Dell Data Protection | Encryption

Enterprise Edition Basic Installation Guide v8.13

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.**

Enterprise Edition Basic Installation Guide

2017 - 05

Rev. A02

Contents

1

Introduction

This guide details how to install and configure the application using the master installer. This guide gives basic installation assistance. See the *Advanced Installation Guide* if you need information about installing the child installers, EE Server/VE Server configuration, or information beyond basic assistance with the master installer.

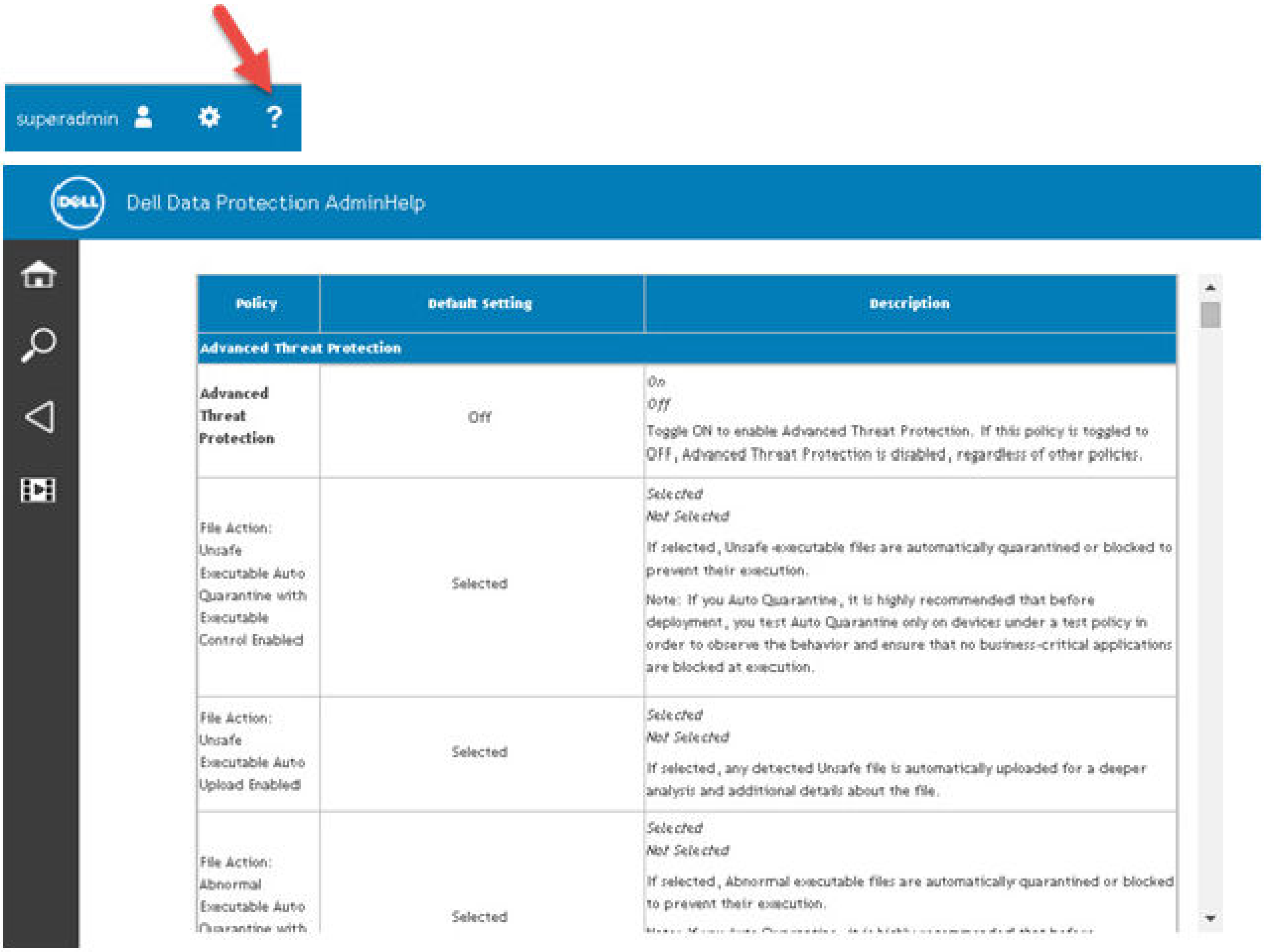
All policy information, and their descriptions are found in the AdminHelp.

Before You Begin

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

   - *DDP Enterprise Server Installation and Migration Guide*
   - *DDP Enterprise Server - Virtual Edition 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 EE Server/VE Server.



Dell Data Protection AdminHelp

Policy	Default Setting	Description
Advanced Threat Protection		
Advanced Threat Protection	Off	*On* *Off* Toggle ON to enable Advanced Threat Protection. If this policy is toggled to OFF, Advanced Threat Protection is disabled, regardless of other policies.
File Action: Unsafe Executable Auto Quarantine with Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Unsafe Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Unsafe file is automatically uploaded for a deeper analysis and additional details about the file.
File Action: Abnormal Executable Auto Quarantine with	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before

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 Data Protection product.

Additionally, online support for Dell Data Protection 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.

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 EE Server/VE Server 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 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 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

    If installing on non-Dell hardware, download updated drivers and firmware from that vendor's website. Installation instructions for ControlVault drivers are provided in Update Dell ControlVault Drivers and Firmware.

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 - Language Support

- The Encryption and BitLocker Manager clients are Multilingual User Interface (MUI) compliant and support 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)

- The SED and Advanced Authentication clients are Multilingual User Interface (MUI) compliant and support the following languages. UEFI Mode and Preboot Authentication are not supported in Russian, Traditional Chinese, or Simplified Chinese.

Language Support

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

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/SLN298707 or Contact Dell ProSupport for help.
- In-place operating system upgrade is not supported with the Encryption client installed. Uninstall and decrypt the Encryption client, upgrade to the new operating system, and then re-install the Encryption client.

  Additionally, 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 Microsoft Visual C++ 2012 Update 4 if not already installed on the computer.

Prerequisite
• Visual C++ 2012 Update 4 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 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
• VMware Workstation 5.5 and higher

> **NOTE:**
> UEFI is mode is not supported on Windows 7, Windows Embedded Standard 7, or Windows Embedded 8.1 Industry Enterprise.

External Media Shield (EMS) Operating Systems

- The following table details the operating systems supported when accessing media protected by EMS.

> **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 EMS.

> **NOTE:**
> Windows XP is supported when using EMS Explorer only.

Windows Operating Systems Supported to Access EMS-Protected Media (32- and 64-bit)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
• Windows 8: Enterprise, Pro, Consumer
• Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
• Windows 10: Education, Enterprise, Pro

Mac Operating Systems Supported to Access EMS-Protected Media (64-bit kernels)
• Mac OS X Yosemite 10.10.5
• Mac OS X El Capitan 10.11.6

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

- macOS Sierra 10.12.4 and 10.12.5

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*.

- SED Management is not supported with Server Encryption.

SED Client Prerequisites

- The master installer installs Microsoft Visual C++2010 SP1 **and** Microsoft Visual C++ 2012 Update 4 if not already installed on the computer.

Prerequisites

- Visual C++ 2010 SP1 or later Redistributable Package (x86 and x64)
- Visual C++ 2012 Update 4 or later Redistributable Package (x86 and x64)

SED Client Hardware

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 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.

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

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 Security Tools. Security Tools 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 Security Tools or uninstall it.
- The Security Tools One-time Password (OTP) feature requires that a TPM is present, enabled, and owned. OTP is not supported with TPM 2.0. To clear and set ownership of the TPM, see https://technet.microsoft.com.

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

Smart Cards

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

- CSP 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

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

Mobile Device Operating Systems

- The following mobile operating systems are supported with Security Tools One-time Password feature.

Android Operating Systems

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS Operating Systems

- iOS 7.x
- iOS 8.x

Windows Phone Operating Systems

- Windows Phone 8.1
- Windows 10 Mobile

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 is not supported with Server Encryption.

BitLocker Manager Client Prerequisites

- The master installer installs Microsoft Visual C++2010 SP1 **and** Microsoft Visual C++ 2012 Update 4 if not already installed on the computer.

Prerequisites

- Visual C++ 2010 SP1 or later Redistributable Package (x86 and x64)
- Visual C++ 2012 Update 4 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
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-bit)
- Windows Server 2012
- 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.
- 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 *EMS Help* to learn how the features of External Media Shield. Access the help from <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS.
  - See the *Security Tools Help* to learn how to use the features of Advanced Authentication. Access the help from <Install dir>: \Program Files\Dell\Dell Data Protection\Security Tools \Help.
- Users should update their policies by right-clicking the Dell Data Protection 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

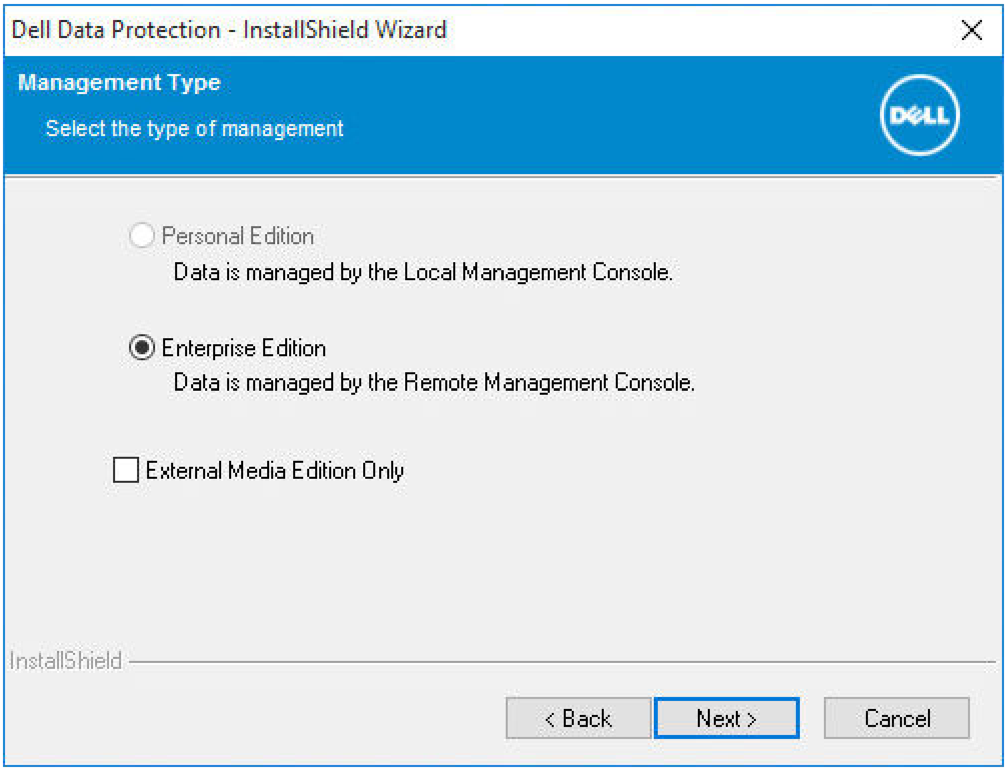
  - Install by Command Line Using the Master Installer

Install Interactively Using the Master Installer

- The master installer can be located at:
  - **From support.dell.com** - If needed, Obtain the Software from support.dell.com and then Extract the Child Installers from the Master Installer.
  - **From Your Dell FTP Account** - Locate the installation bundle at DDP-Enterprise-Edition-8.x.x.xxx.zip
- Use these instructions to install Dell Enterprise Edition interactively using the master installer. This method can be used to install the suite of products on one computer at a time.

1. Locate **DDPSetup.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. Select **Enterprise Edition** and click **Next.**

   Select the External Media Edition only check box if you intend to install External Media Edition only



Dell Data Protection - InstallShield Wizard

Management Type

Select the type of management

○ Personal Edition

Data is managed by the Local Management Console.

● Enterprise Edition

Data is managed by the Remote Management Console.

□ External Media Edition Only

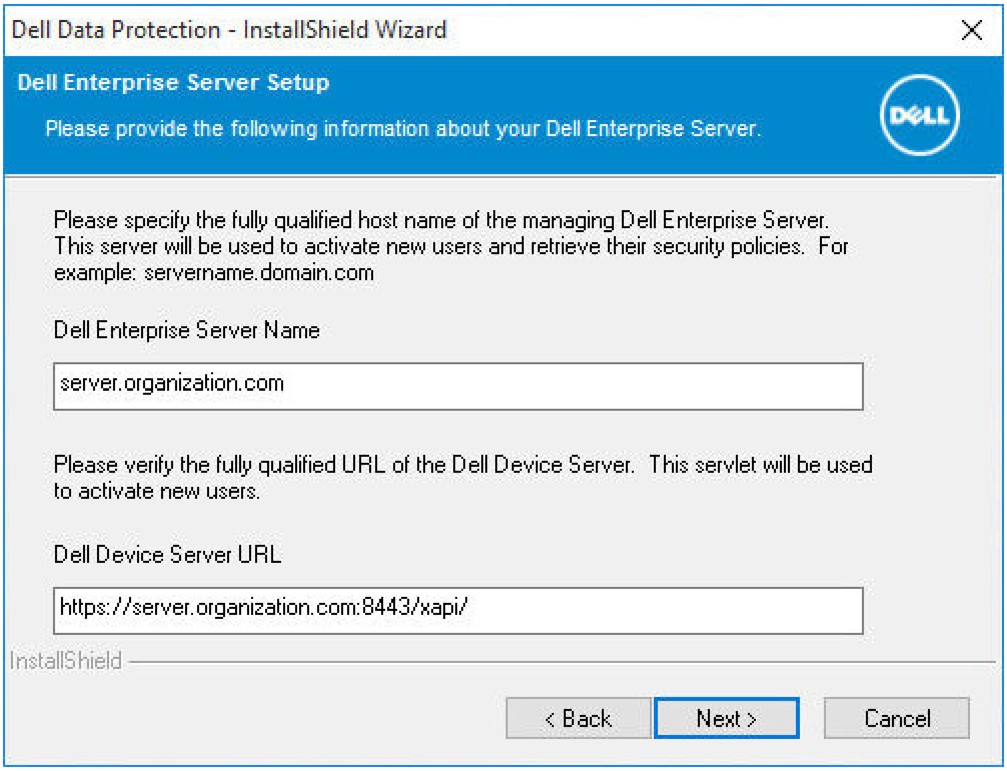
6 In the **Enterprise Server Name** field, enter the fully qualified host name of the EE Server/VE Server that will manage the target user, such as server.organization.com.

In the **Device Server URL** field, enter the URL of the Device Server (Security Server) with which the client will communicate.

If your EE Server is pre-v7.7, the format is https://server.organization.com:**8081**/xapi.

If your EE Server is v7.7 or later, the format is https://server.organization.com:**8443**/xapi**/** (including trailing forward slash).

Click **Next.**


Dell Data Protection - InstallShield Wizard

Dell Enterprise Server Setup

Please provide the following information about your Dell Enterprise Server.

Please specify the fully qualified host name of the managing Dell Enterprise Server. This server will be used to activate new users and retrieve their security policies. For example: servername.domain.com

Dell Enterprise Server Name

server.organization.com

Please verify the fully qualified URL of the Dell Device Server. This servlet will be used to activate new users.

Dell Device Server URL

https://server.organization.com:8443/xapi/

7 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.

8 Select the components to be installed.

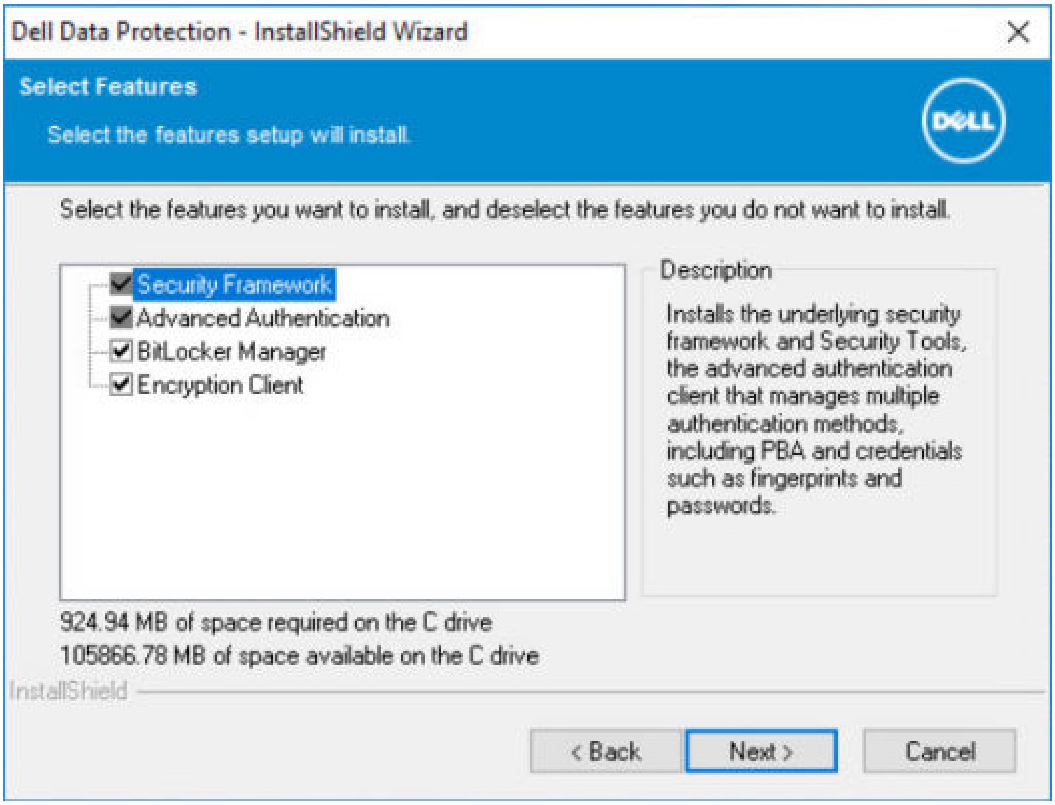
Security Framework installs the underlying security framework and Security Tools, the advanced authentication client that manages multiple authentication methods, including PBA and credentials such as fingerprints and passwords.

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.

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.

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


Dell Data Protection - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

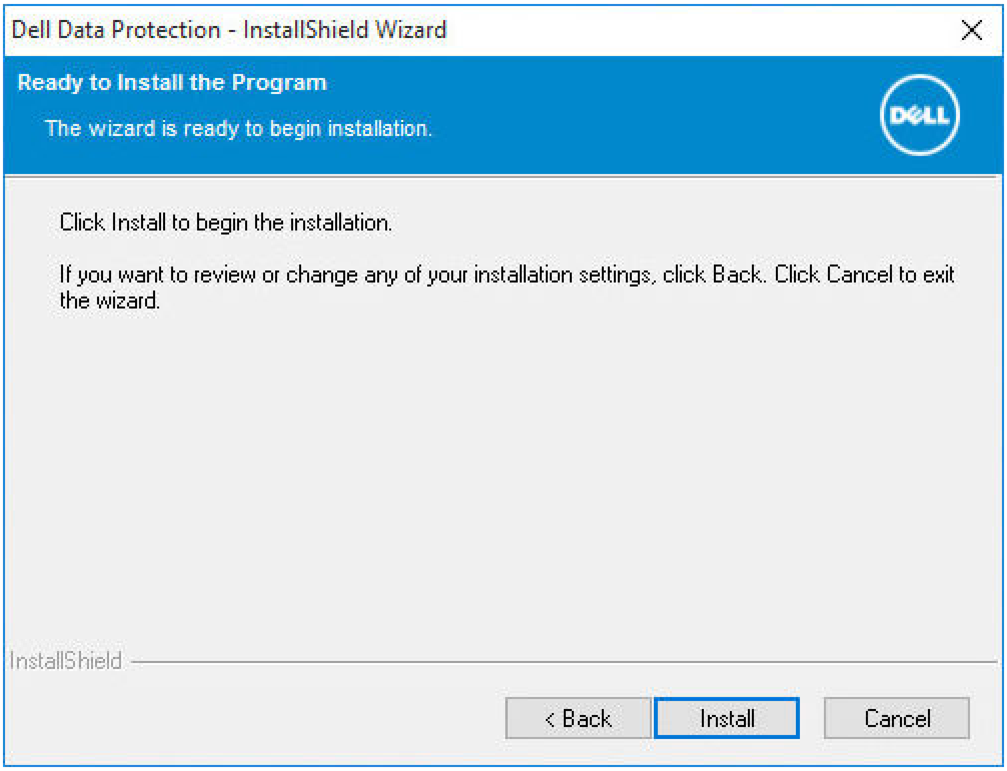
- ☑ Security Framework
- ☑ Advanced Authentication
- ☑ BitLocker Manager
- ☑ Encryption Client

Description

Installs the underlying security framework and Security Tools, the advanced authentication client that manages multiple authentication methods, including PBA and credentials such as fingerprints and passwords.

