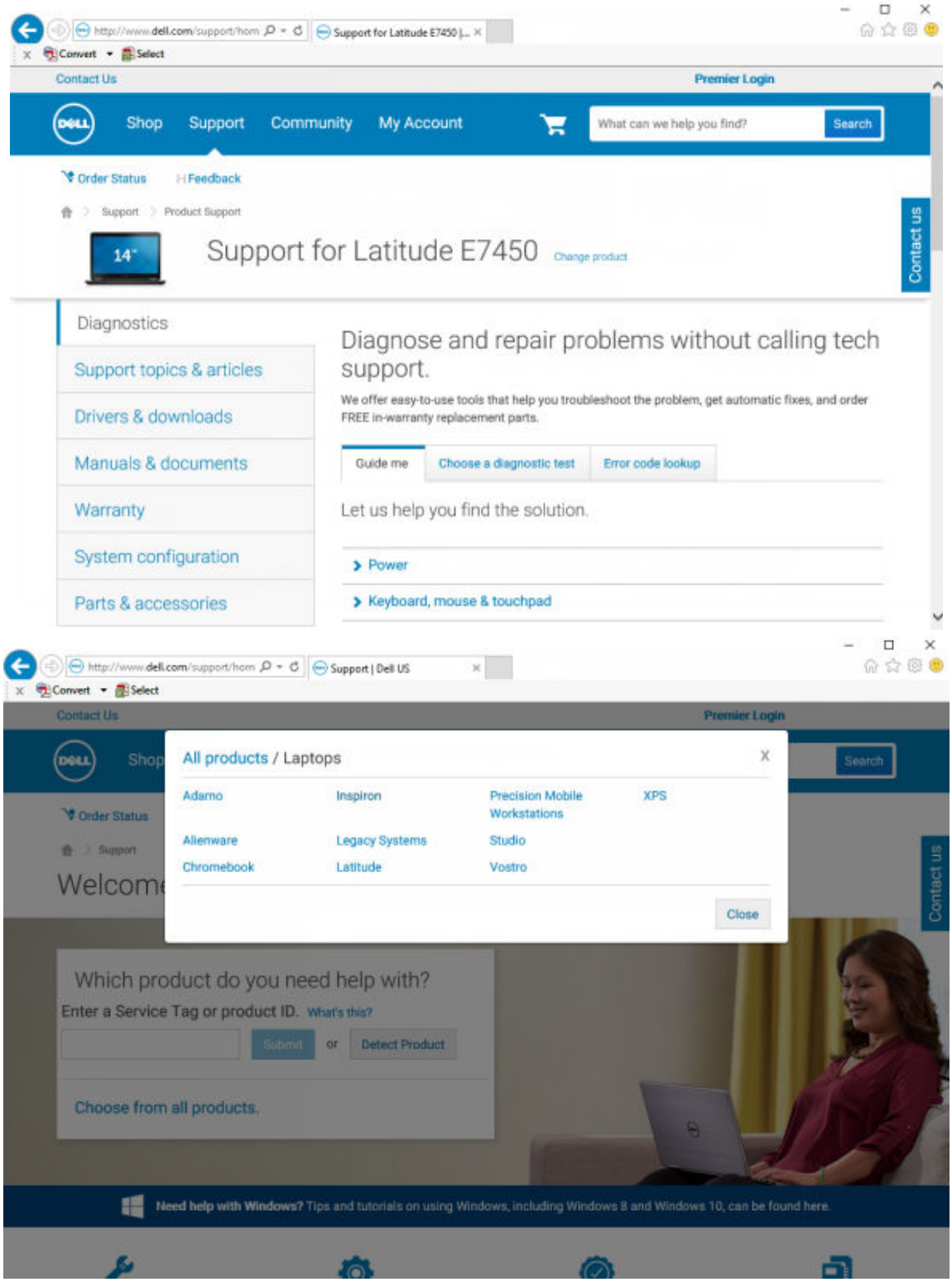
- Dell ControlVault drivers and firmware that are installed on Dell computers at the factory are outdated and should be updated by following this procedure, in this order.
- If an error message is received during client installation prompting you to exit the installer to update Dell ControlVault drivers, 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

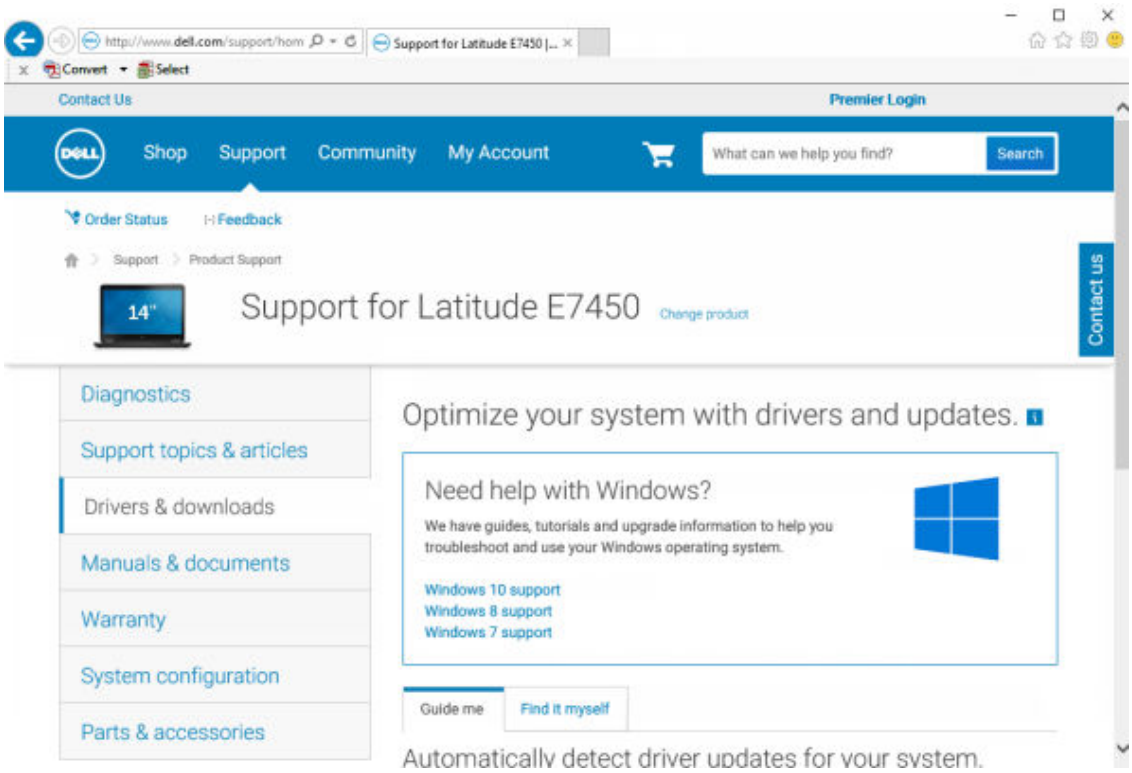
1 Go to support.dell.com.



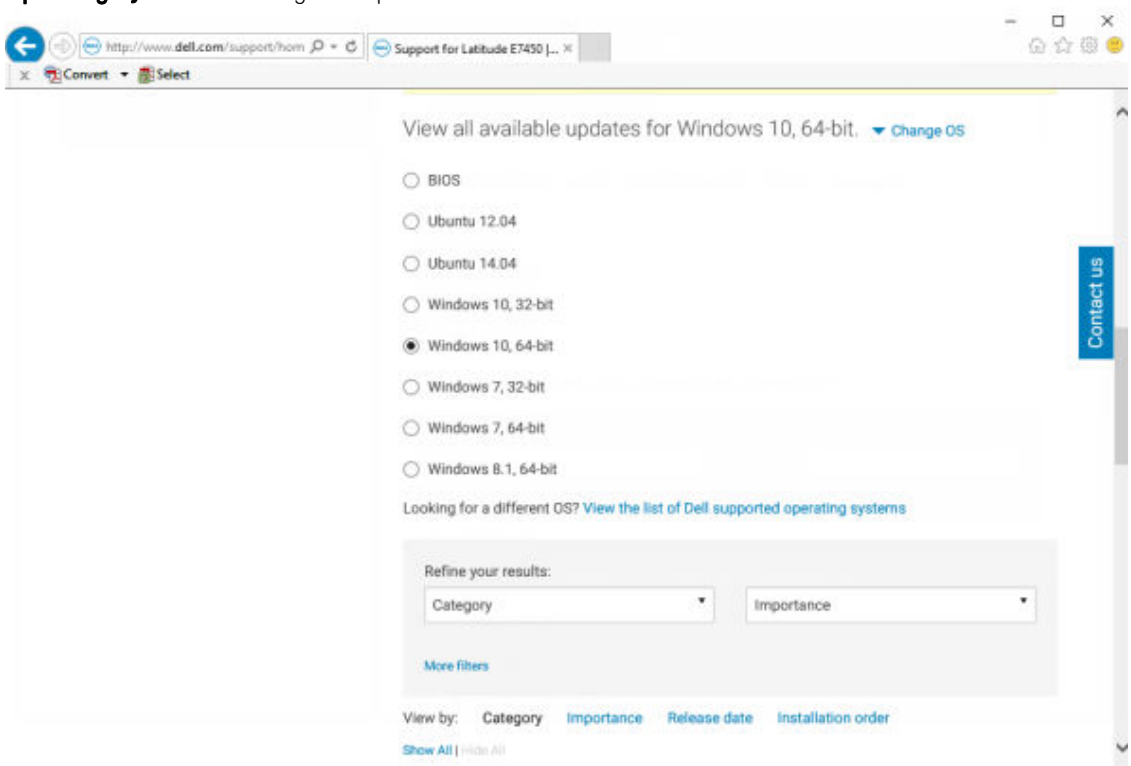
2 Select your computer model.



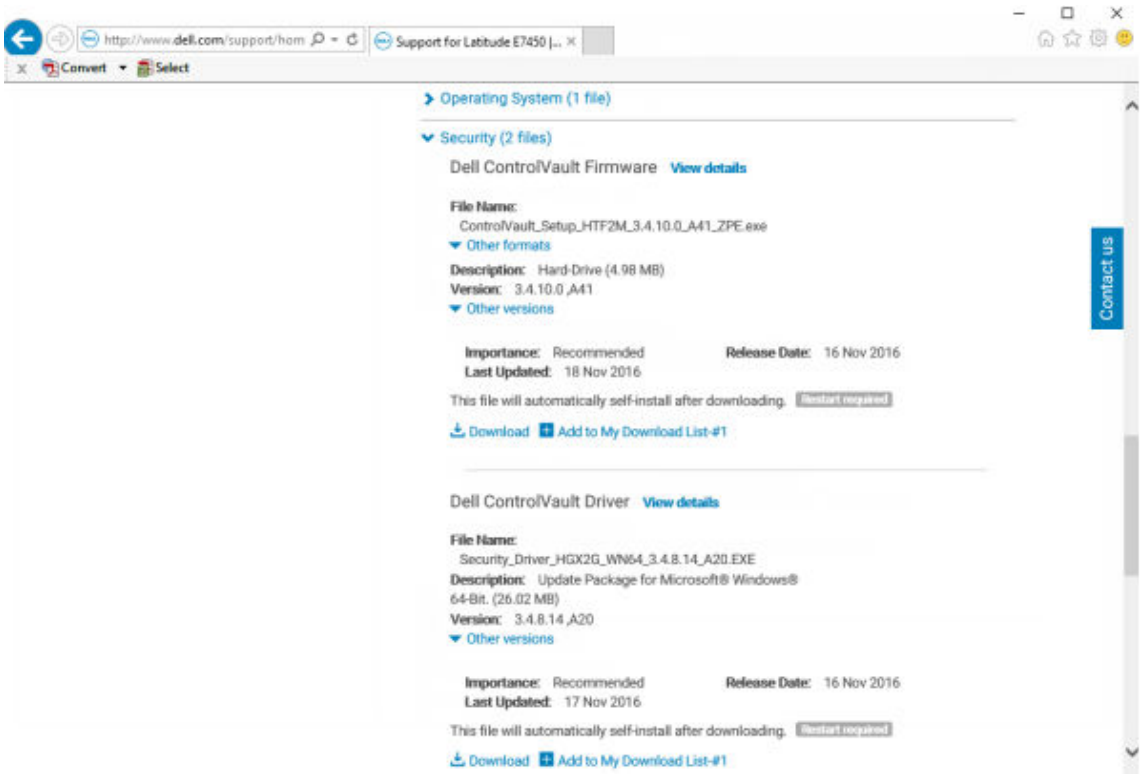
3 Select **Drivers & Downloads**.



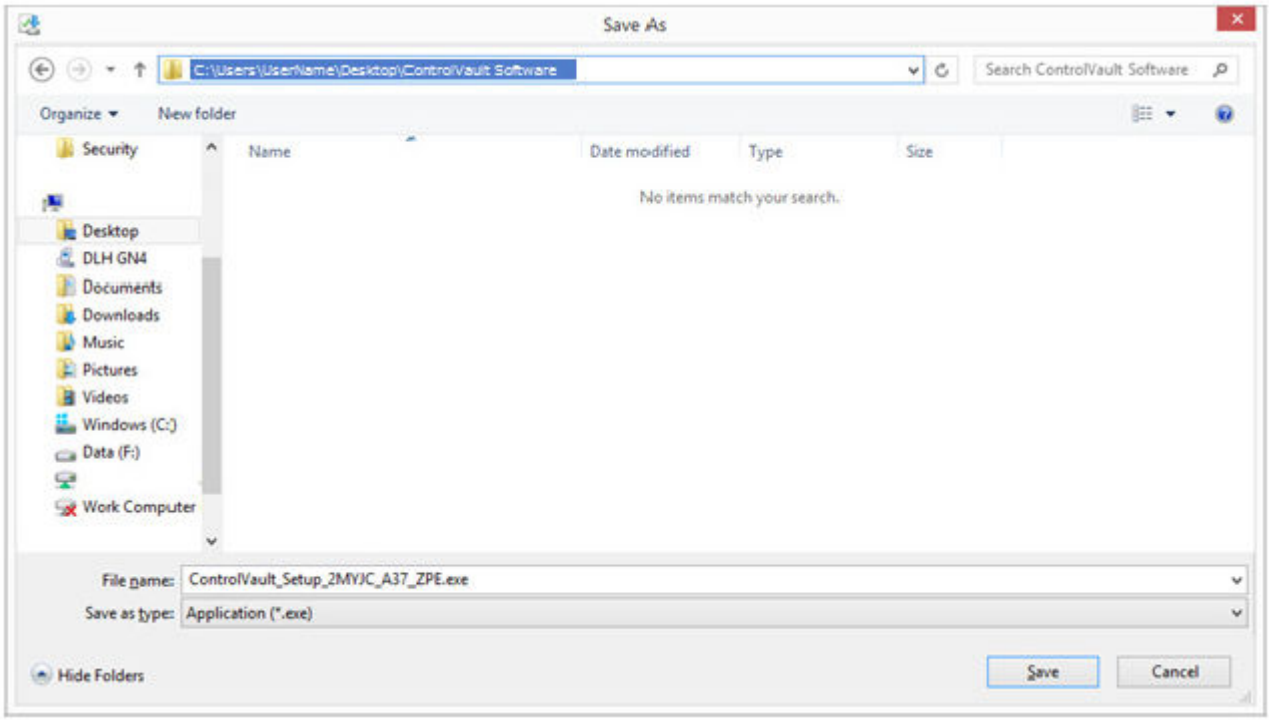
4 Select the **Operating System** of the target computer.