924.94 MB of space required on the C drive
105866.78 MB of space available on the C drive

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


Dell Data Protection - InstallShield Wizard

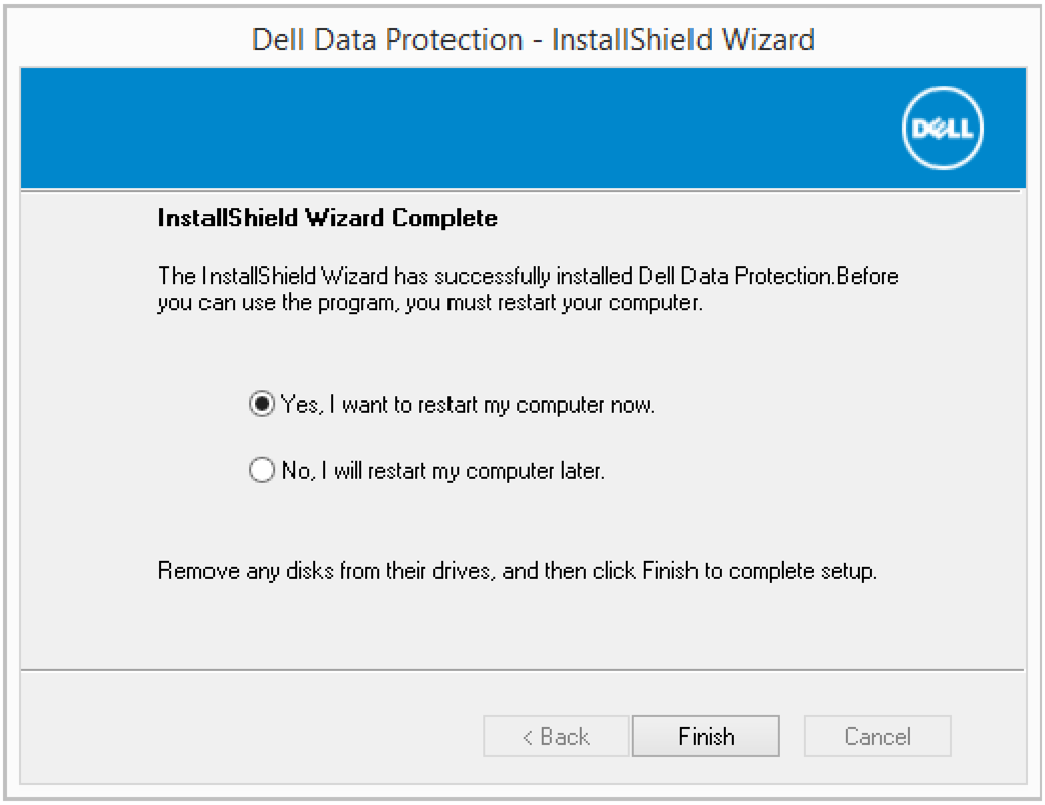
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Dell Data Protection.Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Installation is complete.

Install by Command Line Using the Master Installer

- The switches must be specified first in a command line installation the switches must be specified first. 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 master installer.

Switch	Description
-y -gm2	Pre-extraction of 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 DDPSetup.exe

Parameters

- The following table describes the parameters that can be used with the master installer.

Parameter	Description
SUPPRESSREBOOT	Suppresses the automatic reboot after the installation completes. Can be used in SILENT mode.
SERVER	Specifies the URL of the EE Server/VE Server.
InstallPath	Specifies the path for the installation. Can be used in SILENT mode.

Parameter	Description

FEATURES	Specifies the components that can be installed in SILENT mode.
	DE = Drive Encryption (Encryption client)
	EME = External Media Edition only
	BLM = BitLocker Manager
	SED = Self-encrypting Drive 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 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 EE Server/VE Server.

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

- This example installs SED Management and External Media Edition with the 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 EE Server/VE Server.

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

- This example installs SED Management with the 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 EE Server/VE Server.

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

- This example installs SED Management with the 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 EE Server/VE Server.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=SED\""
```

- This example installs the Encryption client and BitLocker Manager (without the SED Management plugin), with the 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 EE Server/VE Server.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```

- This example installs BitLocker Manager (with the SED Management plugin) and External Media Edition, with the 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 EE Server/VE Server.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
SUPPRESSREBOOT=1\""
```

- This example installs BitLocker Manager (without the SED Management plugin) and External Media Edition, with the 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 EE Server/VE Server.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
SUPPRESSREBOOT=1\""
```

4

Uninstall Using the Master Installer

- Each component must be uninstalled separately, followed by uninstallation of the 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 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.

  b Uninstall SED and Advanced Authentication Clients.

  c Uninstall BitLocker Manager Client.
- Proceed to Uninstall the Master Installer.

Uninstall the 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 master installer.

  ```
  "DDPSetup.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 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 Encryption and Server 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 and EME Shields update the EE Server/VE Server to change the status to *Unprotected* at the beginning of a Shield uninstall process. However, in the event that the client cannot contact the EE Server/VE Server, 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 EE 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 EE Server for instructions. No prior action is needed if the client to uninstall is activated against a VE Server, as VE Server 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 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

Parameter	Selection
Required Properties	
DA_SERVER	FQHN for the EE Server hosting the negotiate session.
DA_PORT	Port on the EE Server for request (default is 8050).
SVCPN	Username in UPN format that the Key Server Service is logged on as on the EE 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 EE 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 EE 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 External Media Edition

Once extracted from the master installer, the Encryption client installer can be located at C:\extracted\Encryption\DDPE_XXbit_setup.exe.

Command Line Uninstallation

Run a command line similar to the following:

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

Reboot the computer when finished.

Uninstall SED and Advanced Authentication Clients

- Network connection to the EE Server/VE Server 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 EE Server/VE Server 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\Security Tools \EMAgent_XXbit_setup.exe.
- Once extracted from the master installer, the SED client installer can be located at C:\extracted\Security Tools\Authentication\<x64/ x86>\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.

Then:

- The following example silently uninstalls the Advanced Authentication client.

```
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 master installer, the BitLocker client installer can be located at C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- The following example silently uninstalls the BitLocker Manager client.

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

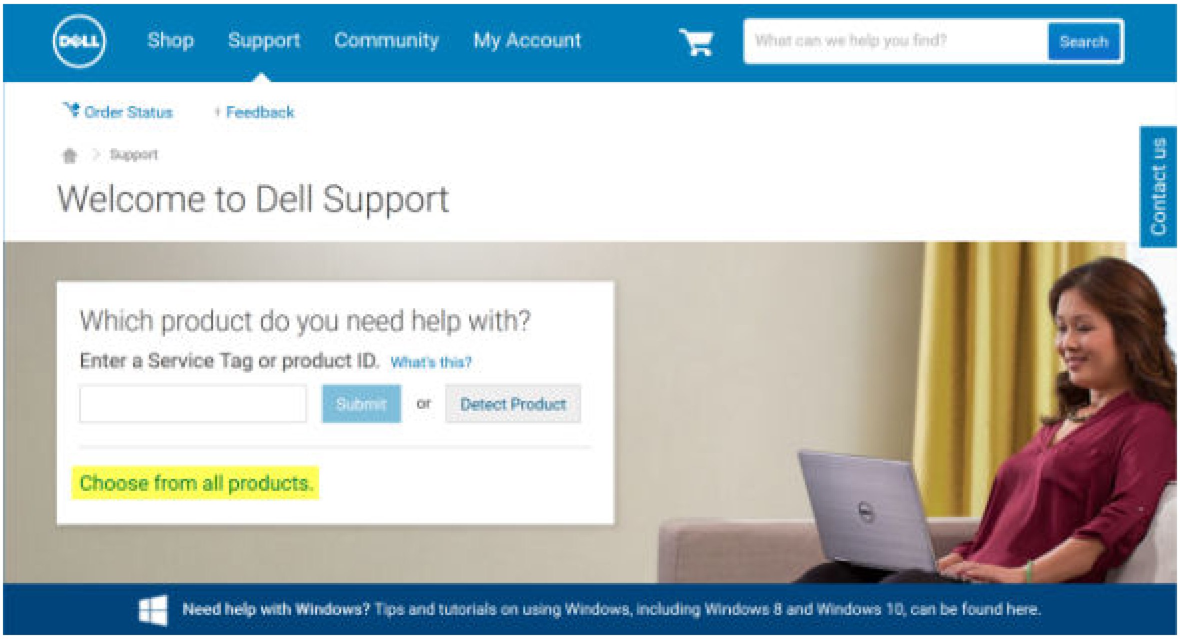
Reboot the computer when finished.

Download the Software

This section details obtaining the software from dell.com/support. If you already have the software, you can skip this section.

Go to dell.com/support to begin.

1 On the Dell Support webpage, select **Choose from all products**.



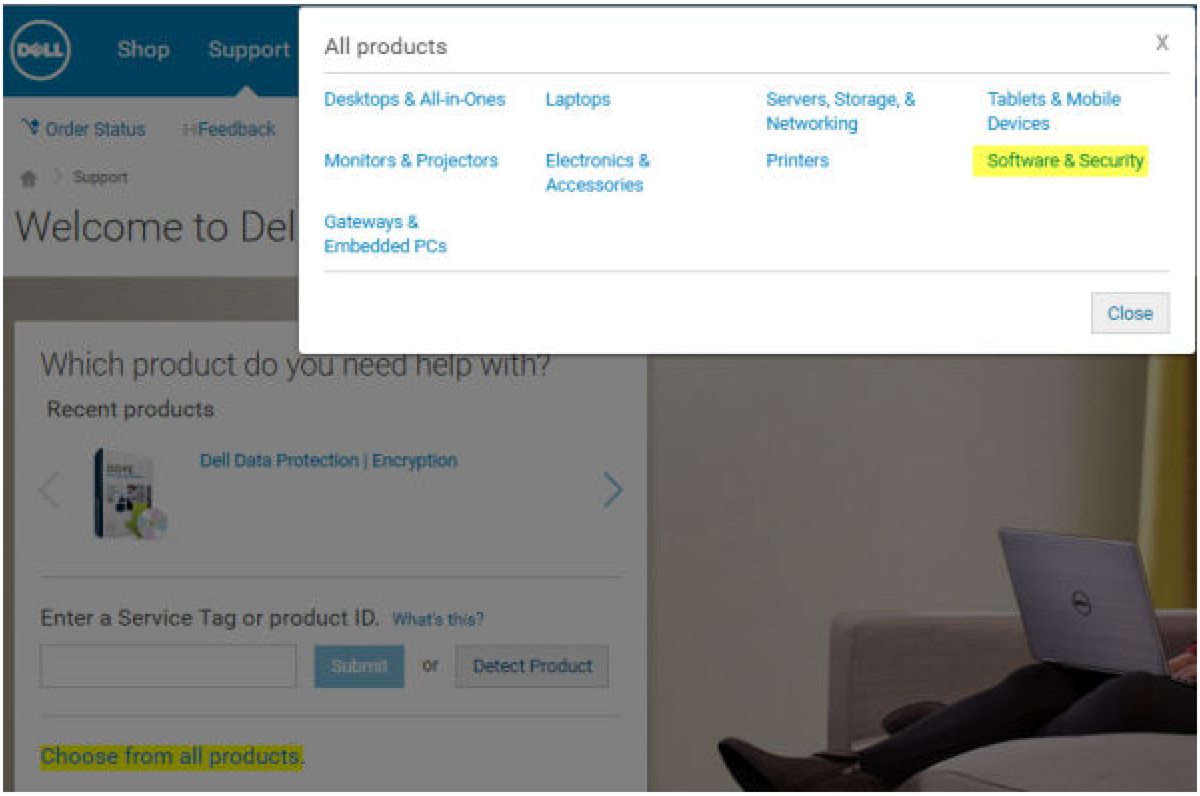
Welcome to Dell Support

Which product do you need help with?

Enter a Service Tag or product ID. What's this?

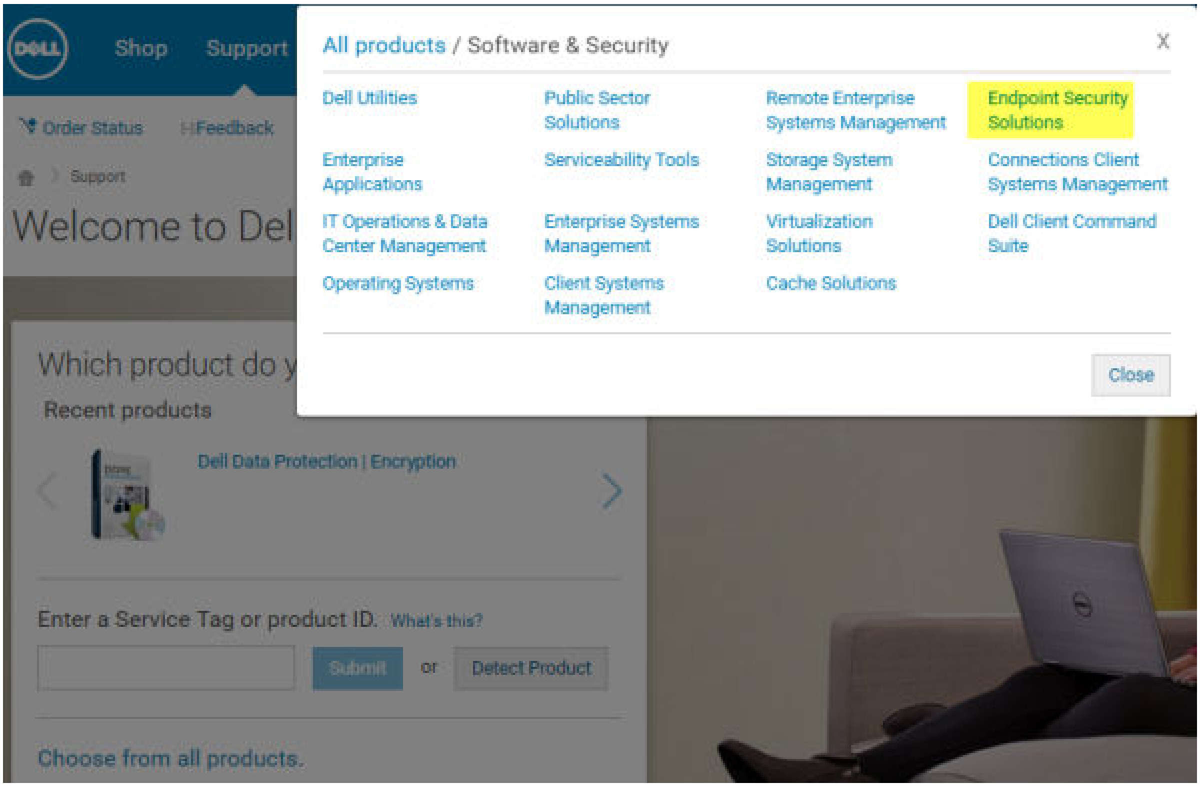
Need help with Windows? Tips and tutorials on using Windows, including Windows 8 and Windows 10, can be found here.

2 Select **Software & Security** from the list of products.



3 Select **Endpoint Security Solutions** in the *Software and Security* section.

After this selection has been made once, the website will remember.


Shop
Support
Order Status
Feedback
Support
Welcome to Del
All products / Software & Security
X
Dell Utilities
Public Sector Solutions
Remote Enterprise Systems Management
Endpoint Security Solutions
Enterprise Applications
Serviceability Tools
Storage System Management
Connections Client Systems Management
IT Operations & Data Center Management
Enterprise Systems Management
Virtualization Solutions
Dell Client Command Suite
Operating Systems
Client Systems Management
Cache Solutions
Close
Which product do y
Recent products
Dell Data Protection | Encryption
Enter a Service Tag or product ID. What's this?
Submit
or
Detect Product
Choose from all products.

4 Select the Dell Data Protection product.

Examples:

Dell Encryption

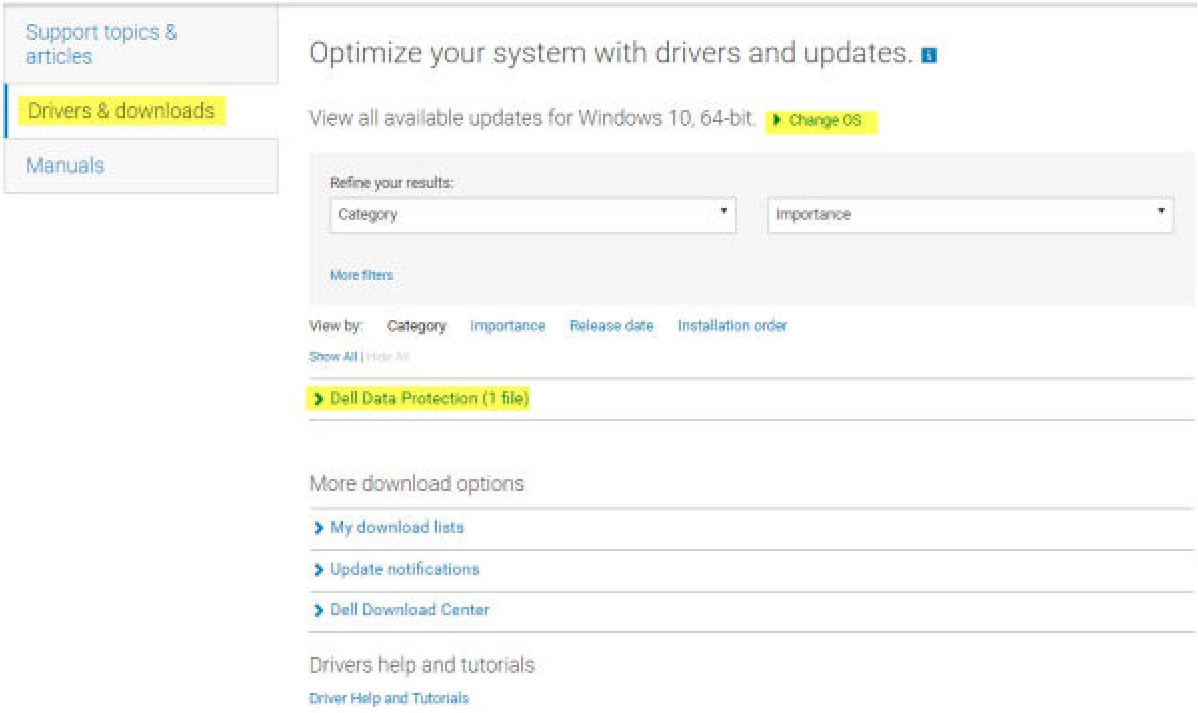
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Select **Drivers & downloads**.

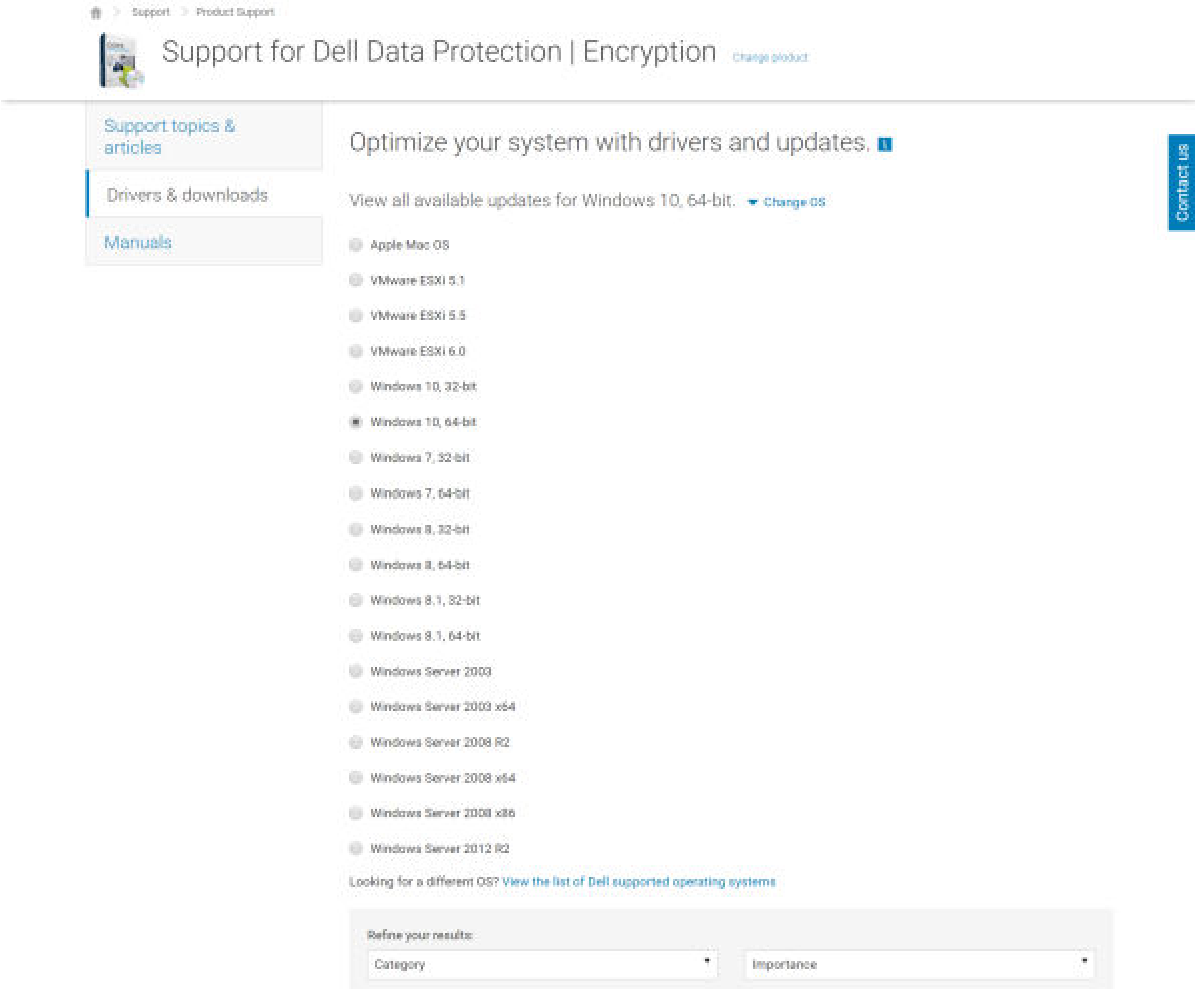
6 Select the desired client operating system type.

7 Select **Dell Data Protection (4 files)** in the matches. This is only an example, so it will likely look slightly different. For example, there may not be 4 files to choose from.



Optimize your system with drivers and updates.

View all available updates for Windows 10, 64-bit.



Support > Product Support

Support for Dell Data Protection | Encryption Change product

Support topics & articles

Drivers & downloads

Manuals

Optimize your system with drivers and updates.

View all available updates for Windows 10, 64-bit. Change OS

○ Apple Mac OS
○ VMware ESXi 5.1
○ VMware ESXi 5.5
○ VMware ESXi 6.0
○ Windows 10, 32-bit
● Windows 10, 64-bit
○ Windows 7, 32-bit
○ Windows 7, 64-bit
○ Windows 8, 32-bit
○ Windows 8, 64-bit
○ Windows 8.1, 32-bit
○ Windows 8.1, 64-bit
○ Windows Server 2003
○ Windows Server 2003 x64
○ Windows Server 2008 R2
○ Windows Server 2008 x64
○ Windows Server 2008 x86
○ Windows Server 2012 R2

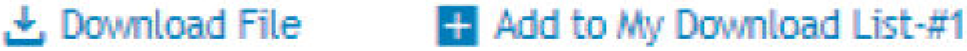
Looking for a different OS? View the list of Dell supported operating systems

Refine your results:

Category

Importance

8 Select **Download File** or A**dd to My Download List #XX**.



Extract the Child Installers from the 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.

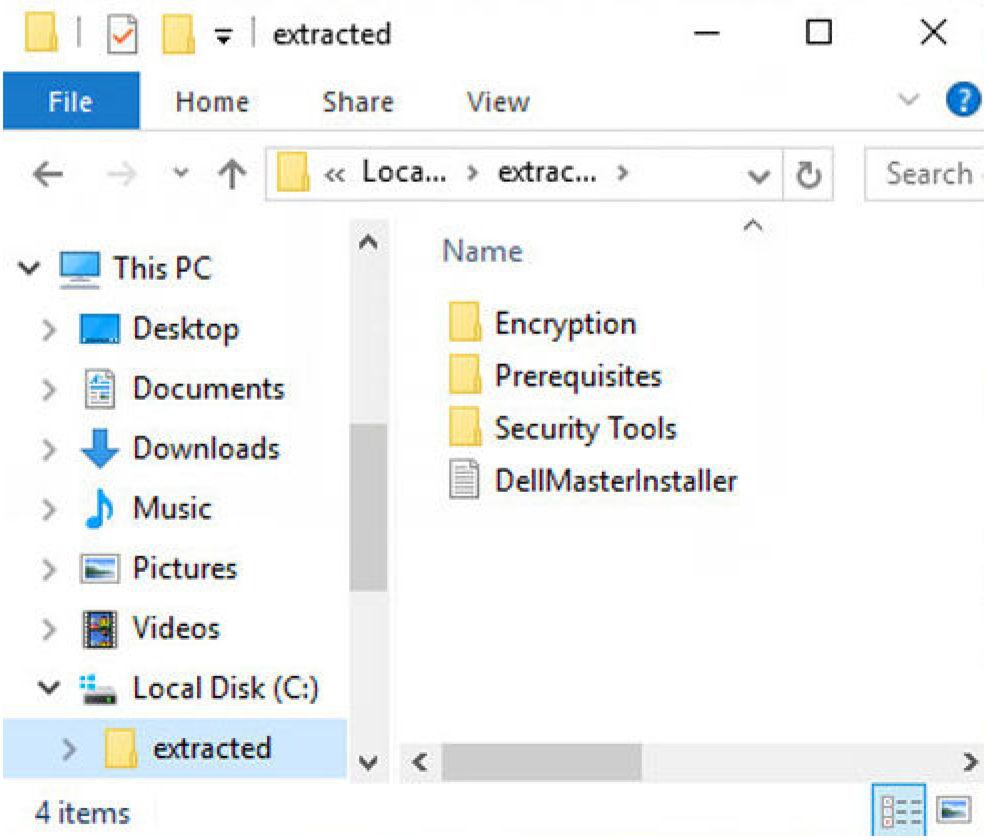
1 From the Dell installation media, copy the **DDPSetup.exe** file to the local computer.

2 Open a command prompt in the same location as the **DDPSetup.exe** file and enter:

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

The extraction path cannot exceed 63 characters.

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



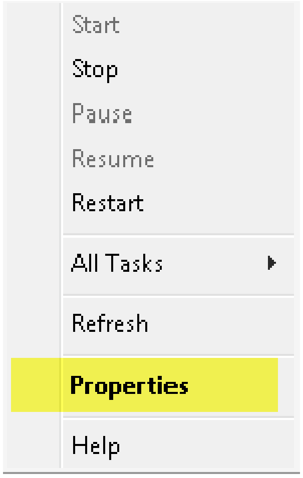
8

Configure Key Server for Uninstallation of Encryption Client Activated Against EE Server

- This section explains how to configure components for use with Kerberos Authentication/Authorization when using an EE Server. The VE Server 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 VE Server does not use the Key Server, typical uninstallation is affected. When an Encryption client that is activated against a VE Server 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 EE Server, navigate to the Services panel (Start > Run... > services.msc > OK).
2. Right-click Key Server and select **Properties**.

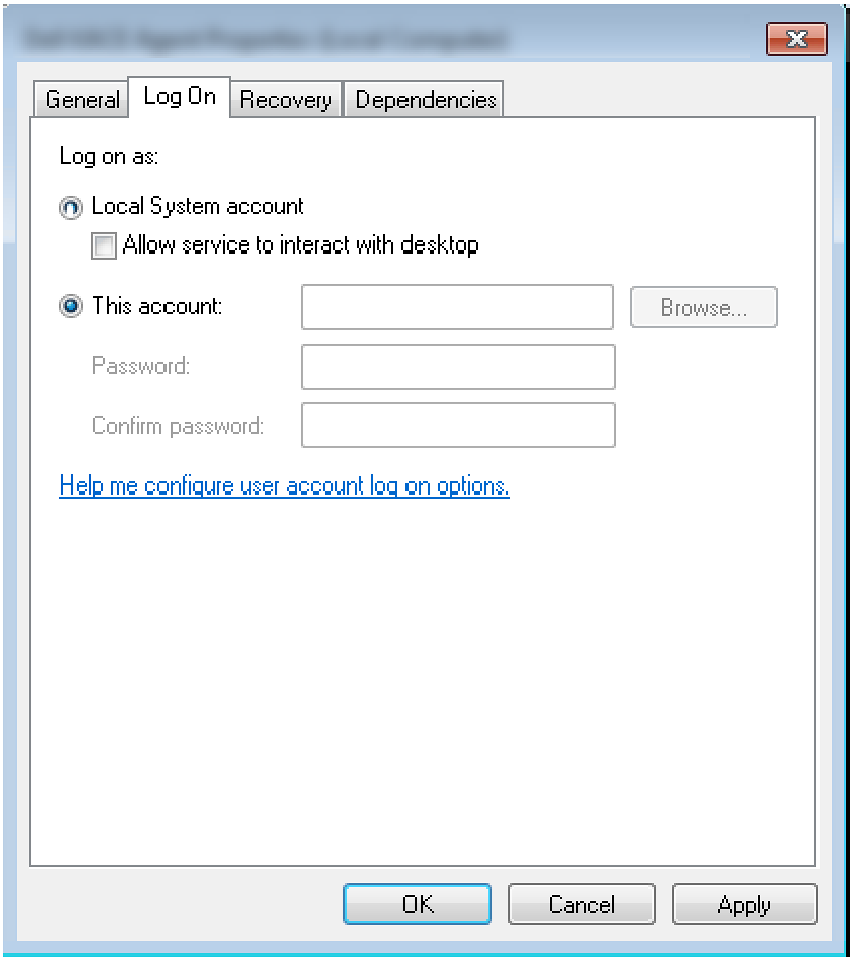


3. Select the Log On tab and select the **This account:** option.

   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**



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account:

Password:

Confirm password:

Help me configure user account log on options.

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 EE 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 EE 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

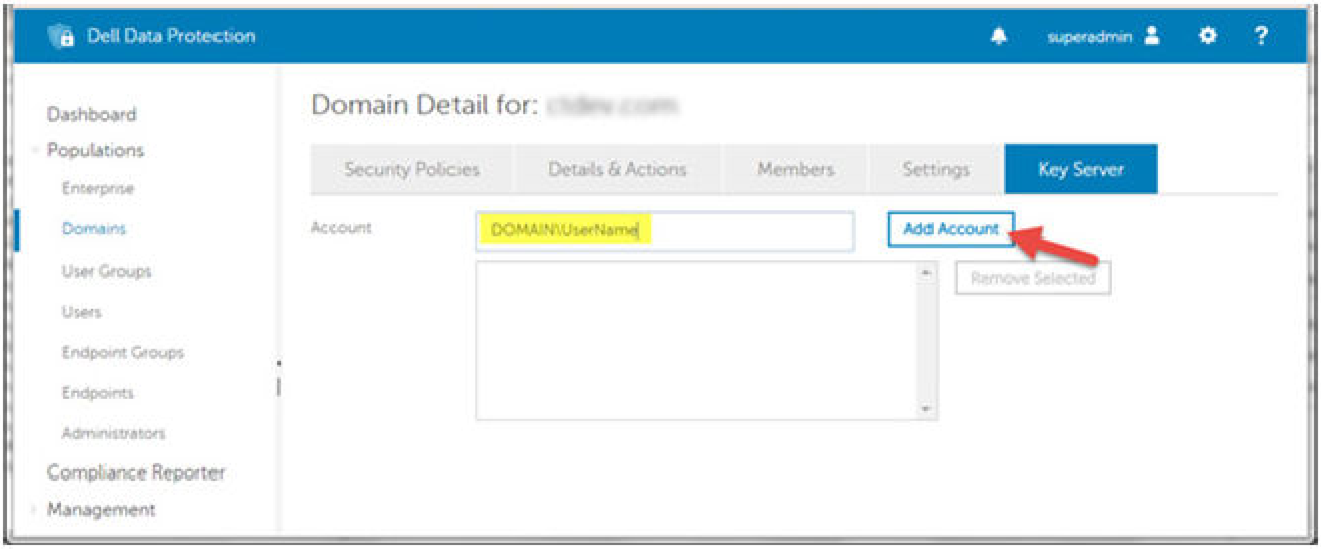
1 If needed, log on to the Remote Management Console.

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**.



Domain Detail for: [redacted]

Account DOMAIN\UserName

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.

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 EE Server/VE Server.
- 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/. If your EE Server is pre-v7.7, the format is https://deviceserver.domain.com:8081/xapi (different port number, without the trailing slash).

   Dell Admin: Name of the administrator with forensic administrator credentials (enabled in the Remote Management Console), such as jdoe

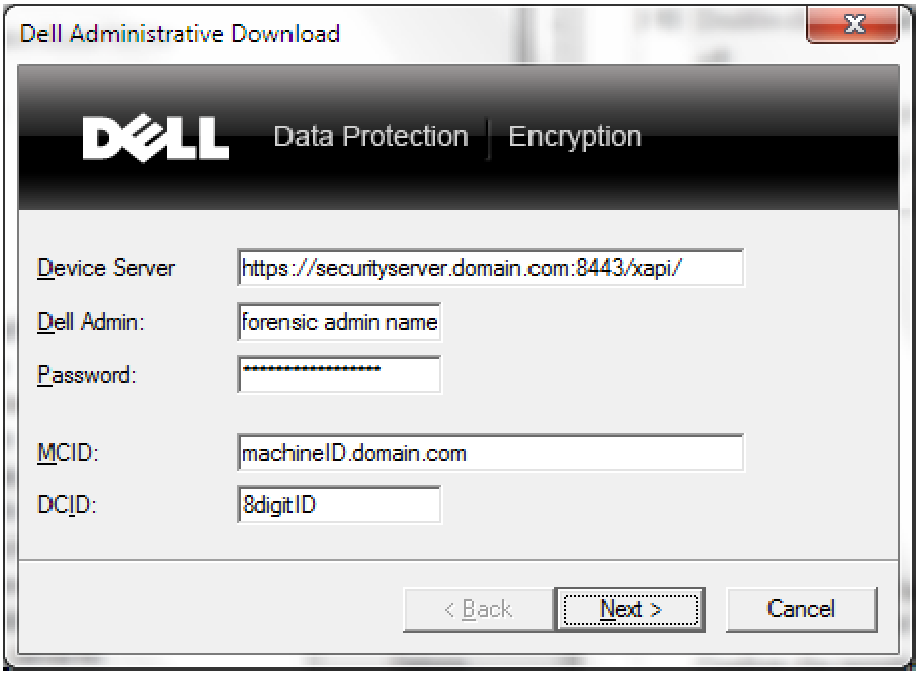
   Password: Forensic administrator password

   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**.



Device Server: https://securityserver.domain.com:8443/xapi/

Dell Admin: forensic admin name

Password: ******************

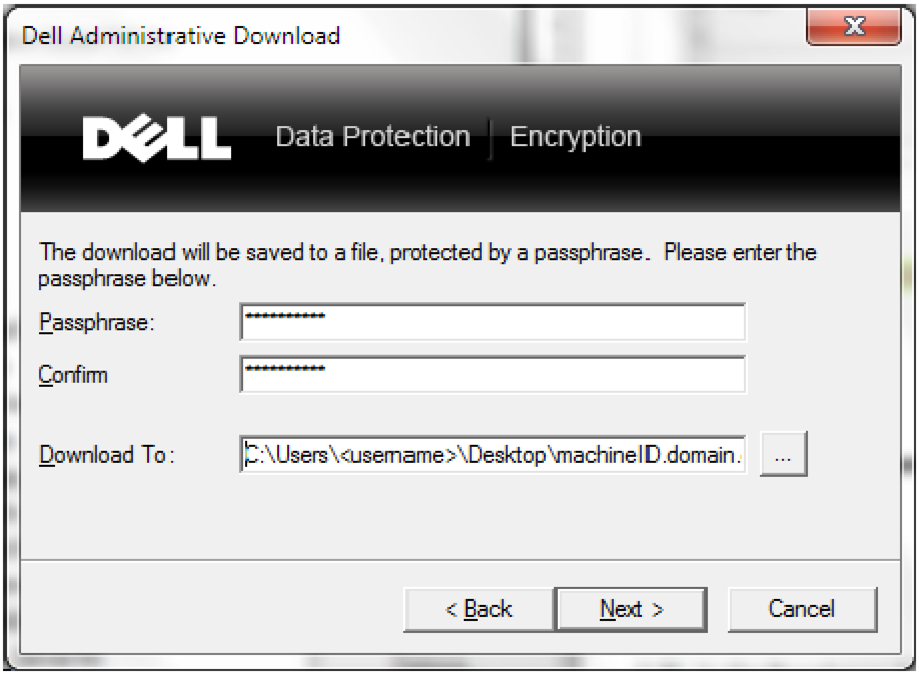
MCID: machineID.domain.com

DCID: 8digitID

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**.



The download will be saved to a file, protected by a passphrase. Please enter the passphrase below.

Passphrase: ************

Confirm ************

Download To: C:\Users\<username>\Desktop\machineID.domain.

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

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

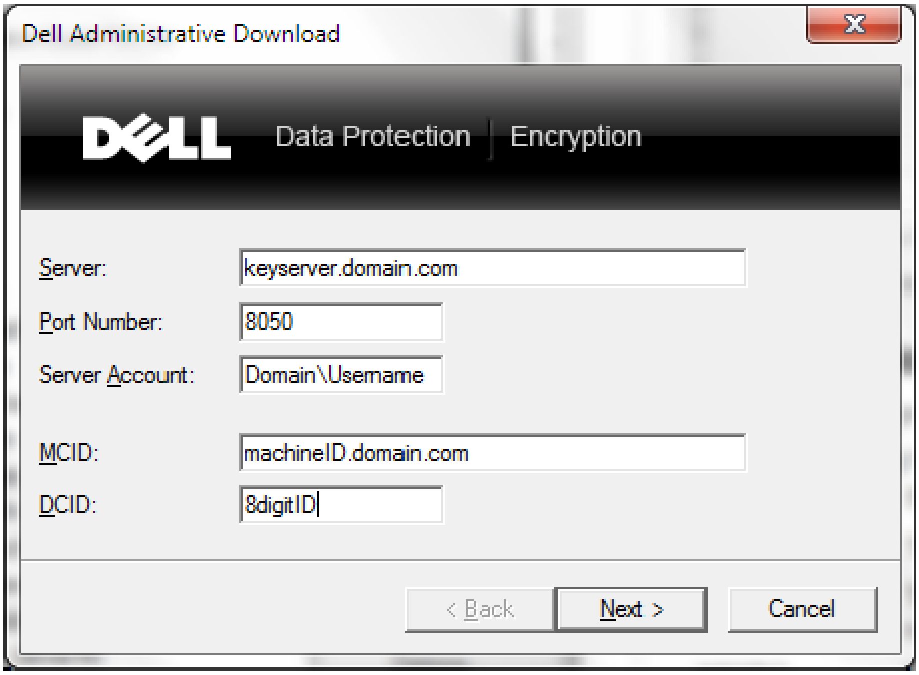
Server Account: The domain user the Key Server is running as. The format is domain\username. The domain user running the utility must be authorized to perform the download from the Key Server

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**.



Server: keyserver.domain.com

Port Number: 8050

Server Account: Domain\Username

MCID: machineID.domain.com

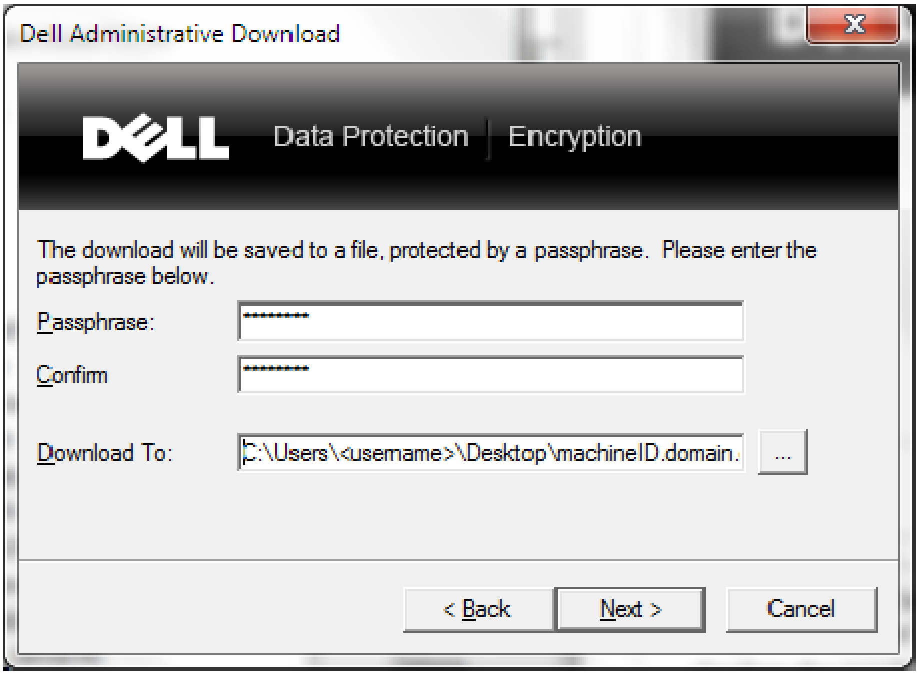
DCID: 8digitID

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**.



Dell Administrative Download

The download will be saved to a file, protected by a passphrase. Please enter the passphrase below.

Passphrase: *********

Confirm *********

Download To: C:\Users\<username>\Desktop\machineID.domain.

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

4 Click **Finish** when complete.

10

Troubleshooting

All Clients - Troubleshooting

- **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.
- See *Dell Data Protection | Security Tools Compatibility* 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.

Encryption and Server Encryption Client Troubleshooting

Upgrade to the Windows 10 Anniversary Update

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

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 the 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 admin rights.

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

Possible Solution**:** In the Activation dialog, enter credentials for a domain Administrator and ensure that they are in UPN format.

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 DDP Security 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 DDP 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.

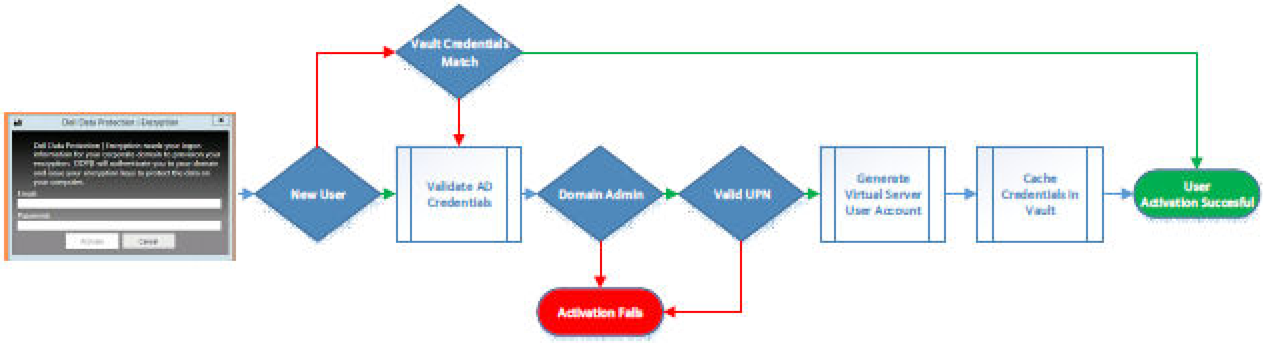
Error Message: Activation failed because the Server is unable to support this request.

Possible Solutions

- Server Encryption cannot be activated against a legacy server; the DDP Server version must be version 9.1 or higher. If necessary, upgrade your DDP Server to version 9.1 or higher.
- Check the DDP 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 Server Encryption 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 box displays when one of the two following things happens:

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

    The initial activation process is as follows:

1. The user logs in.
2. Detecting a new (unmanaged) user, the Activate dialog displays. The user clicks **Cancel**.

3 The user opens the Server Encryption's About box to confirm that it is running in Server mode.

4 The user right-clicks the Encryption client icon in the system tray 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 Server Encryption from being rolled out to other server environments that do not support it. To disable the requirement for Domain Administrator credentials, see Before You Begin.

6 DDP 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 DDP Server creates a new user account for the virtual server user, and stores the credentials in the DDP Server's vault.

The **virtual server user account** is for the exclusive use of the Encryption client. It will be 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 part of activation, Authentication and Device Activation.

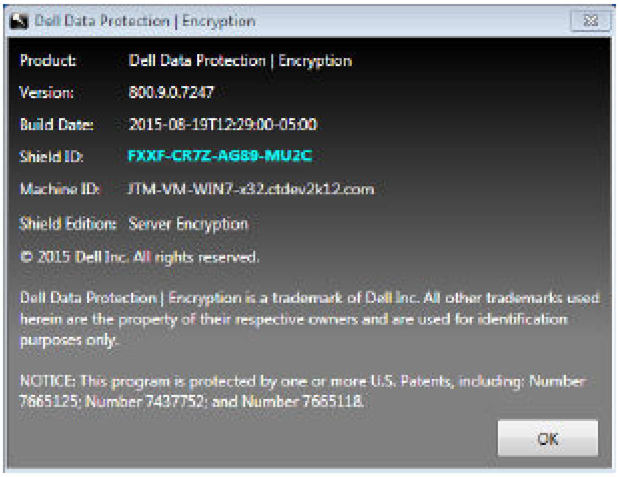
Troubleshooting Authentication and Device Activation

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, Server Encryption automatically logs in as the virtual server user, requesting the Machine key from the DDP Enterprise Server. This takes place even before any user can log in.

- Open the About dialog to confirm that Server Encryption is authenticated and in Server mode.



Product: Dell Data Protection | Encryption

Version: 800.9.0.7247

Build Date: 2015-08-19T12:29:00-05:00

Shield ID: FXXF-CR7Z-AG89-MU2C

Machine ID: JTM-VM-WIN7-x32.ctdev2k12.com

Shield Edition: Server Encryption

© 2015 Dell Inc. All rights reserved.

Dell Data Protection | Encryption is a trademark of Dell Inc. All other trademarks used herein are the property of their respective owners and are used for identification purposes only.

NOTICE: This program is protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

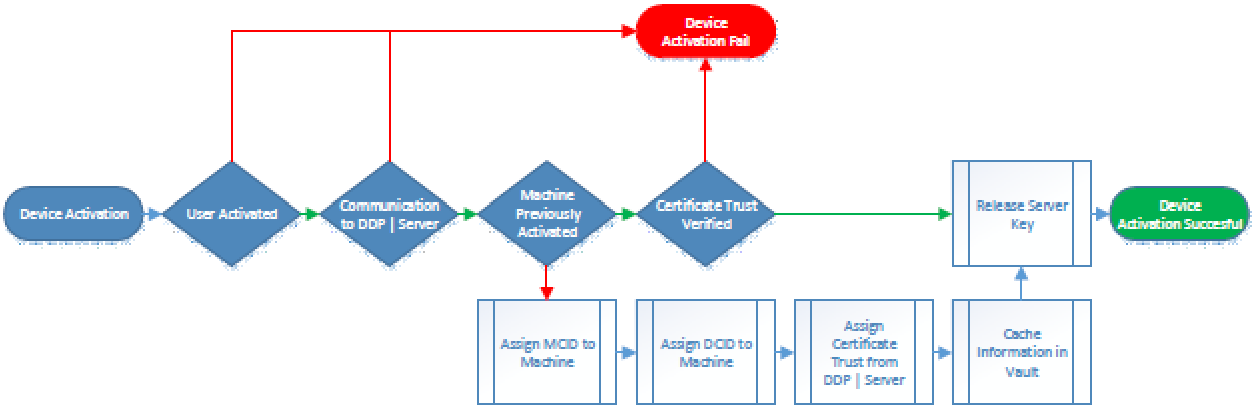
- If the Shield ID is red, encryption has not yet been activated.
- In the Remote Management Console, the version of a server with Server Encryption installed is listed as *Shield for Server*.
- If the Machine key retrieval fails due to a network failure, Server Encryption registers for network notifications 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.

    Refer to AdminHelp, available in the Remote Management Console, for details on the *Retry Interval Upon network Failure* policy.

Authentication and Device Activation Process

The following diagram illustrates successful authentication and device activation.


Device Activation Fail
Device Activation
User Activated
Communication to DDP | Server
Machine Previously Activated
Certificate Trust Verified
Release Server Key
Device Activation Succesful
Assign MCID to Machine
Assign DCID to Machine
Assign Certificate Trust from DDP | Server
Cache Information in Vault

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 DDP Server:

- If the computer has not previously device-activated, the DDP Server assigns the computer an MCID, a DCID, and a trust certificate, and stores all of the information in the DDP Server's vault.
- If the computer had previously been device-activated, the DDP Server verifies the trust certificate.

3 After the DDP 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.

EMS 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 Port Control System - Storage Class: External Drive Control policy. If you intend to set the EMS 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

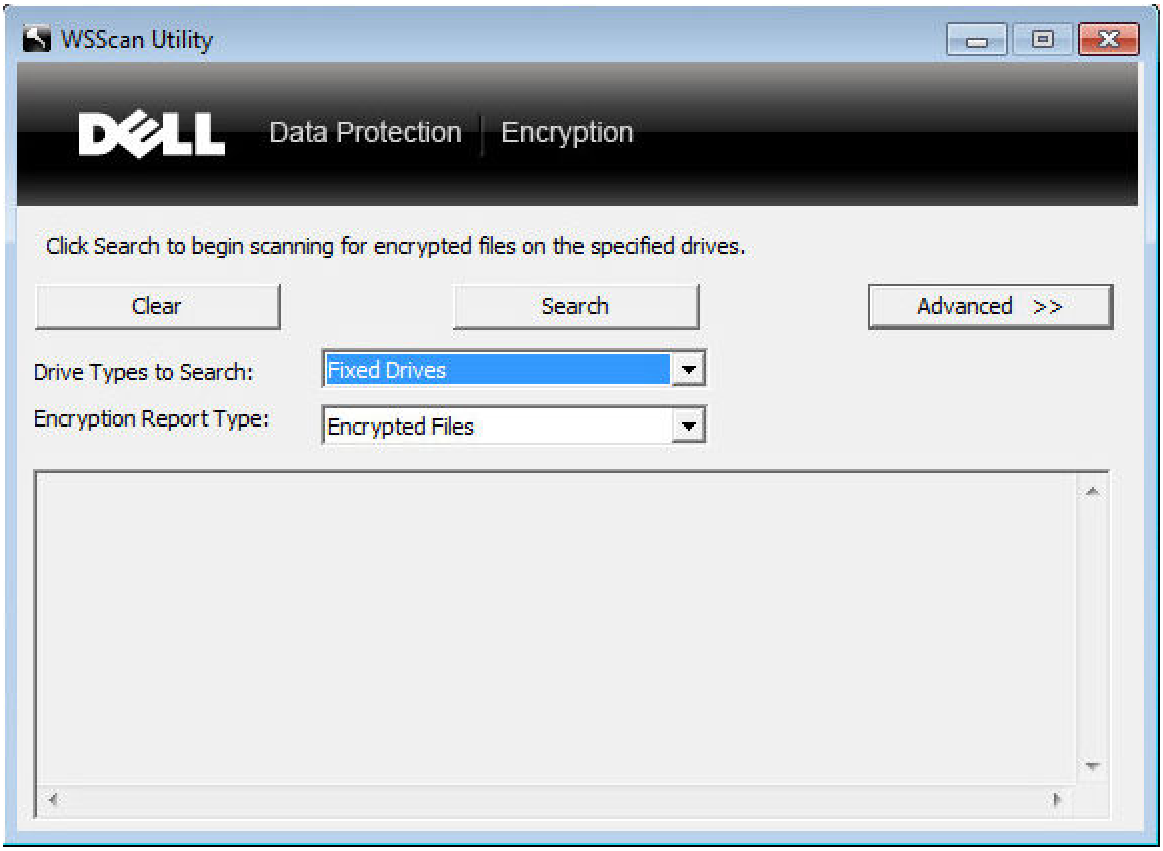
- Set EMS Encrypt External Media = True.
- Set EMS Exclude CD/DVD Encryption = False.
- Set Subclass Storage: Optical Drive Control = UDF Only.

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/ DVDROM*s.
5. Select the desired Encryption Report Type from the drop-down menu: *Encrypted FIles*, *Unencrypted FIles*, *All FIles*, or *Unencrypted FIles in Violation*:
   - *Encrypted FIles* - 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 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 Search to begin scanning for encrypted files on the specified drives.

Drive Types to Search: Fixed Drives

Encryption Report Type: Encrypted Files

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.

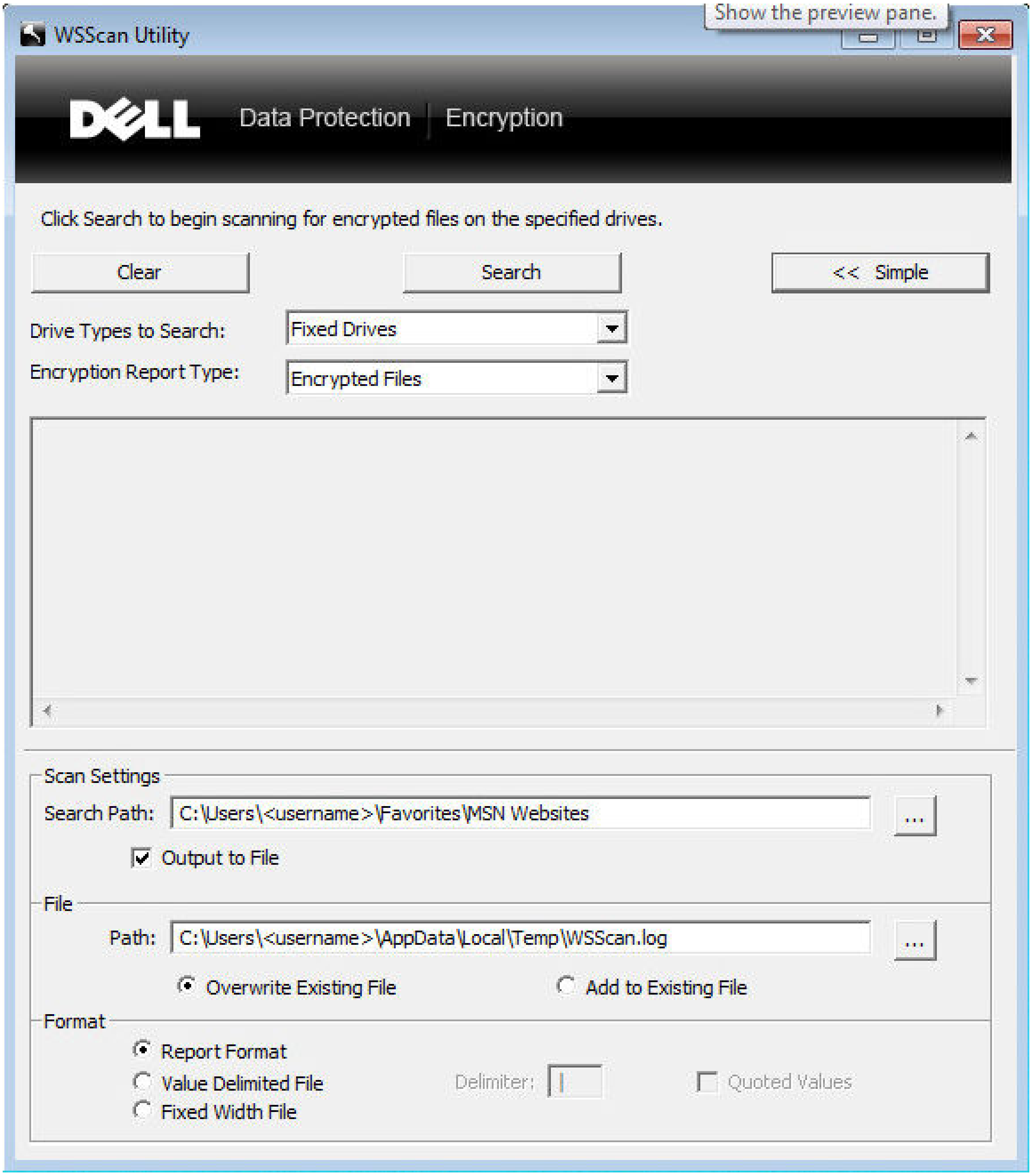
5 Select **Add to Existing File** if you do not want to overwrite any existing WSScan output files.

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.



Click Search to begin scanning for encrypted files on the specified drives.

Drive Types to Search: Fixed Drives

Encryption Report Type: Encrypted Files

Scan Settings

Search Path: C:\Users\<username>\Favorites\MSN Websites

☑ Output to File

File

Path: C:\Users\<username>\AppData\Local\Temp\WSScan.log

● Overwrite Existing File ○ Add to Existing File

Format

● Report Format

○ Value Delimited File Delimiter: | □ Quoted Values

○ Fixed Width File

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
```