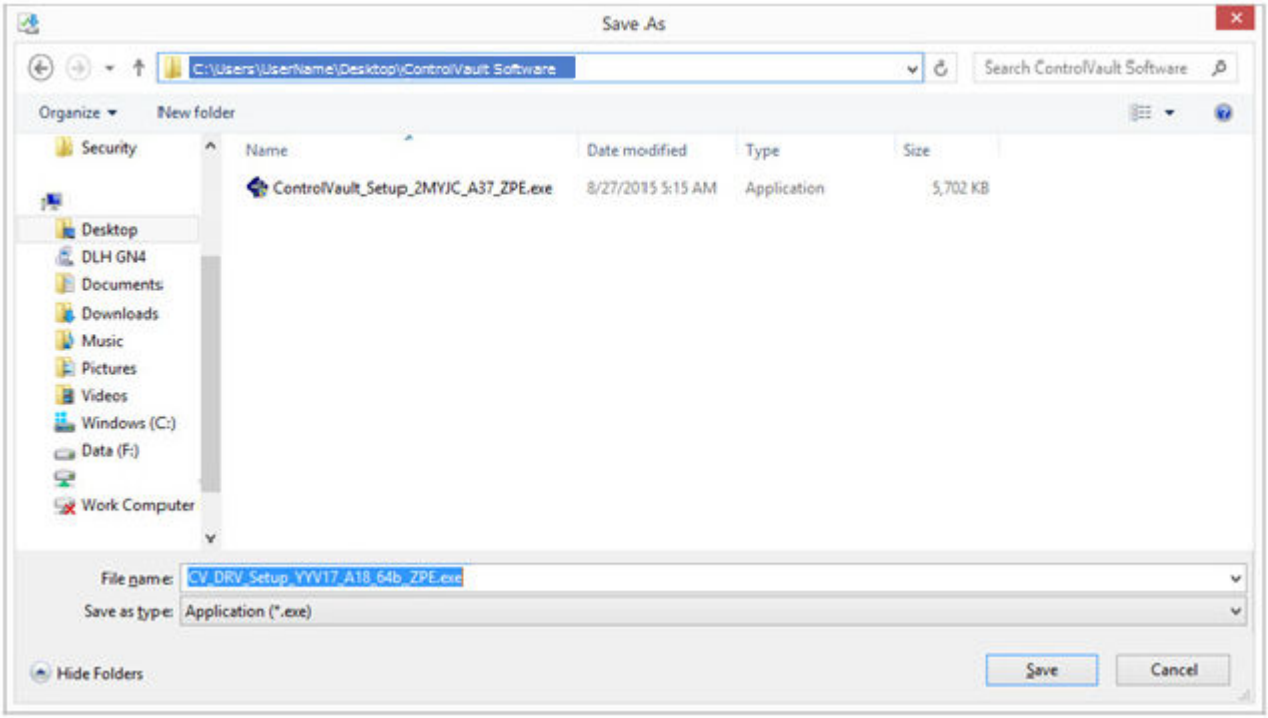
5 Expand the **Security** category.



6 Download and save the Dell ControlVault Drivers.



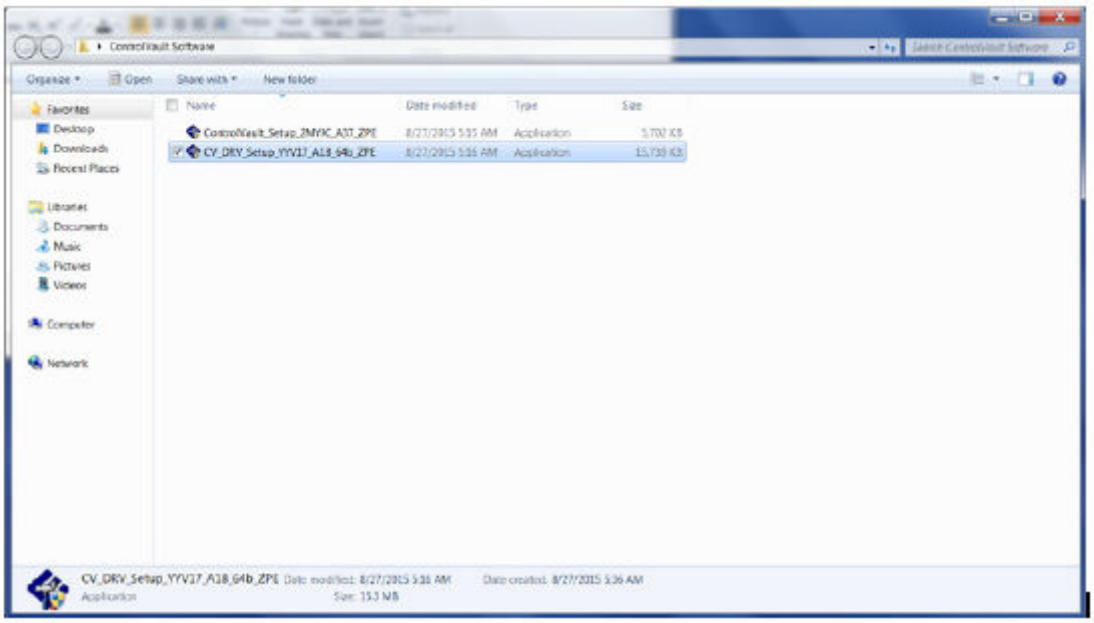
7 Download and save the Dell ControlVault Firmware.



8 Copy the drivers and firmware to the target computers, if needed.

Install Dell ControlVault Driver

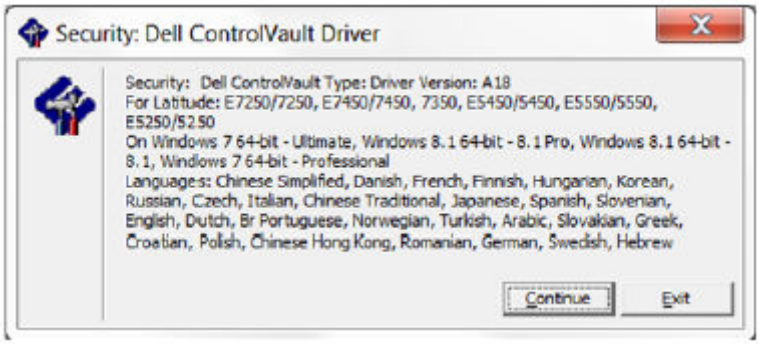
1 Navigate to the folder which you downloaded the driver installation file.