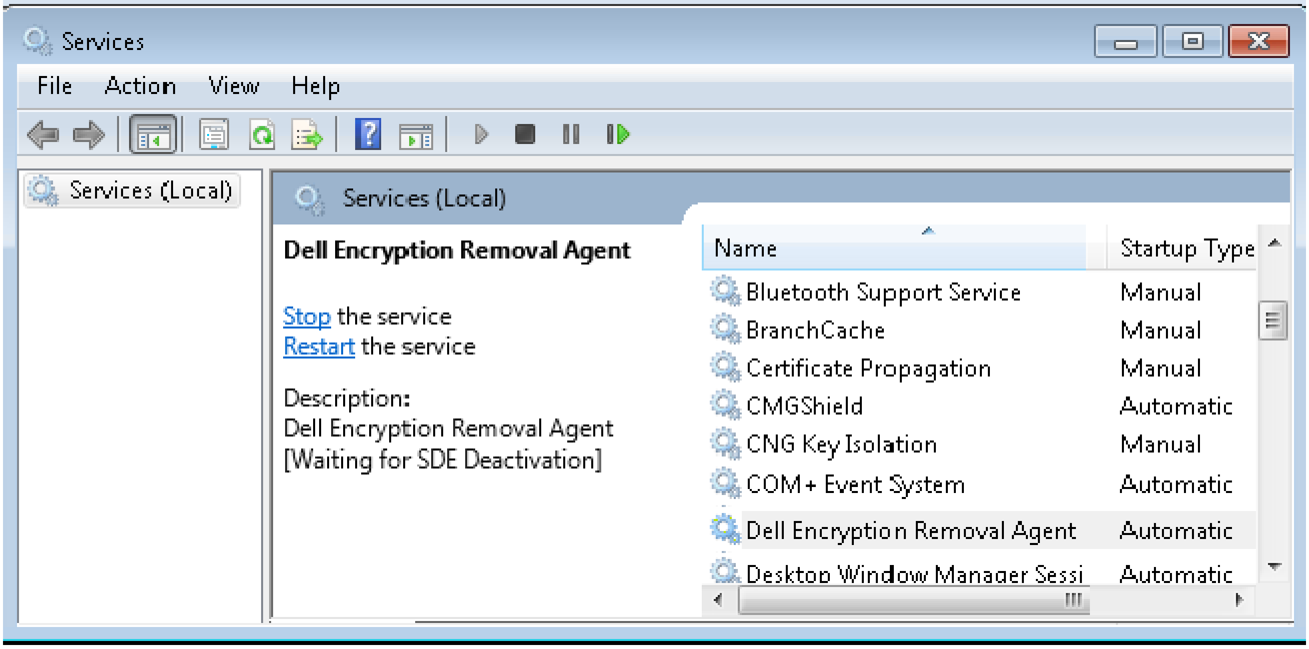
Output	Meaning
Date/time stamp	The date and time the file was scanned.
Encryption type	The type of encryption used to encrypt the file. **SysData:** SDE Encryption Key. **User:** User Encryption Key. **Common:** Common Encryption Key. WSScan does not report files encrypted using Encrypt for Sharing.
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 Encryption Removal Agent