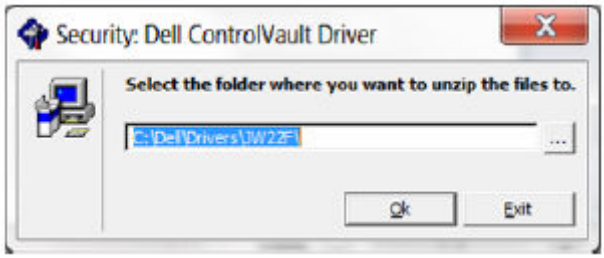
2 Double-click the Dell ControlVault driver to launch the self-extracting executable file.

> **TIP:**
> Be sure to install the driver first. The filename of the driver *at the time of this document creation* is ControlVault_Setup_2MYJC_A37_ZPE.exe.

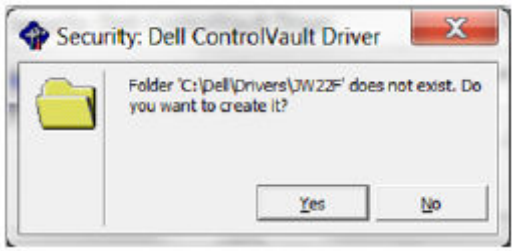
3 Click **Continue** to begin.



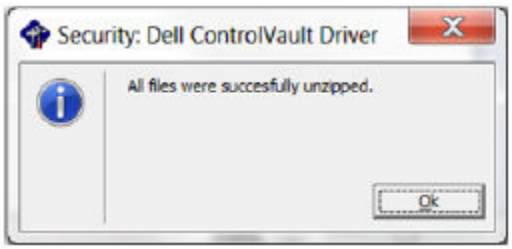
4 Click **Ok** to unzip the driver files in the default location of C:\Dell\Drivers\<New Folder>.



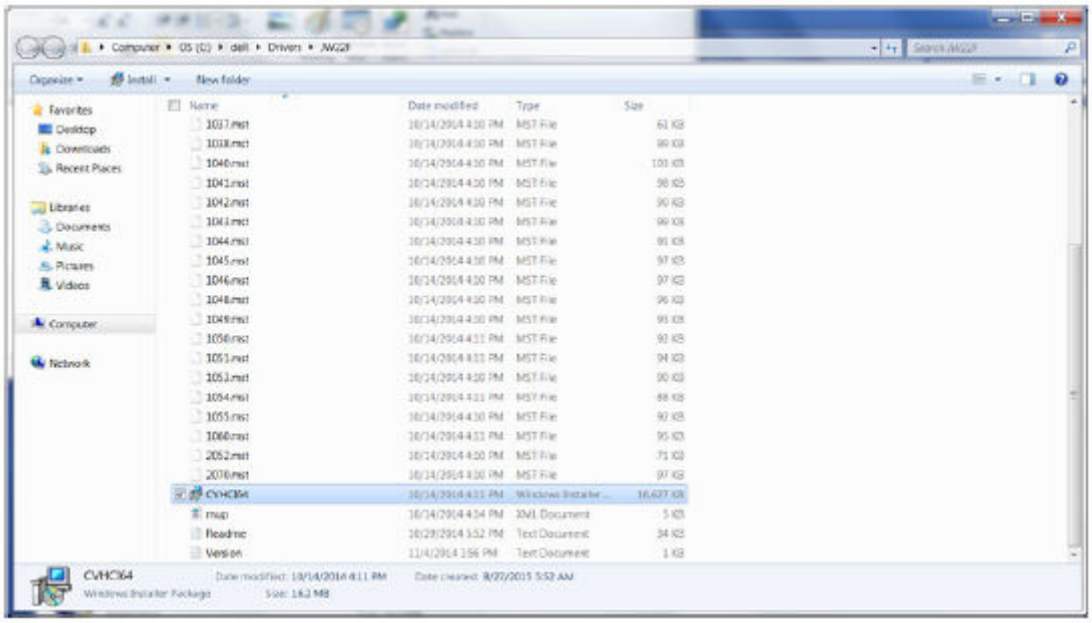
5 Click **Yes** to allow the creation of a new folder.



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



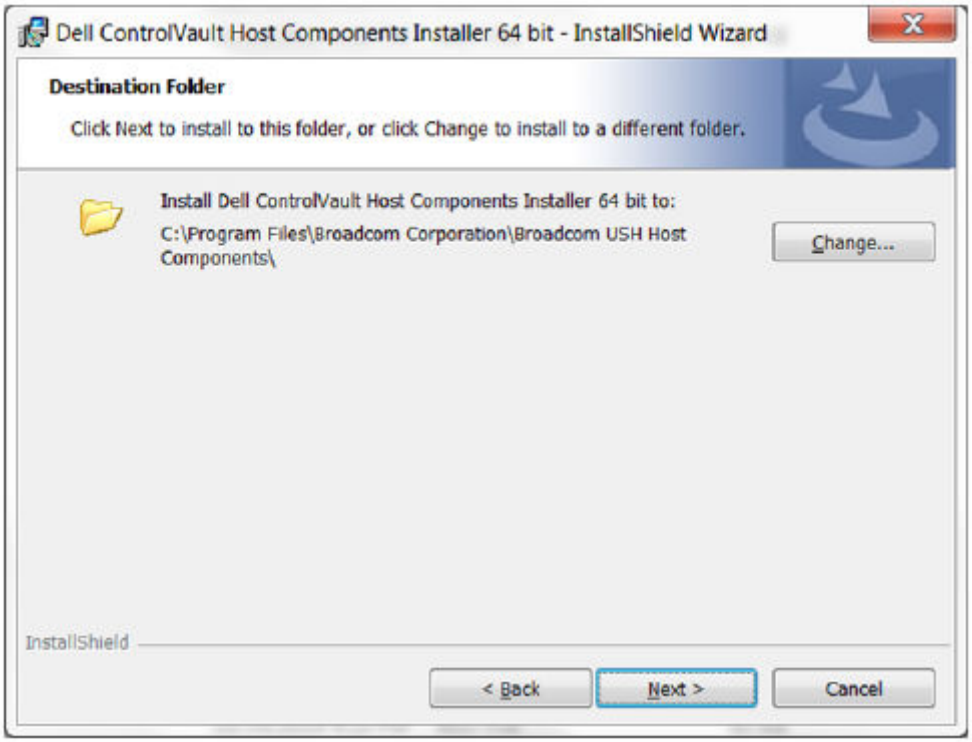
7 The folder which contains the files should display after extraction. If not, navigate to the folder to which you extracted the files. In this case, the folder is **JW22F**.



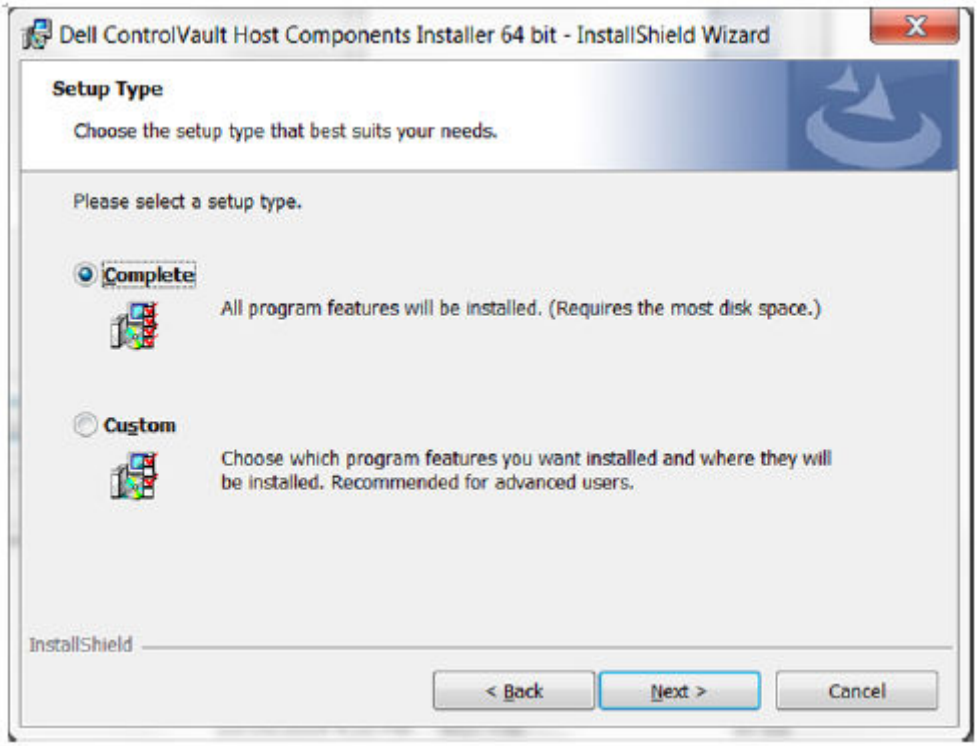
8 Double-click **CVHCI64.MSI** to launch the driver installer. [this example is **CVHCI64.MSI** in this example (CVHCI for a 32-bit computer)].

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

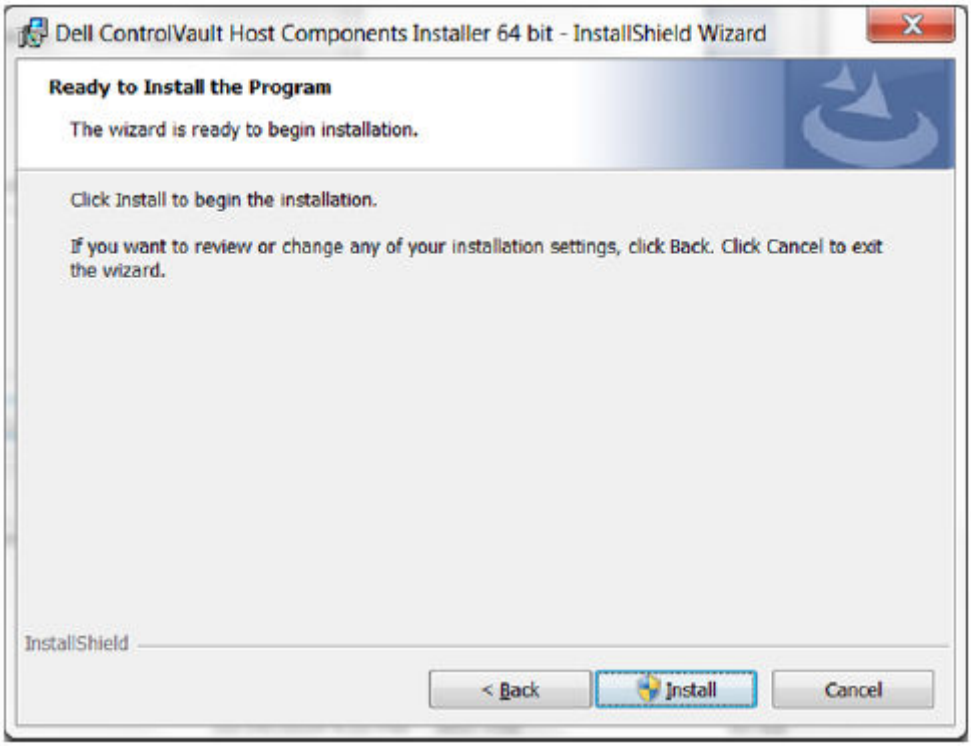
10 Click **Next** to install the drivers in the default location of C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.



11 Select the **Complete** option and click **Next**.



12 Click **Install** to begin the installation of the drivers.



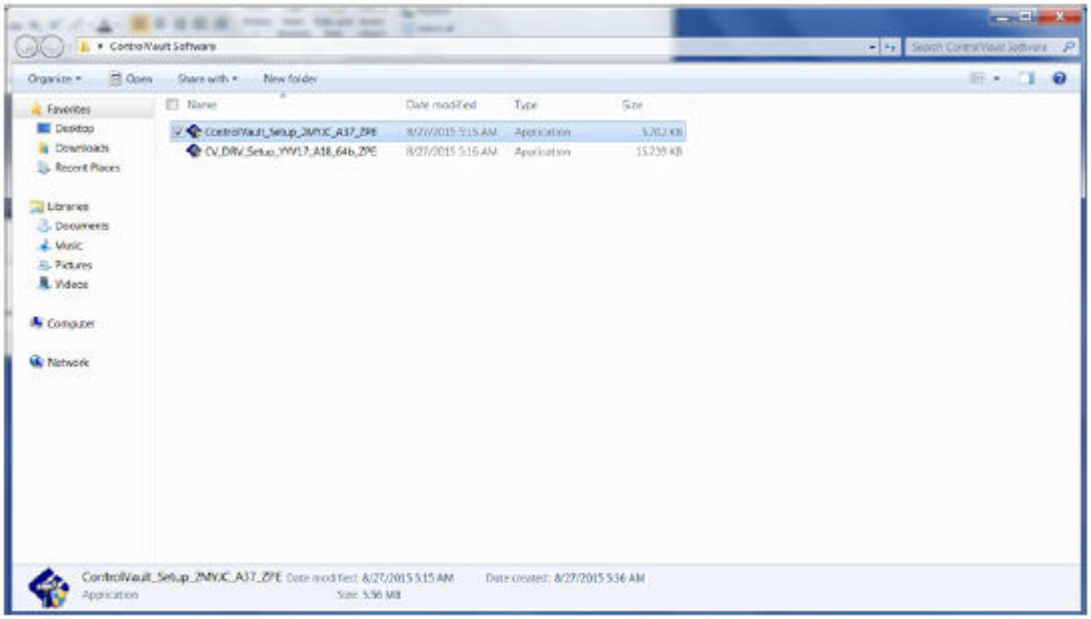
13 Optionally check the box to display the installer log file. Click **Finish** to exit the wizard.

Verify Driver Installation

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

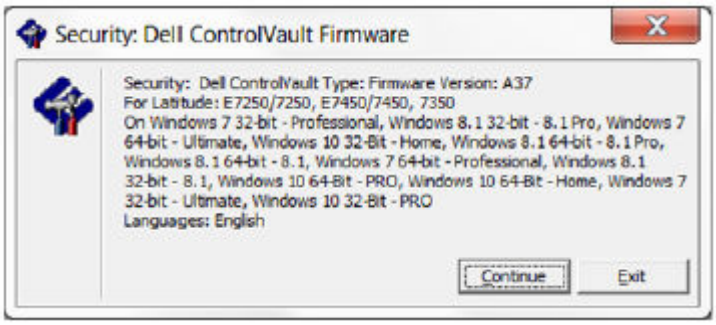
Install Dell ControlVault Firmware

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

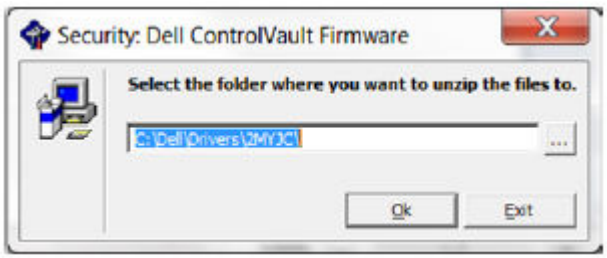


2 Double-click the Dell ControlVault firmware to launch the self-extracting executable file.

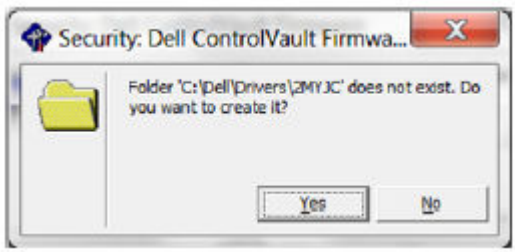
3 Click **Continue** to begin.