Stop the service
Restart the service

Description:
Dell Encryption Removal Agent
[Waiting for SDE Deactivation]

Name	Startup Type
Bluetooth Support Service	Manual
BranchCache	Manual
Certificate Propagation	Manual
CMGShield	Automatic
CNG Key Isolation	Manual
COM+ Event System	Automatic
Dell Encryption Removal Agent	Automatic
Desktop Window Manager Sessi	Automatic

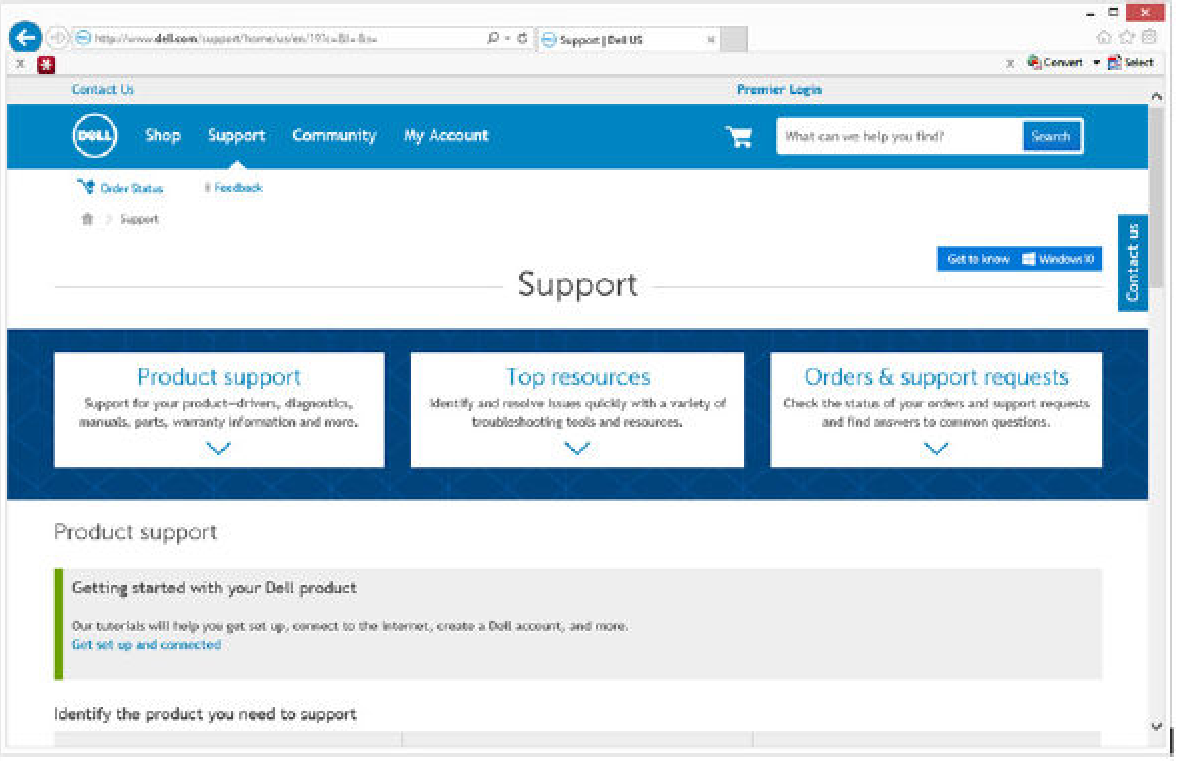
Dell ControlVault Drivers

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.



Support

Product support

Support for your product—drivers, diagnostics, manuals, parts, warranty information and more.

Top resources

Identify and resolve issues quickly with a variety of troubleshooting tools and resources.

Orders & support requests

Check the status of your orders and support requests and find answers to common questions.

Product support

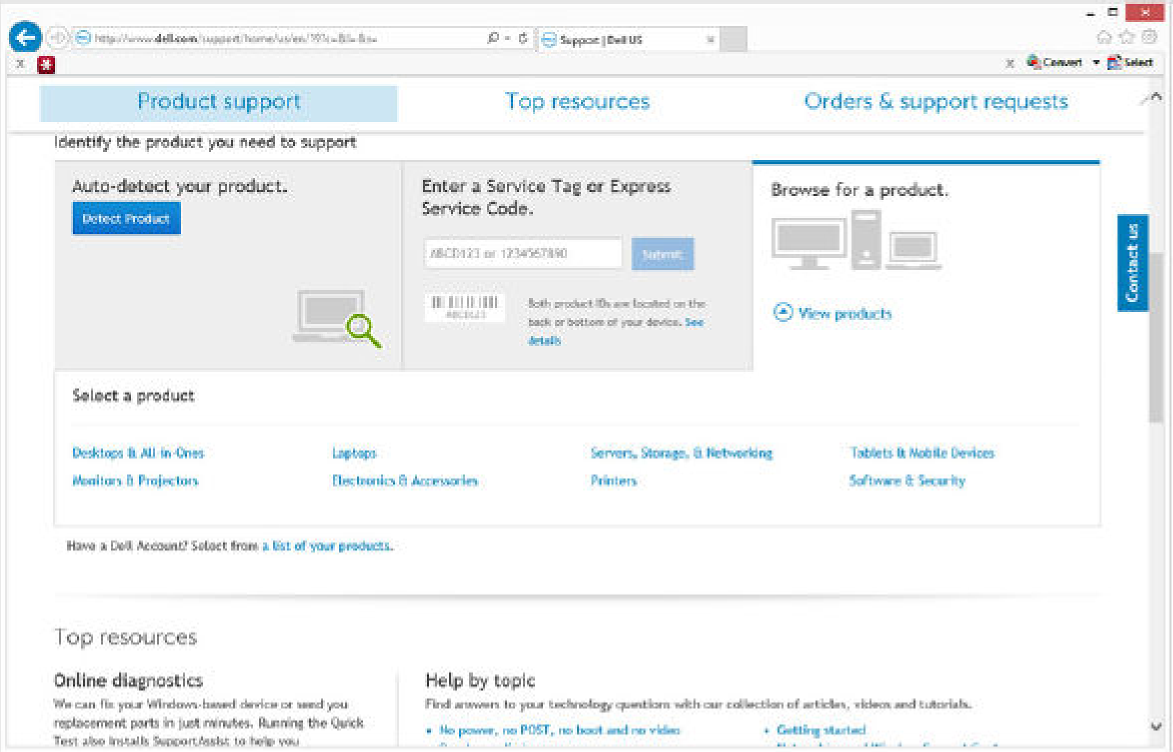
Getting started with your Dell product

Our tutorials will help you get set up, connect to the internet, create a Dell account, and more.

Get set up and connected

Identify the product you need to support

2 Select your computer model.



Identify the product you need to support

Auto-detect your product.

Enter a Service Tag or Express Service Code.

Both product IDs are located on the back or bottom of your device. See details

Browse for a product.

Select a product

Desktops & All-in-Ones
Laptops
Servers, Storage, & Networking
Tablets & Mobile Devices
Monitors & Projectors
Electronics & Accessories
Printers
Software & Security

Have a Dell Account? Select from a list of your products.

Top resources

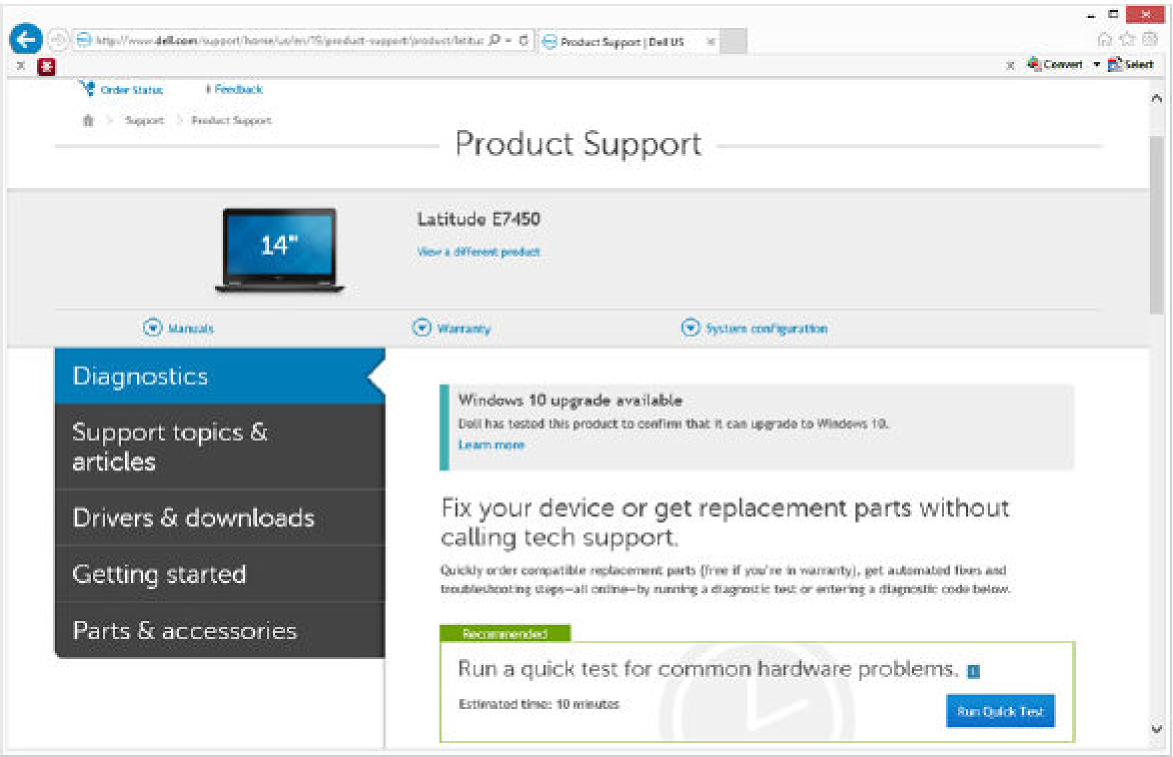
Online diagnostics

We can fix your Windows-based device or send you replacement parts in just minutes. Running the Quick Test also installs SupportAssist to help you

Help by topic

Find answers to your technology questions with our collection of articles, videos and tutorials.

- No power, no POST, no boot and no video
- Getting started



Product Support

Latitude E7450

Windows 10 upgrade available

Dell has tested this product to confirm that it can upgrade to Windows 10.

Learn more

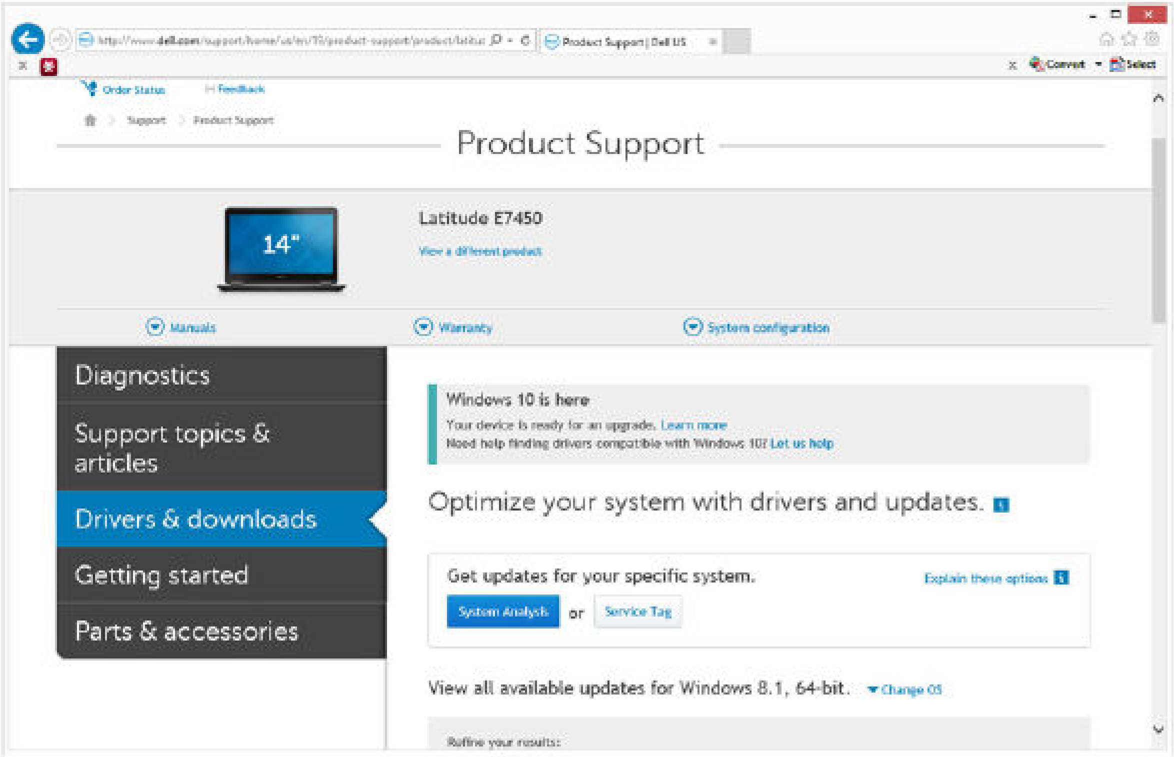
Fix your device or get replacement parts without calling tech support.

Quickly order compatible replacement parts (free if you're in warranty), get automated fixes and troubleshooting steps—all online—by running a diagnostic test or entering a diagnostic code below.

Run a quick test for common hardware problems.

Estimated time: 10 minutes

3 Select **Drivers & Downloads**.



Windows 10 is here

Your device is ready for an upgrade. Learn more

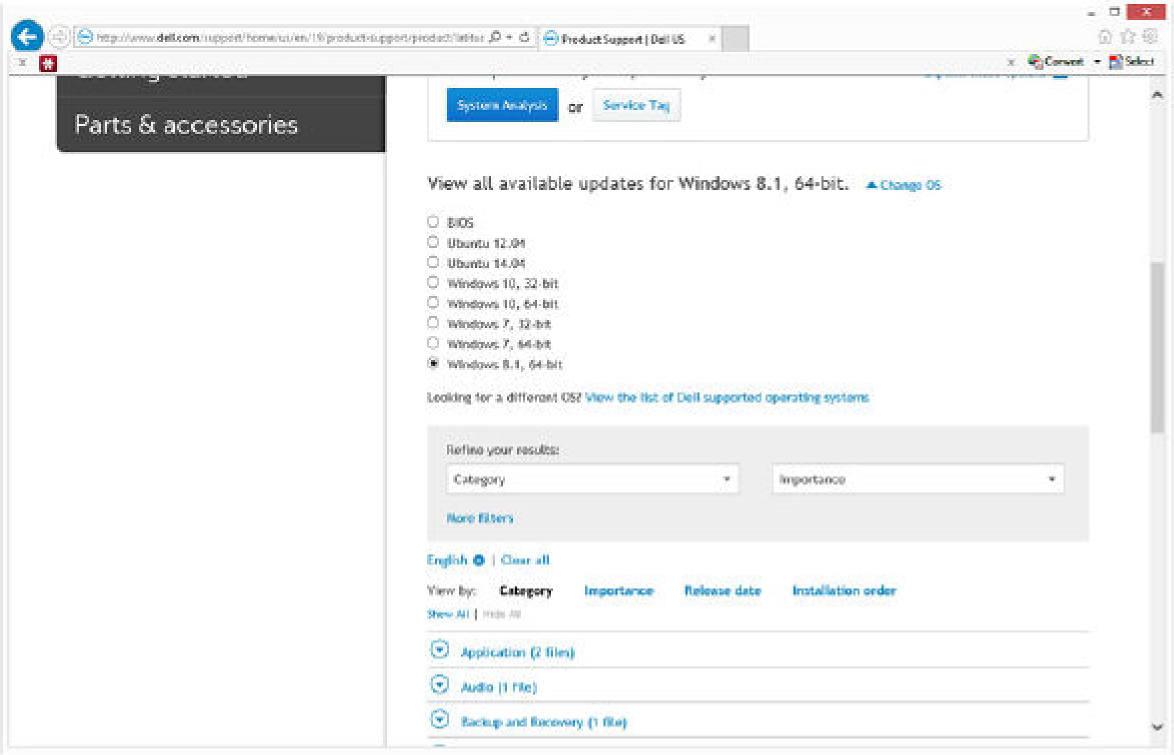
Need help finding drivers compatible with Windows 10? Let us help

Optimize your system with drivers and updates.

Get updates for your specific system.

View all available updates for Windows 8.1, 64-bit.

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



View all available updates for Windows 8.1, 64-bit.

○ BIOS
○ Ubuntu 12.04
○ Ubuntu 14.04
○ Windows 10, 32-bit
○ Windows 10, 64-bit
○ Windows 7, 32-bit
○ Windows 7, 64-bit
● Windows 8.1, 64-bit

Looking for a different OS? View the list of Dell supported operating systems

Refine your results:

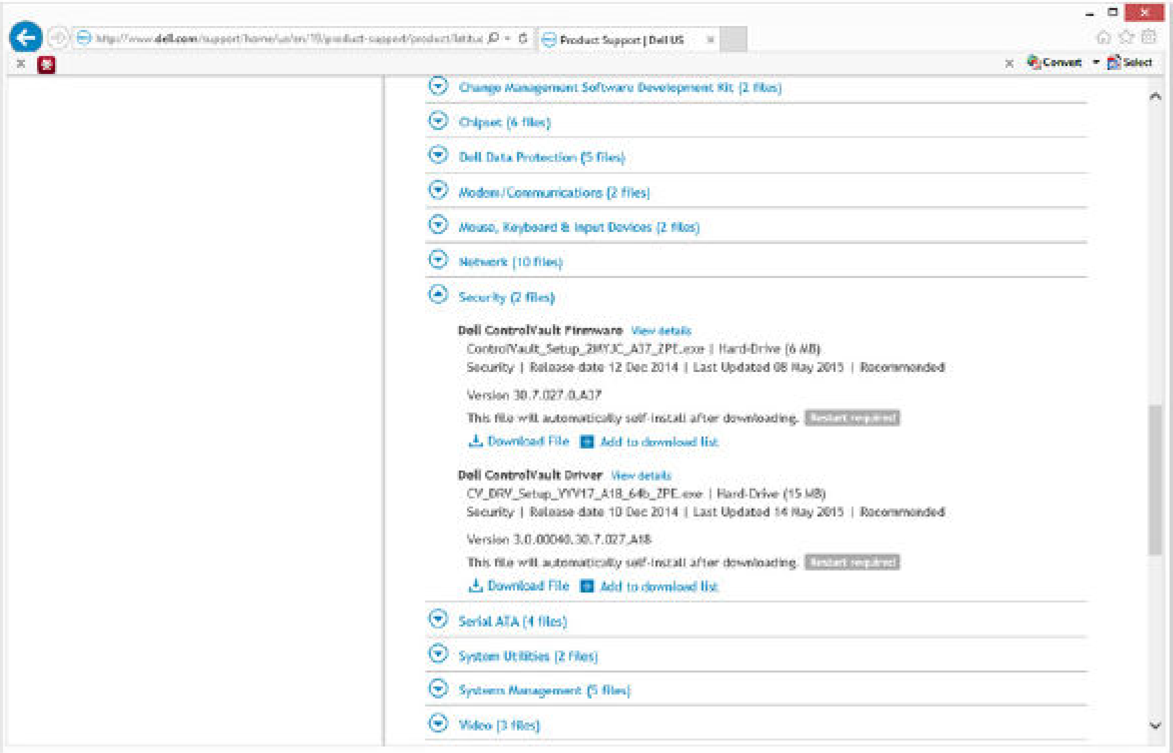
View by: **Category** Importance Release date Installation order

Application (2 files)

Audio (1 File)

Backup and Recovery (1 file)

5 Expand the **Security** category.


http://www.dell.com/support/home/us/en/19/product-support/product/latitu
Product Support | Dell US
Convert
Select

Change Management Software Development Kit (2 files)

Chipset (6 files)

Dell Data Protection (5 files)

Modem/Communications (2 files)

Mouse, Keyboard & Input Devices (2 files)

Network (10 files)

Security (2 files)

Dell ControlVault Firmware View details
ControlVault_Setup_2MYJC_A37_ZPE.exe | Hard-Drive (6 MB)
Security | Release date 12 Dec 2014 | Last Updated 08 May 2015 | Recommended

Version 30.7.027.0.A37

This file will automatically self-install after downloading. Restart required

Download File Add to download list

Dell ControlVault Driver View details
CV_DRV_Setup_YYV17_A18_64b_ZPE.exe | Hard-Drive (15 MB)
Security | Release date 10 Dec 2014 | Last Updated 14 May 2015 | Recommended

Version 3.0.00040.30.7.027.A18

This file will automatically self-install after downloading. Restart required

Download File Add to download list

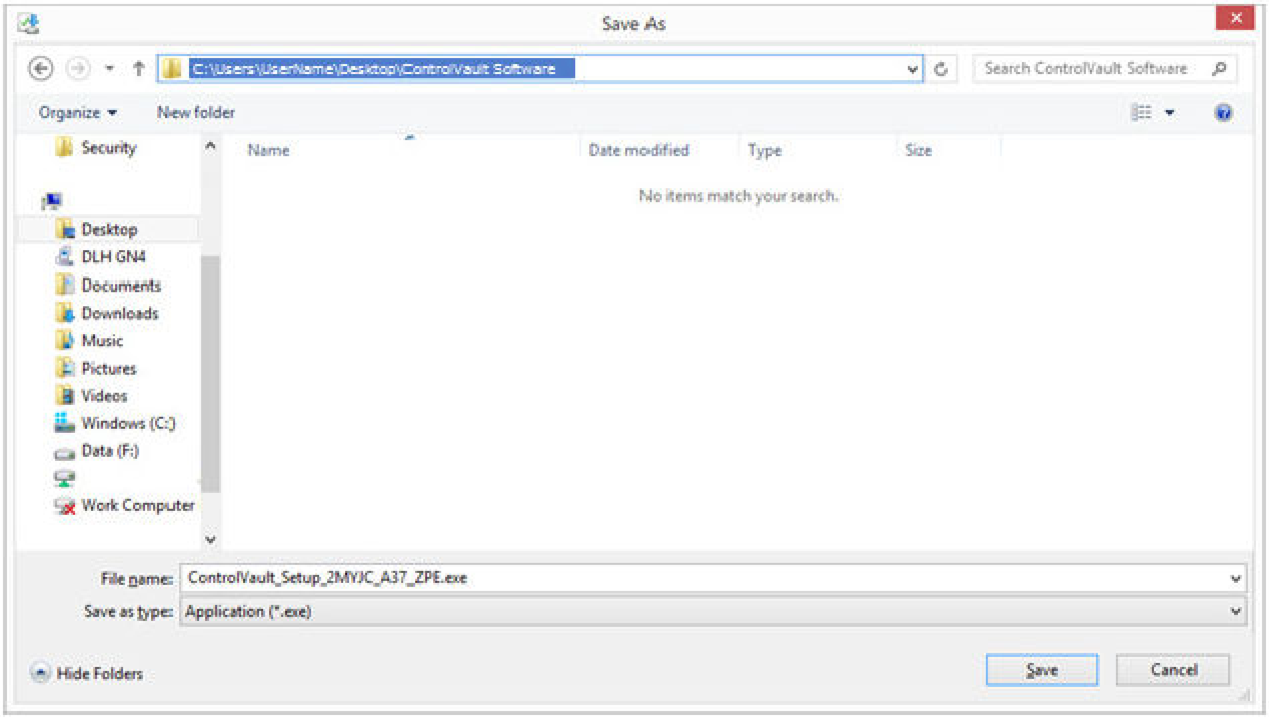
Serial ATA (4 files)

System Utilities (2 files)

Systems Management (5 files)

Video (3 files)

6 Download and save the Dell ControlVault Drivers.



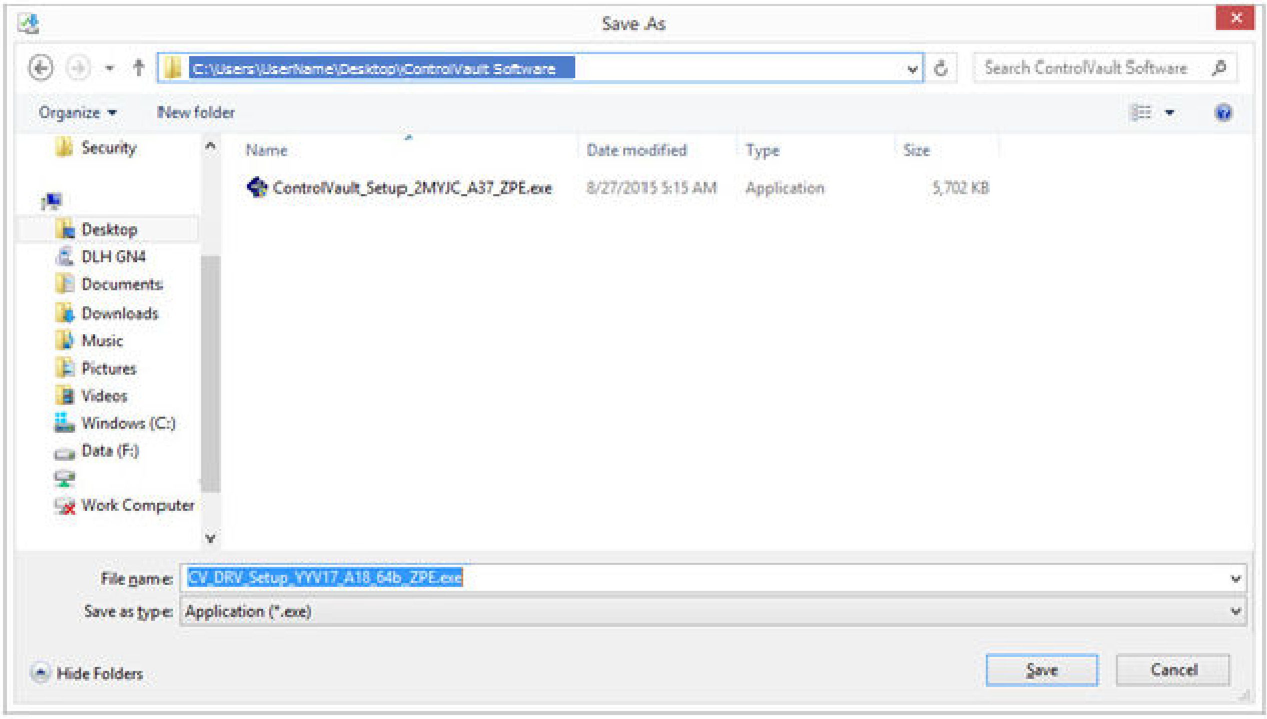
C:\Users\UserName\Desktop\ControlVault Software

No items match your search.

File name: ControlVault_Setup_2MYJC_A37_ZPE.exe

Save as type: Application (*.exe)

7 Download and save the Dell ControlVault Firmware.



C:\Users\UserName\Desktop\ControlVault Software

Name	Date modified	Type	Size
ControlVault_Setup_2MYJC_A37_ZPE.exe	8/27/2015 5:15 AM	Application	5,702 KB

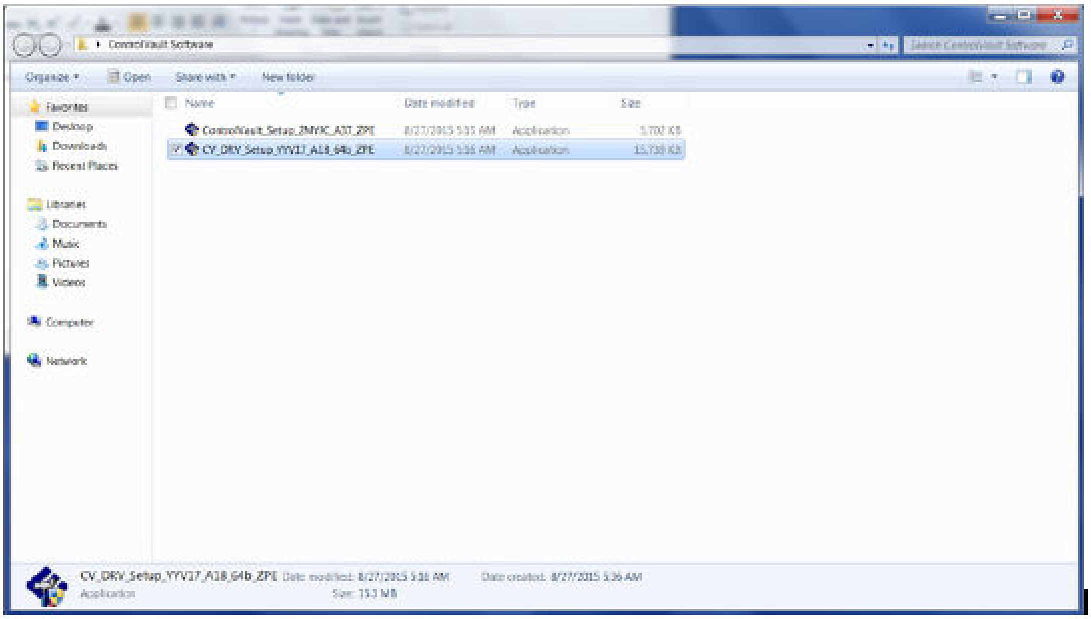
File name: CV_DRV_Setup_YYV17_A18_64b_ZPE.exe

Save as type: Application (*.exe)

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.



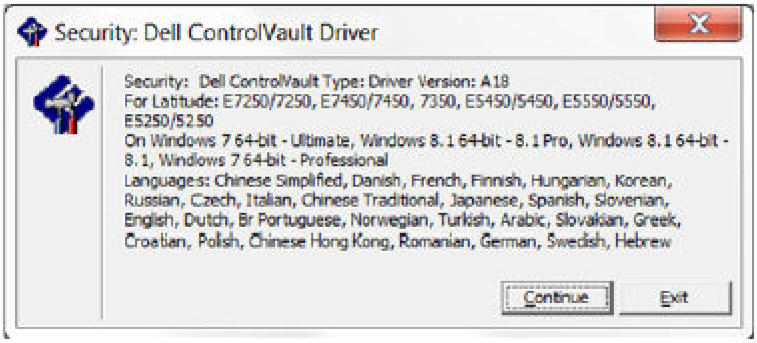
Name	Date modified	Type	Size
ControlVault_Setup_2MYJC_A37_ZPE	8/27/2015 5:15 AM	Application	5,702 KB
CV_DRV_Setup_YYV17_A18_64b_ZPE	8/27/2015 5:16 AM	Application	15,730 KB

CV_DRV_Setup_YYV17_A18_64b_ZPE Date modified: 8/27/2015 5:16 AM Date created: 8/27/2015 5:36 AM
Application Size: 15.3 MB

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.

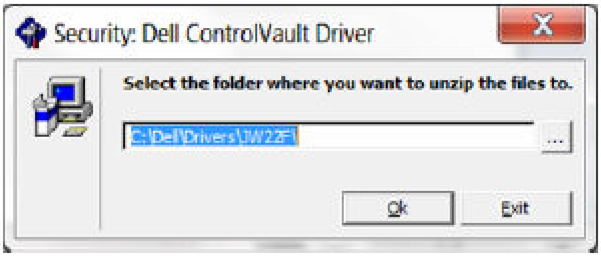
3 Click **Continue** to begin.



Security: Dell ControlVault Driver

Security: Dell ControlVault Type: Driver Version: A18
For Latitude: E7250/7250, E7450/7450, 7350, E5450/5450, E5550/5550, E5250/5250
On Windows 7 64-bit - Ultimate, Windows 8.1 64-bit - 8.1 Pro, Windows 8.1 64-bit - 8.1, Windows 7 64-bit - Professional
Languages: Chinese Simplified, Danish, French, Finnish, Hungarian, Korean, Russian, Czech, Italian, Chinese Traditional, Japanese, Spanish, Slovenian, English, Dutch, Br Portuguese, Norwegian, Turkish, Arabic, Slovakian, Greek, Croatian, Polish, Chinese Hong Kong, Romanian, German, Swedish, Hebrew

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

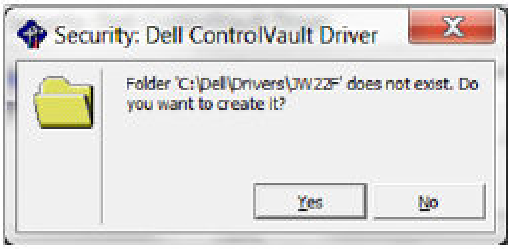


Security: Dell ControlVault Driver

Select the folder where you want to unzip the files to.

C:\Dell\Drivers\JW22F

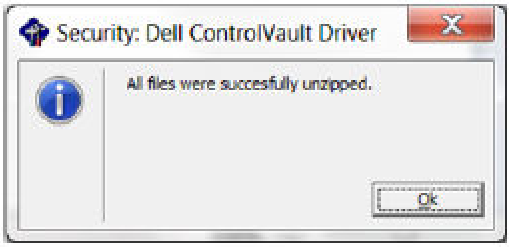
5 Click **Yes** to allow the creation of a new folder.



Security: Dell ControlVault Driver

Folder 'C:\Dell\Drivers\JW22F' does not exist. Do you want to create it?

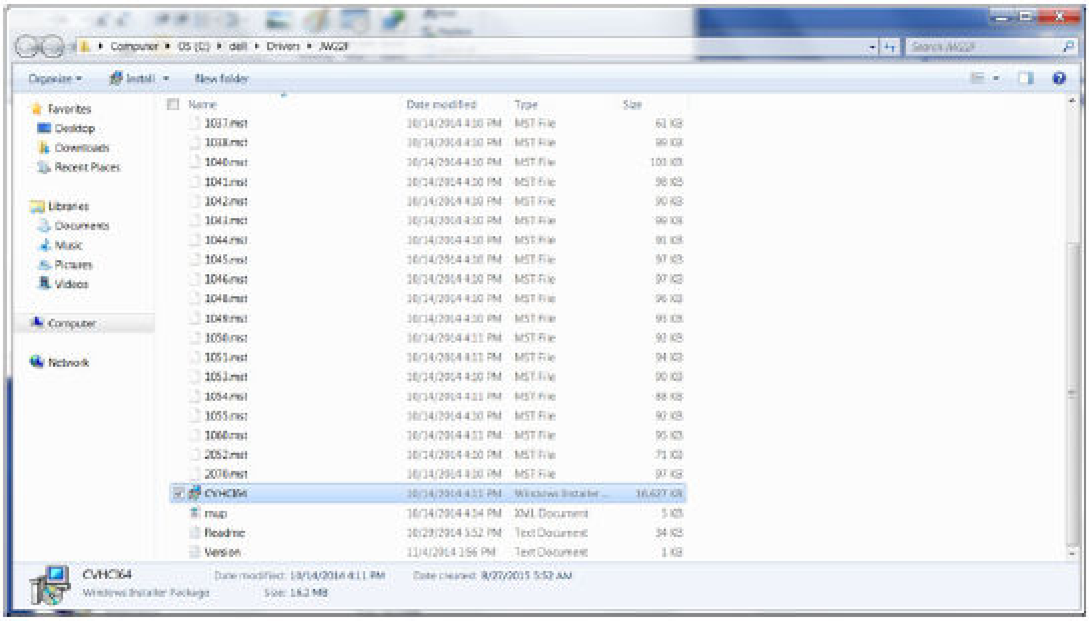
6 Click **Ok** when the successfully unzipped message displays.



Security: Dell ControlVault Driver

All files were succesfully unzipped.

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**.



Computer ▸ OS (C:) ▸ dell ▸ Drivers ▸ JWG2F

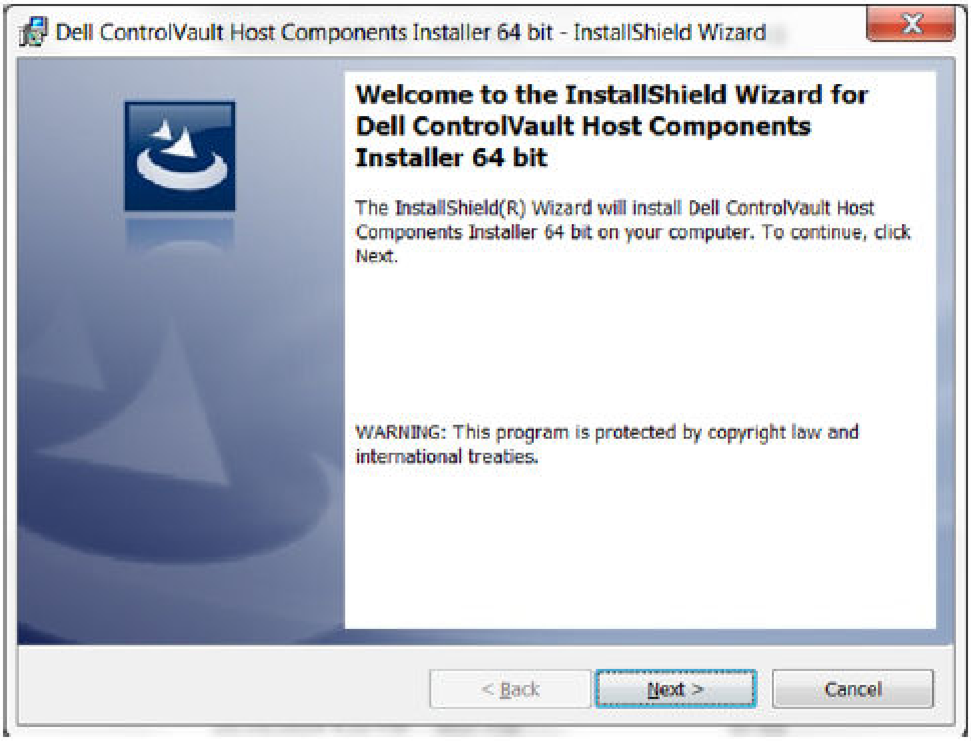
Organize ▾ Install ▾ New folder

Name	Date modified	Type	Size
1037.mst	10/14/2014 4:10 PM	MST File	61 KB
1038.mst	10/14/2014 4:10 PM	MST File	99 KB
1040.mst	10/14/2014 4:10 PM	MST File	103 KB
1041.mst	10/14/2014 4:10 PM	MST File	98 KB
1042.mst	10/14/2014 4:10 PM	MST File	90 KB
1043.mst	10/14/2014 4:10 PM	MST File	99 KB
1044.mst	10/14/2014 4:10 PM	MST File	91 KB
1045.mst	10/14/2014 4:10 PM	MST File	97 KB
1046.mst	10/14/2014 4:10 PM	MST File	97 KB
1048.mst	10/14/2014 4:10 PM	MST File	96 KB
1049.mst	10/14/2014 4:10 PM	MST File	95 KB
1050.mst	10/14/2014 4:11 PM	MST File	93 KB
1051.mst	10/14/2014 4:11 PM	MST File	94 KB
1053.mst	10/14/2014 4:10 PM	MST File	90 KB
1054.mst	10/14/2014 4:11 PM	MST File	88 KB
1055.mst	10/14/2014 4:10 PM	MST File	92 KB
1060.mst	10/14/2014 4:11 PM	MST File	95 KB
2052.mst	10/14/2014 4:10 PM	MST File	71 KB
2076.mst	10/14/2014 4:10 PM	MST File	97 KB
CVHCI64	10/14/2014 4:11 PM	Windows Installer ...	16,427 KB
map	10/14/2014 4:14 PM	XML Document	5 KB
Readme	10/29/2014 3:52 PM	Text Document	34 KB
Version	11/4/2014 1:56 PM	Text Document	1 KB

CVHCI64 Date modified: 10/14/2014 4:11 PM Date created: 8/27/2015 5:52 AM
Windows Installer Package Size: 16.2 MB

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.