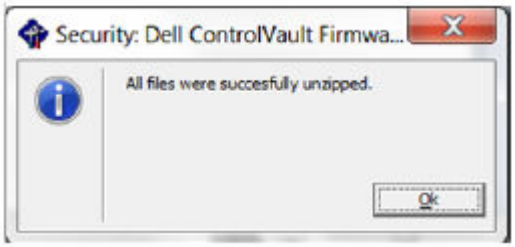
4 Click **Ok** to unzip the driver files in the default location of **C:\Dell\Drivers\<New Folder>**.



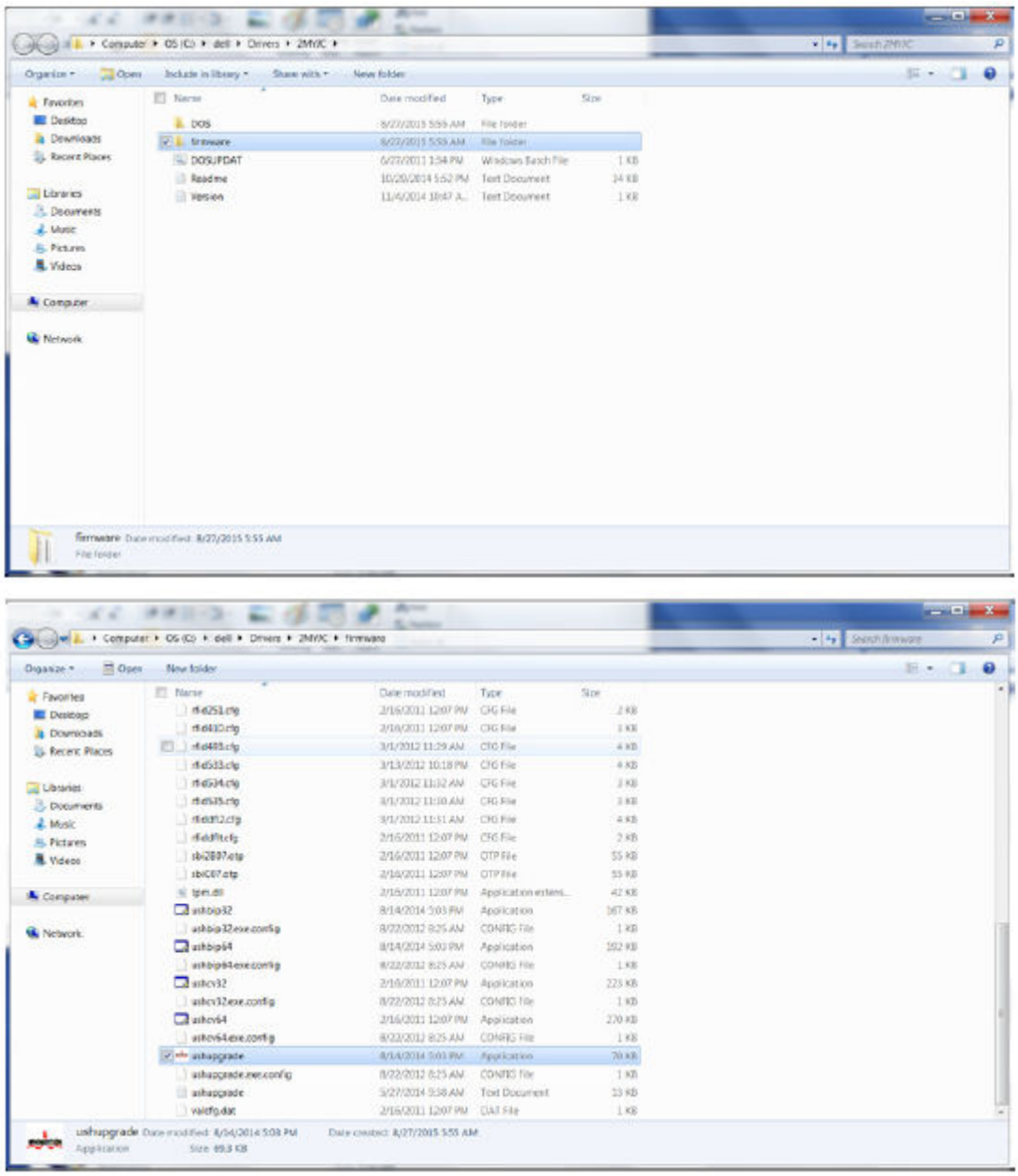
5 Click **Yes** to allow the creation of a new folder.



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

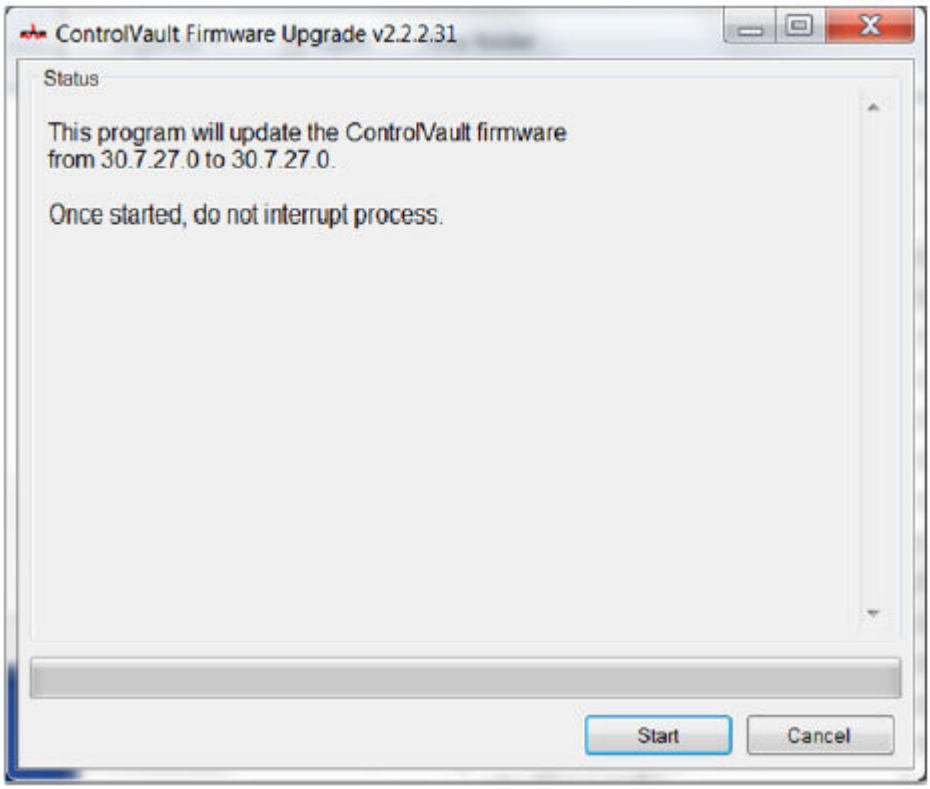


7 The folder which contains the files should display after extraction. If not, navigate to the folder to which you extracted the files. Select the **firmware** folder.