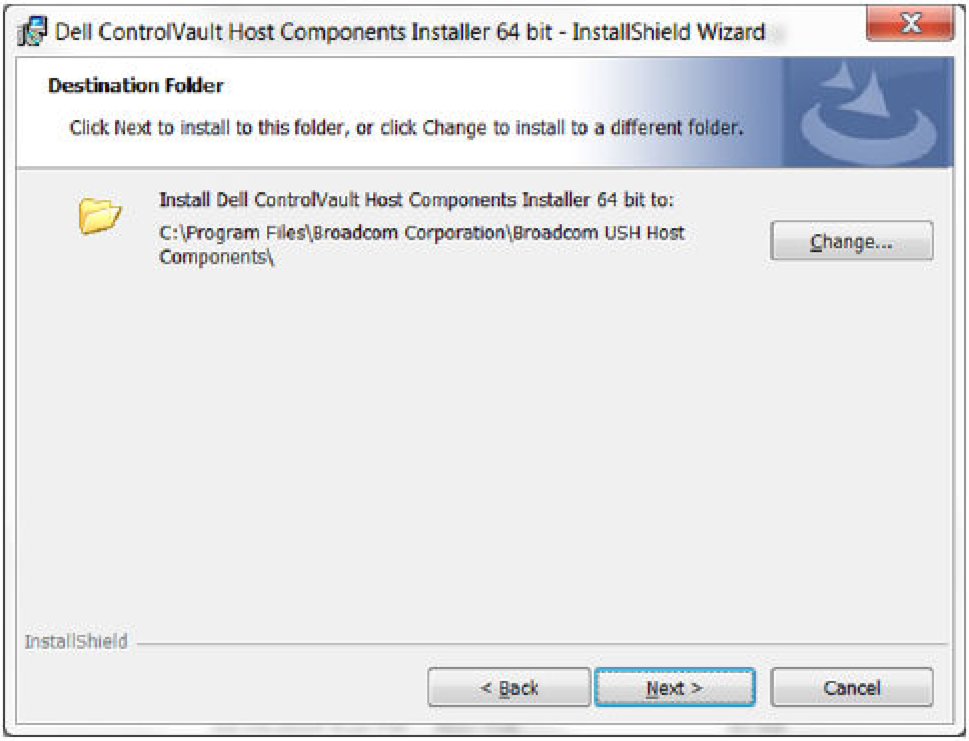
Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

Welcome to the InstallShield Wizard for Dell ControlVault Host Components Installer 64 bit

The InstallShield(R) Wizard will install Dell ControlVault Host Components Installer 64 bit on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



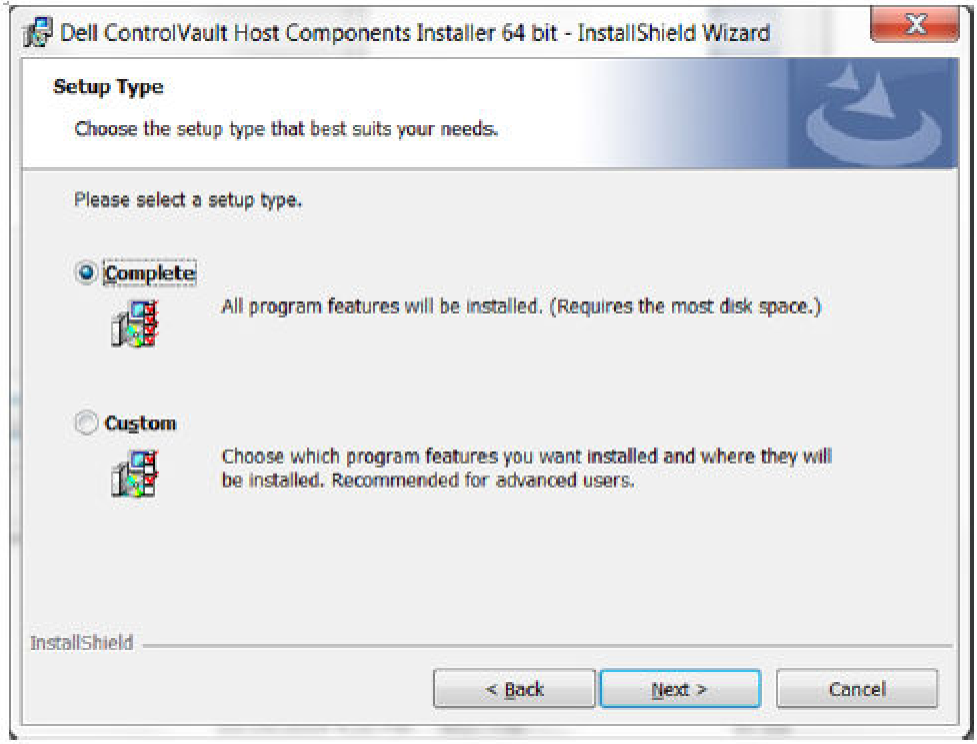
Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Dell ControlVault Host Components Installer 64 bit to:
C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

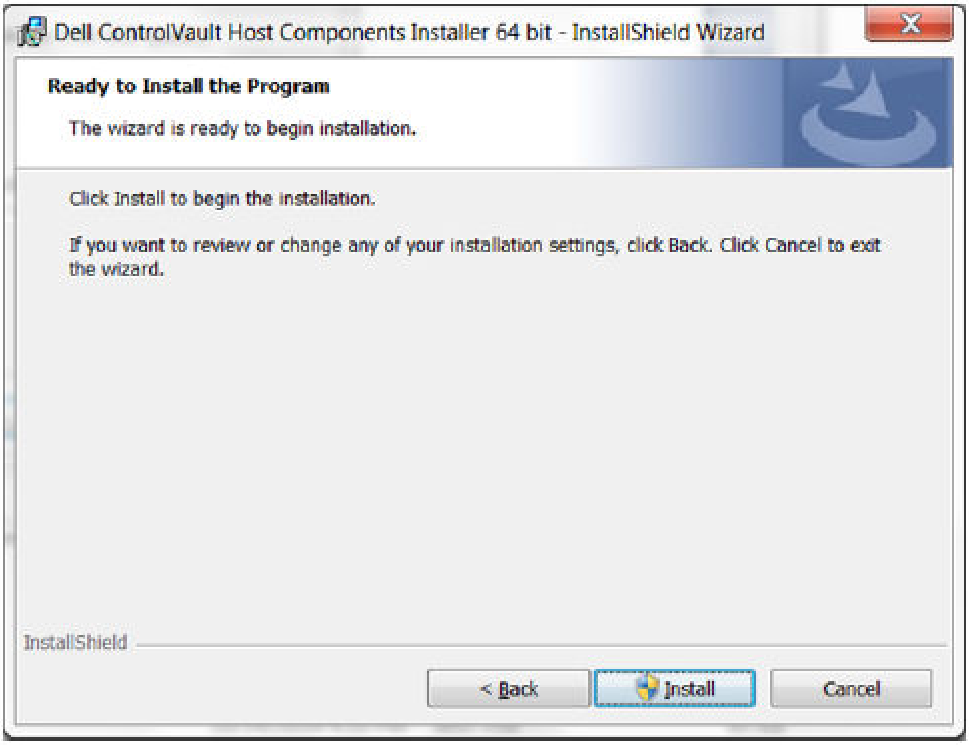
● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

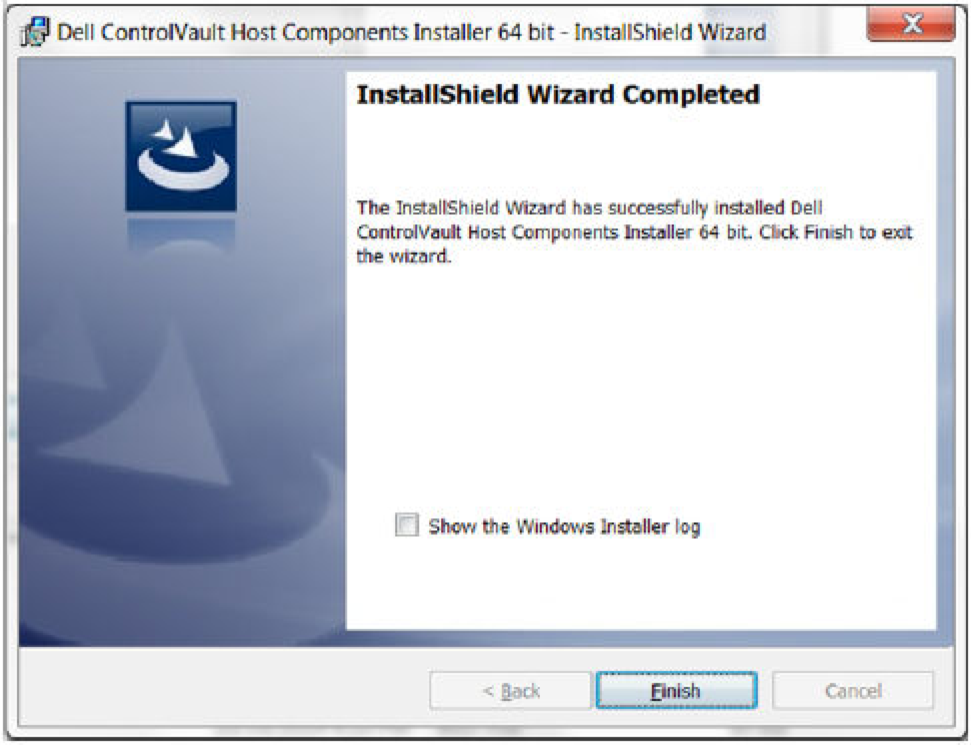
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Dell ControlVault Host Components Installer 64 bit. Click Finish to exit the wizard.

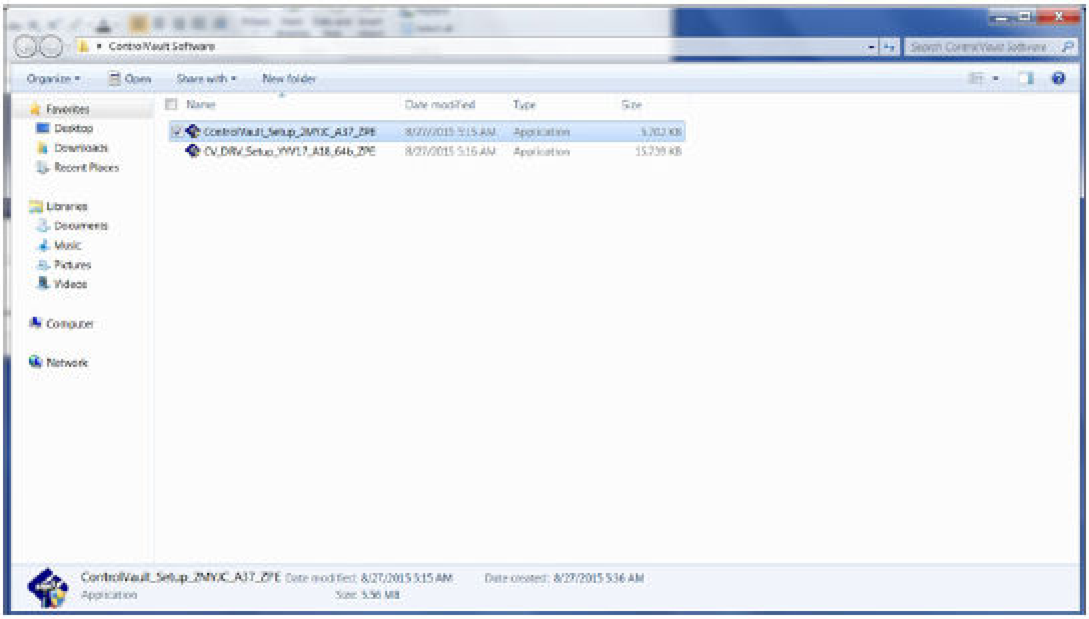
□ Show the Windows Installer log

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.

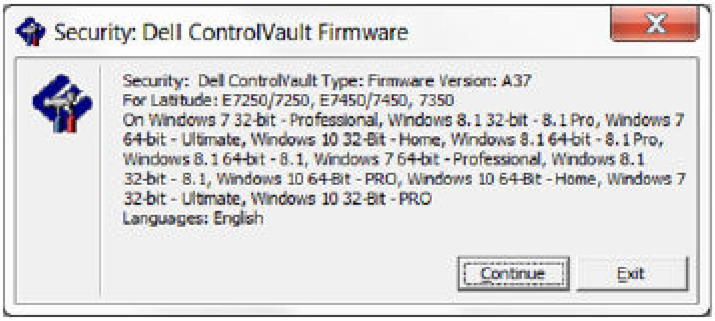


Name	Date modified	Type	Size
ControlVault_Setup_2MYJC_A37_ZPE	8/27/2015 5:15 AM	Application	5,702 KB
CV_DRV_Setup_YWV17_A18_64b_ZPE	8/27/2015 5:16 AM	Application	15,739 KB

ControlVault_Setup_2MYJC_A37_ZPE Date modified: 8/27/2015 5:15 AM Date created: 8/27/2015 5:36 AM
Application Size: 5.56 MB

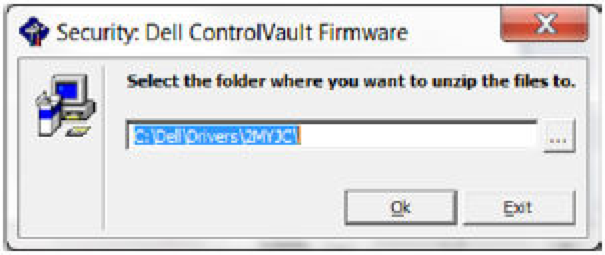
2 Double-click the Dell ControlVault firmware to launch the self-extracting executable file.

3 Click **Continue** to begin.


Security: Dell ControlVault Firmware

Security: Dell ControlVault Type: Firmware Version: A37
For Latitude: E7250/7250, E7450/7450, 7350
On Windows 7 32-bit - Professional, Windows 8.1 32-bit - 8.1 Pro, Windows 7 64-bit - Ultimate, Windows 10 32-Bit - Home, Windows 8.1 64-bit - 8.1 Pro, Windows 8.1 64-bit - 8.1, Windows 7 64-bit - Professional, Windows 8.1 32-bit - 8.1, Windows 10 64-Bit - PRO, Windows 10 64-Bit - Home, Windows 7 32-bit - Ultimate, Windows 10 32-Bit - PRO
Languages: English

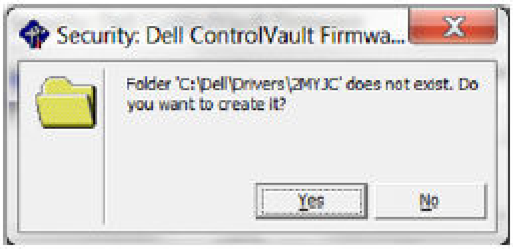
4 Click **Ok** to unzip the driver files in the default location of C:\Dell\Drivers\<New Folder>.


Security: Dell ControlVault Firmware

Select the folder where you want to unzip the files to.

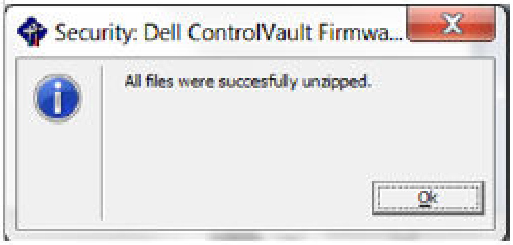
C:\Dell\Drivers\2MYJC\

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


Security: Dell ControlVault Firmwa...

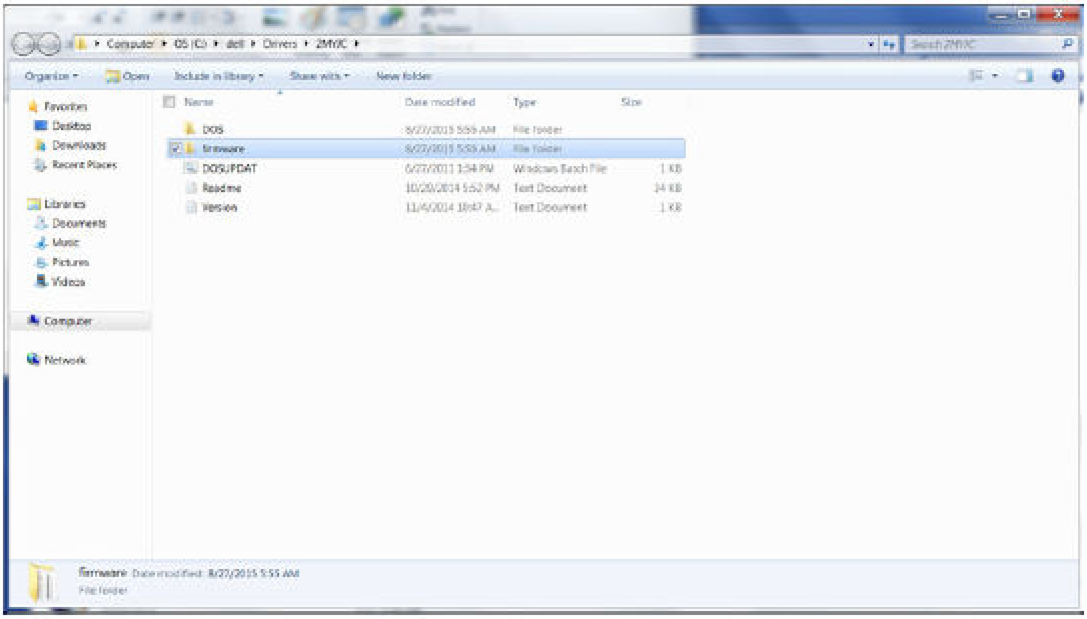
Folder 'C:\Dell\Drivers\2MYJC' does not exist. Do you want to create it?

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



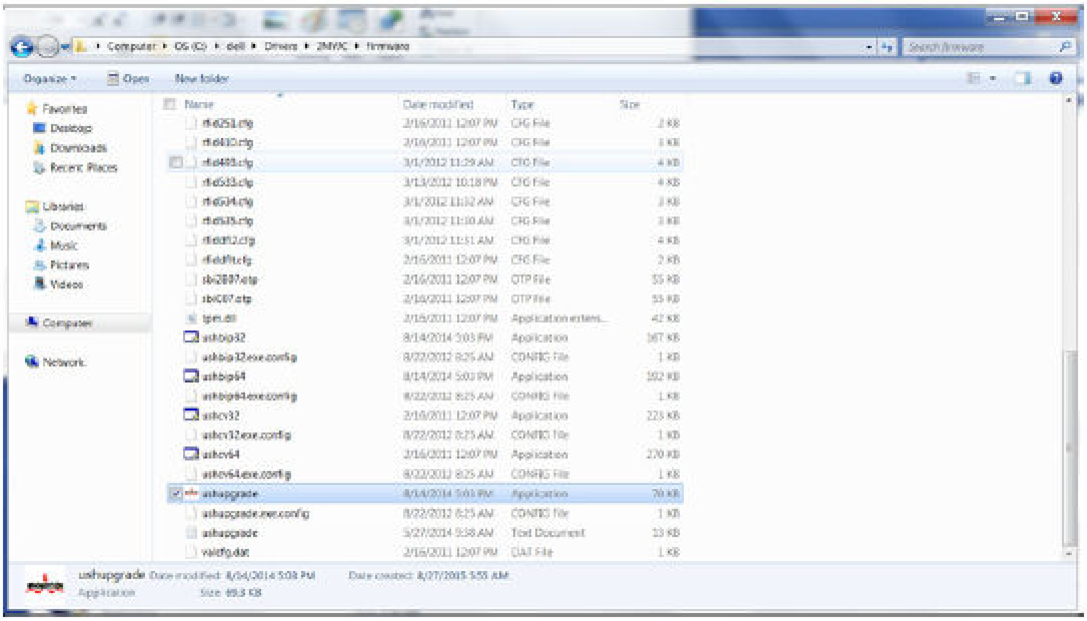
All files were succesfully unzipped.

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.



☐ Name	Date modified	Type	Size
DOS	8/27/2015 5:55 AM	File folder	
☑ firmware	8/27/2015 5:55 AM	File folder	
DOSUPDAT	6/27/2011 1:34 PM	Windows Batch File	1 KB
Readme	10/20/2014 5:52 PM	Text Document	24 KB
Version	11/4/2014 10:47 A...	Text Document	1 KB

firmware Date modified: 8/27/2015 5:55 AM
File folder

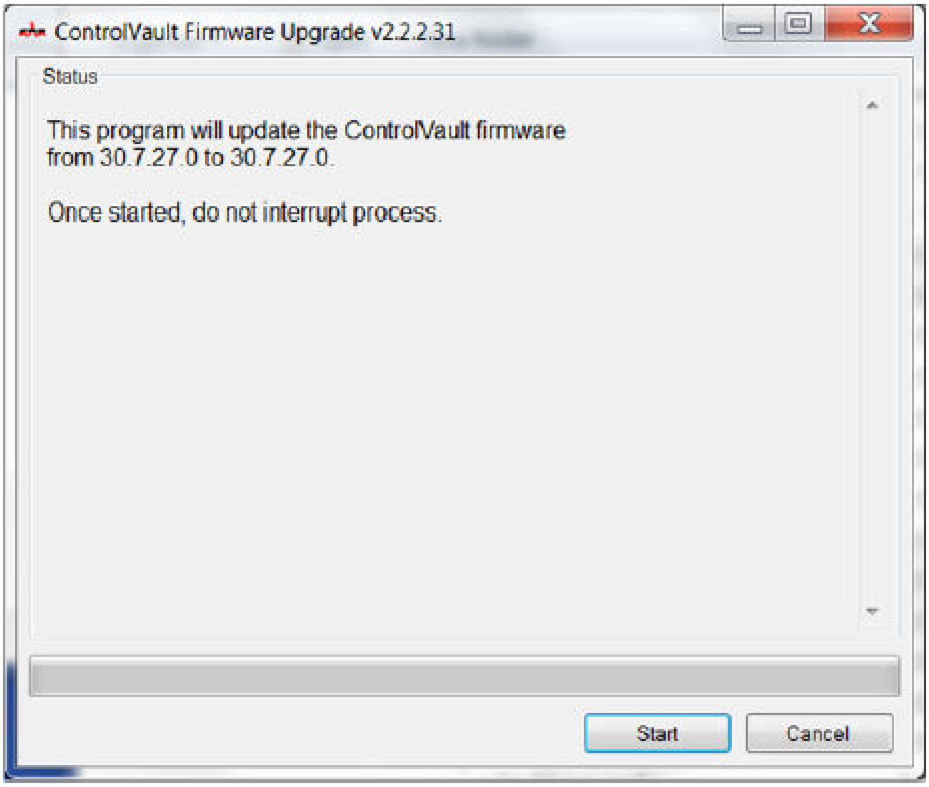


☐ Name	Date modified	Type	Size
rfid251.cfg	2/16/2011 12:07 PM	CFG File	2 KB
rfid410.cfg	2/16/2011 12:07 PM	CFG File	1 KB
☐ rfid483.cfg	3/1/2012 11:29 AM	CFG File	4 KB
rfid533.cfg	3/13/2012 10:18 PM	CFG File	4 KB
rfid534.cfg	3/1/2012 11:32 AM	CFG File	3 KB
rfid535.cfg	3/1/2012 11:30 AM	CFG File	3 KB
rfiddf12.cfg	3/1/2012 11:51 AM	CFG File	4 KB
rfiddflt.cfg	2/16/2011 12:07 PM	CFG File	2 KB
sbi2887.otp	2/16/2011 12:07 PM	OTP File	55 KB
sbiC07.otp	2/16/2011 12:07 PM	OTP File	55 KB
tpm.dll	2/16/2011 12:07 PM	Application extens...	42 KB
ushbip32	8/14/2014 5:03 PM	Application	167 KB
ushbip32.exe.config	8/22/2012 8:25 AM	CONFIG File	1 KB
ushbip64	8/14/2014 5:03 PM	Application	192 KB
ushbip64.exe.config	8/22/2012 8:25 AM	CONFIG File	1 KB
ushcv32	2/16/2011 12:07 PM	Application	223 KB
ushcv32.exe.config	8/22/2012 8:25 AM	CONFIG File	1 KB
ushcv64	2/16/2011 12:07 PM	Application	270 KB
ushcv64.exe.config	8/22/2012 8:25 AM	CONFIG File	1 KB
☑ ushupgrade	8/14/2014 5:03 PM	Application	70 KB
ushupgrade.exe.config	8/22/2012 8:25 AM	CONFIG File	1 KB
ushupgrade	5/27/2014 9:38 AM	Text Document	13 KB
valdfg.dat	2/16/2011 12:07 PM	DAT File	1 KB

ushupgrade Date modified: 8/14/2014 5:03 PM Date created: 8/27/2015 5:55 AM
Application Size: 69.3 KB

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

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



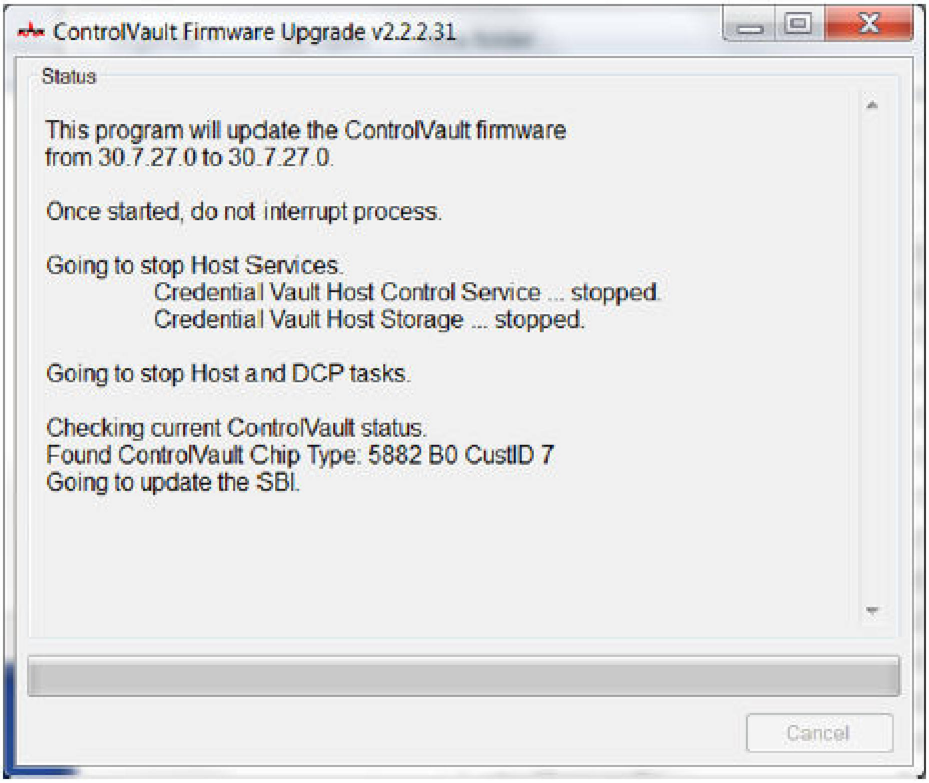
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

Once started, do not interrupt process.

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.



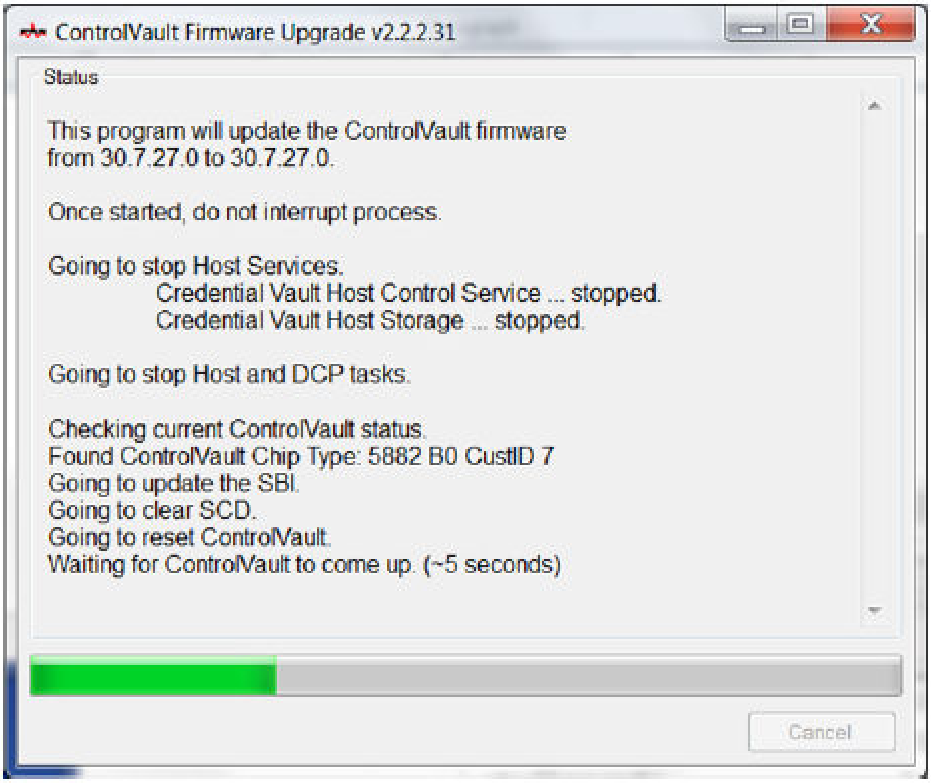
```
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

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.
```



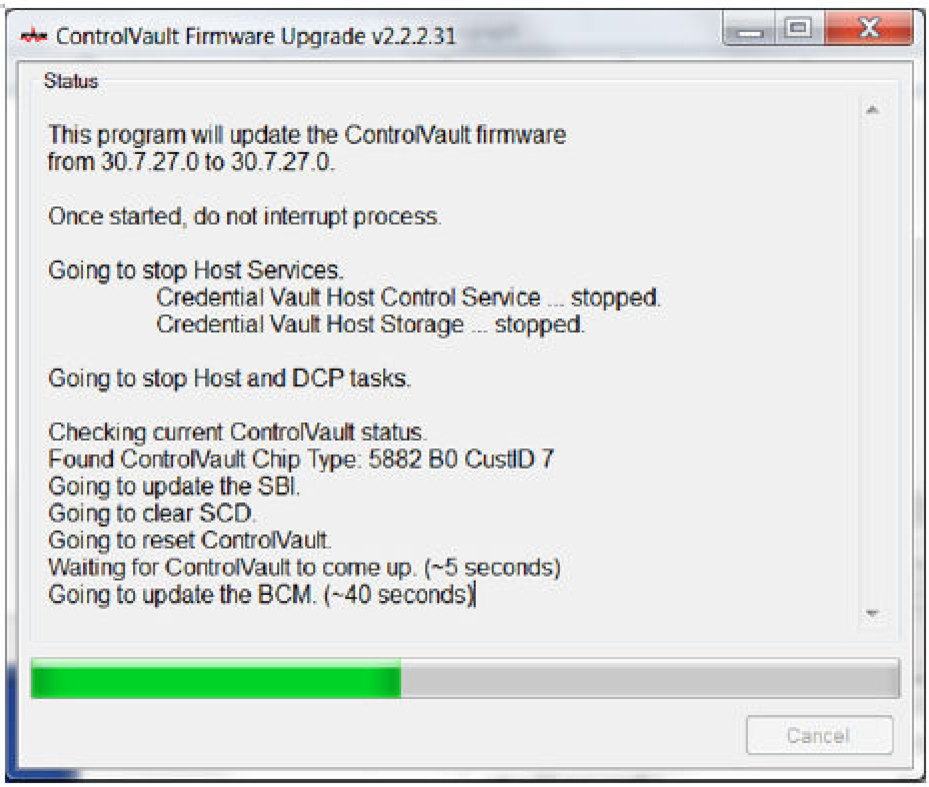
```
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

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)
```



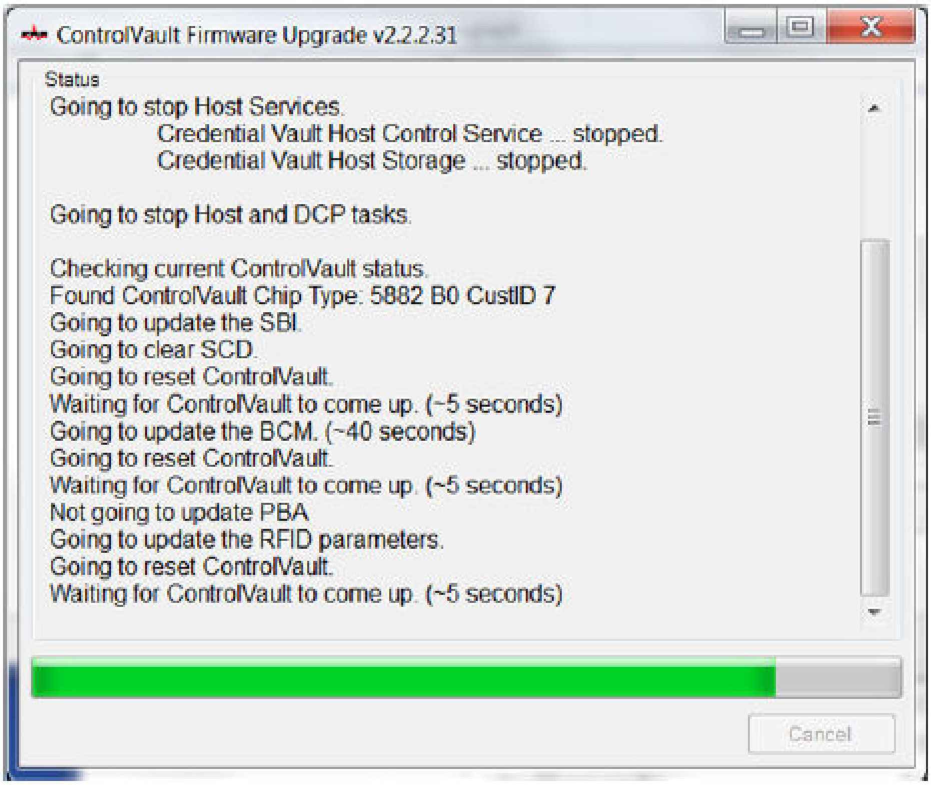
```
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

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)
```

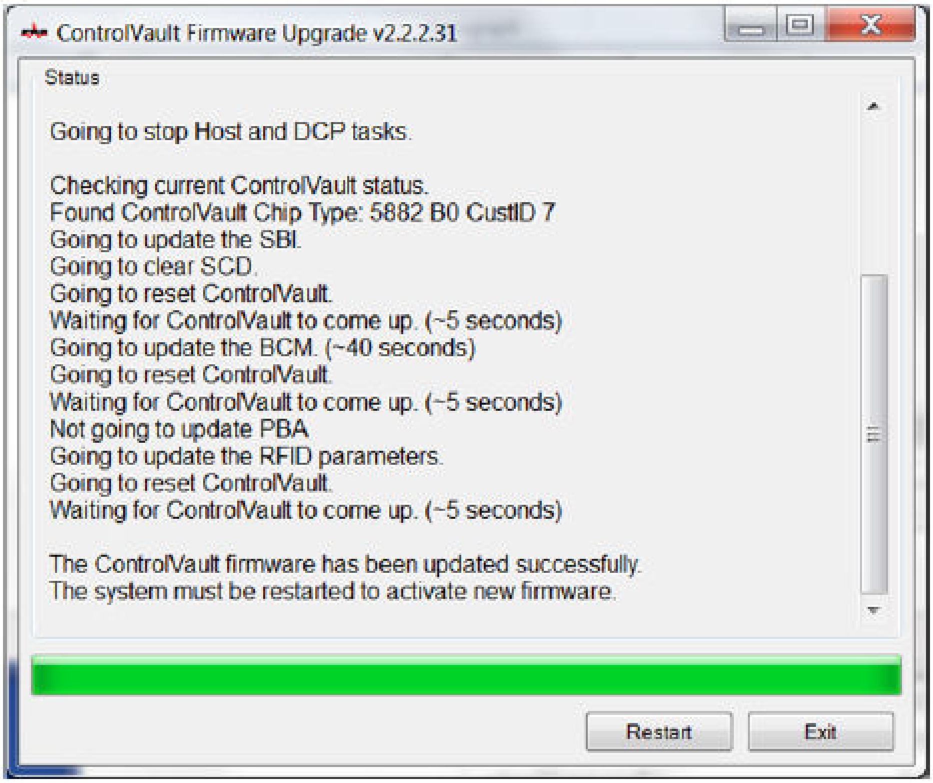


```
Going to stop Host Services.
        Credential Vault Host Control Service ... stopped.
        Credential Vault Host Storage ... stopped.

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)
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Not going to update PBA
Going to update the RFID parameters.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
```

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



```
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)
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Not going to update PBA
Going to update the RFID parameters.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)

The ControlVault firmware has been updated successfully.
The system must be restarted to activate new firmware.
```

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

11

Glossary

Advanced Authentication - The Advanced Authentication product provides fully-integrated fingerprint, smart card, and contactless smart card reader options. Advanced Authentication helps manage these multiple hardware authentication methods, 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.

EMS - External Media Shield - This service within the Dell Encryption client applies policies to removable media and external storage devices.

EMS Access Code - This service within the Dell Enterprise Server/VE allows for recovery of External Media Shield 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 or mobile hardware device that is managed by Dell Enterprise Server/VE.

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.

Machine key – When encryption is installed on a server, the Machine key protects a server's file encryption and policy keys. The Machine Key is stored on the Dell Enterprise Server/VE. The new Server exchanges certificates with the DDP Server during activation and uses the certificate for subsequent authentication events.

One-Time Password (OTP) - A one-time password is a password that can be used only once and is valid for a limited length of time. OTP requires that the TPM is present, enabled, and owned. To enable OTP, a mobile device is paired with the computer using the Security Console and the Security Tools Mobile app. The Security Tools Mobile app generates the password on the mobile device that is used to log onto the computer at the Windows logon screen. Based on policy, the OTP feature may be used to recover access to the computer if a password is expired or forgotten, if OTP has not been used to log on to the computer. The OTP feature can be used either for authentication or for recovery, but not both. OTP security exceeds that of some other authentication methods since the generated password can be used only once and expires in a short time.

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.

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