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

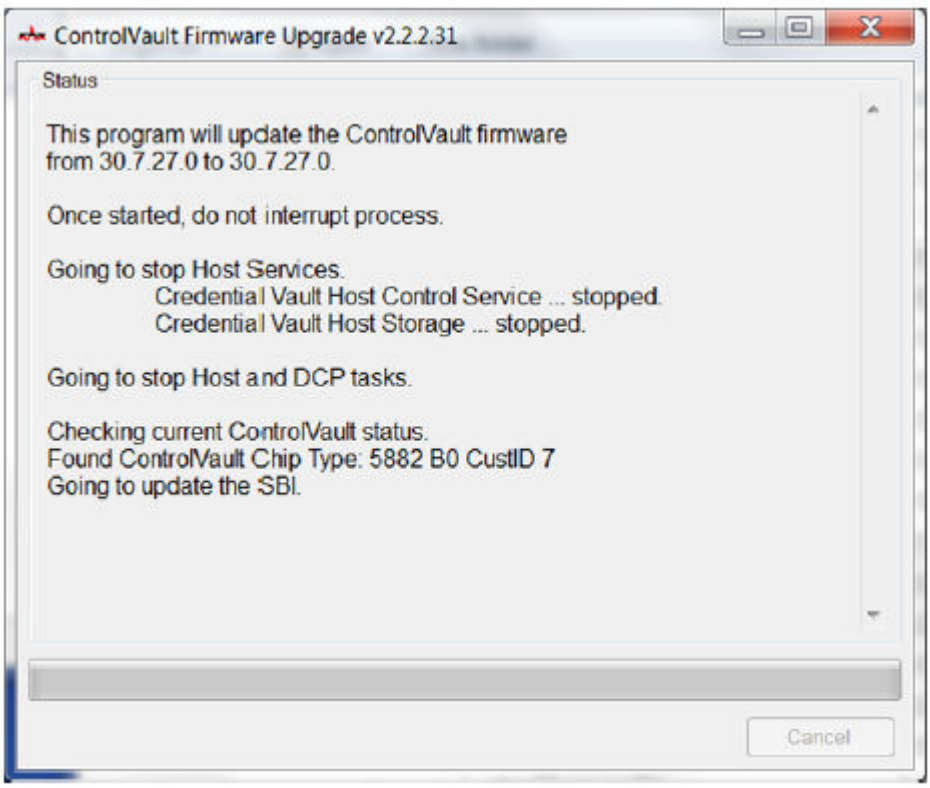
9 Click **Start** to begin the firmware upgrade.

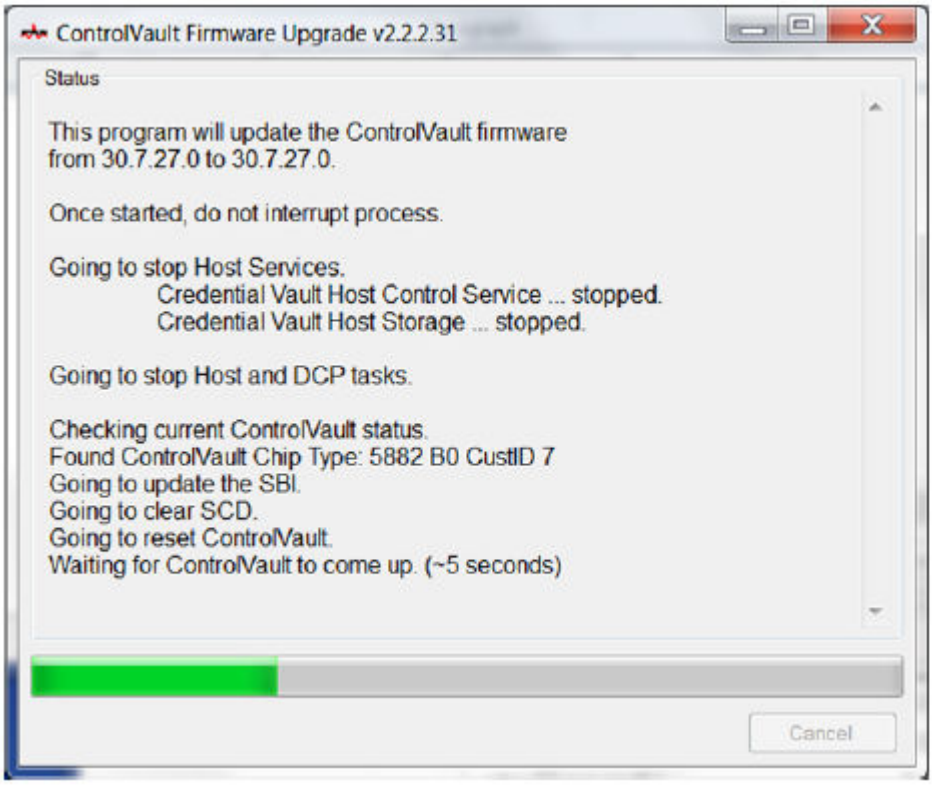


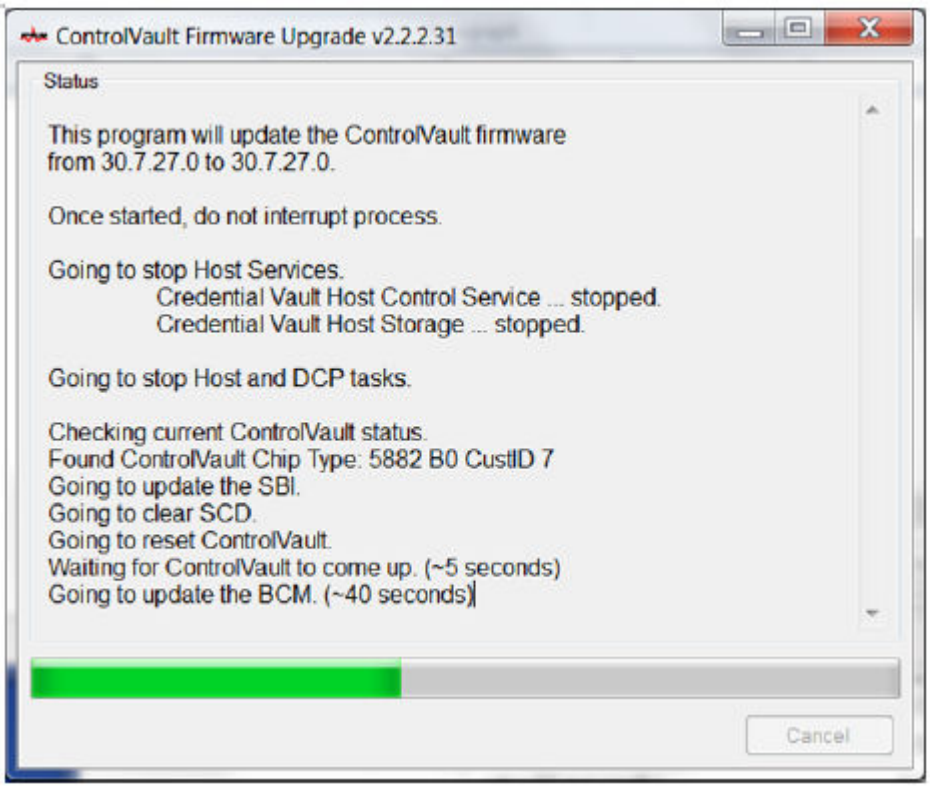
IMPORTANT:

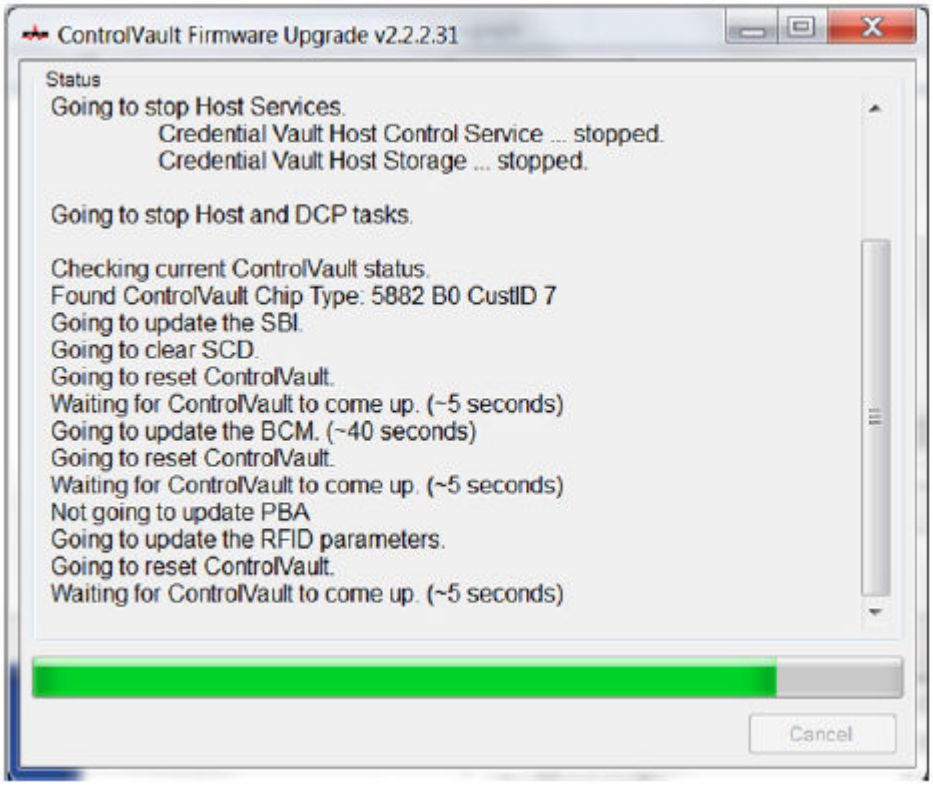
You may be asked to enter the admin password if upgrading from an older version of firmware. Enter **Broadcom** as the password and click **Enter** if presented with this dialog.

Several status messages display.

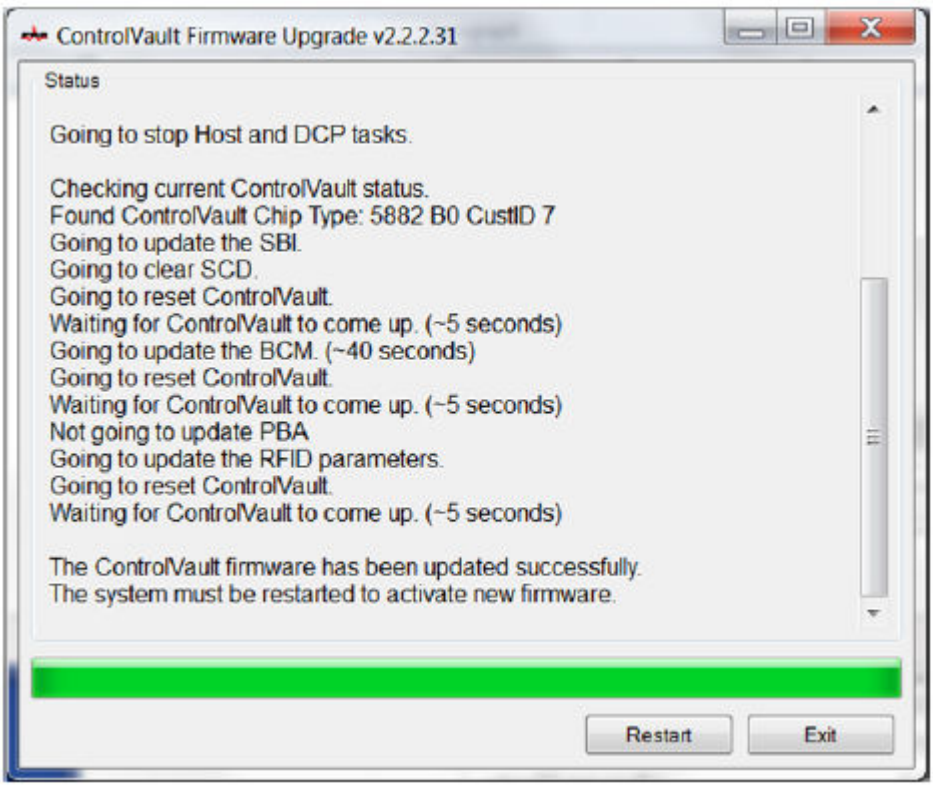



ControlVault Firmware Upgrade v2.2.2.31
Status
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.
Once started, do not interrupt process.
Going to stop Host Services.
Credential Vault Host Control Service ... stopped.
Credential Vault Host Storage ... stopped.
Going to stop 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)
Cancel


ControlVault Firmware Upgrade v2.2.2.31
Status
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)
Cancel



10 Click **Restart** to complete the firmware upgrade.



The update of the Dell ControlVault drivers and firmware is complete.

10

Glossary

Advanced Authentication - The Advanced Authentication product supports login with self-encrypting drives, SSO, and manages user credentials and passwords. In addition, Advanced Authentication can be used to access not only PCs, but any website, SaaS, or application. Once users enroll their credentials, Advanced Authentication allows use of those credentials to logon to the device and perform password replacement.

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 Remote 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 the Dell Encryption client applies policies to removable media and external storage devices.

Encryption External Media Access Code - This service within the Security Management Server/Security Management Server Virtual 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 removable media or external storage device.

Encryption Client - The Encryption client is the 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, the Encryption client 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 - a computer that is managed by Security Management Server/Security Management Server Virtual.

Encryption Sweep - An encryption sweep is the process of scanning the folders to be encrypted on a managed endpoint 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 will occur 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 will be 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 versus user), will trigger a sweep. In addition, toggling between encryption enabled and disabled will trigger 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 will be able to administer your enterprise more quickly and easily.

Threat Protection - The Threat Protection product is based on centrally managed policies that protect enterprise computers against security threats. Threat Protection consists of: - Malware Protection - Checks for viruses, spyware, unwanted programs, and other threats by automatically scanning items when accessed or based on schedules defined in policy. - Client Firewall - Monitors communication between the computer and resources on the network and the Internet and intercepts potentially malicious communications. - Web

Protection - Blocks unsafe websites and downloads from those websites during online browsing and searching, based on safety ratings and reports for websites.