

Dell Encryption Personal

Installation Guide v10.0



Notes, cautions, and warnings

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

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

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

© 2012-2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

Installation Guide v10.0

2018 - 08

Rev. A01

Contents

1 Encryption Personal Overview.....	5
Encryption Personal.....	5
Advanced Authentication.....	5
Contact Dell ProSupport.....	5
2 Encryption Personal Requirements.....	6
Encryption Client.....	6
Encryption Client Prerequisites.....	7
Encryption Client Hardware.....	7
Encryption Client Operating Systems.....	7
Operating Systems for Encryption External Media.....	8
Encryption Client Localization.....	8
SED Client.....	8
SED Client Hardware.....	9
SED Client International KeyboardsSED Client LocalizationSED Client Operating Systems.....	10
3 Download the Software.....	12
4 Install Encryption Personal.....	16
Choose an Installation Method.....	16
Install Encryption Personal Using the Master Installer - RECOMMENDED.....	16
Install Encryption Personal Using the Child Installers.....	20
5 Advanced Authentication and Encryption Personal Setup Wizards.....	23
6 Configure Dell Encryption Management Agent Settings.....	31
Change the Administrator Password and Backup Location.....	31
Configure Encryption and Preboot Authentication.....	33
Change Encryption and Preboot Authentication Settings.....	36
Manage Users' Authentication.....	36
Remove All of a User's Enrolled Credentials.....	36
7 Uninstall the Master Installer.....	37
Choose an Uninstallation Method.....	37
Uninstall Interactively.....	37
Uninstall from the Command Line.....	37
8 Uninstall Using the Child Installers.....	38
Uninstall Encryption Client.....	38
Choose an Uninstallation Method.....	38
Uninstall Encryption Management Agent.....	40
Choose an Uninstallation Method.....	40
9 Data Security Uninstaller.....	42

Uninstall Encryption Personal.....	42
10 Policies and Template Descriptions.....	47
Policies.....	47
Template Descriptions.....	64
Aggressive Protection for All Fixed Drives and External Drives.....	64
PCI Regulation Targeted.....	64
Data Breach Regulation Targeted.....	64
HIPAA Regulation Targeted.....	65
Basic Protection for All Fixed Drives and External Drives (Default).....	65
Basic Protection for All Fixed Drives.....	65
Basic Protection for System Drive Only.....	65
Basic Protection for External Drives.....	66
Encryption Disabled.....	66
11 Extract Child Installers.....	67
12 Troubleshooting.....	68
Encryption Client Troubleshooting.....	68
Upgrade to the Windows 10 Creators Update.....	68
(Optional) Create an Encryption Removal Agent Log File.....	68
Find TSS Version.....	69
Encryption External Media and PCS Interactions.....	69
Use WSScan.....	69
Check Encryption Removal Agent Status.....	72
How to Encrypt an iPod with Encryption External Media.....	73
Dell ControlVault Drivers.....	74
Update Dell ControlVault Drivers and Firmware.....	74
Registry Settings.....	88
Encryption Client.....	88
Authentication.....	89
13 Glossary.....	91

Encryption Personal Overview

This guide assumes that Advanced Authentication is installed with Encryption Personal.

Encryption Personal

The purpose of Encryption Personal is to protect data on your computer, even if the computer is lost or stolen.

To ensure the security of your confidential data, Encryption Personal encrypts data on your Windows computer. You can always access the data when logged into the computer, but unauthorized users do not have access to this protected data. Data always remains encrypted on the drive, but because encryption is transparent, there is no need to change the way you work with applications and data.

Normally, the Encryption client decrypts data as you work with it. Occasionally, an application may try to access a file at the same moment that the Encryption client is encrypting or decrypting it. If this happens, after a second or two, the Encryption client displays a dialog that gives you the option of waiting or canceling the encryption/decryption. If you choose to wait, the Encryption client releases the file as soon as it is finished (generally within a few seconds).

Advanced Authentication

The Dell Data Security Console is the Advanced Authentication interface that guides users through configuring their PBA credentials and self-recovery questions, based on policy set by the local administrator.

See [Configure Advanced Authentication Administrator Settings](#) and refer to the *Dell Data Security Console User Guide* to learn how to use advanced authentication.

Contact Dell ProSupport

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

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

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

For phone numbers outside of the United States, see [Dell ProSupport International Phone Numbers](#).

Encryption Personal Requirements

These requirements detail everything needed for Encryption Personal installation.

Encryption Client

- Encryption Personal requires an entitlement to successfully install. The entitlement is supplied when you purchase Encryption Personal. Depending on how you purchase Encryption Personal, you may manually install the entitlement, using the simple instructions that accompany it. You may also enter the entitlement at the command line. If Encryption Personal is installed using Dell Digital Delivery, the entitlement installation is taken care of by the Dell Digital Delivery service. (The same binaries are used for Encryption Enterprise and Encryption Personal. The entitlement tells the installer which version to install.)
 - A Windows password is required (if one does not already exist) to protect access to your encrypted data. Creating a password for your computer prevents others from logging on to your user account without your password. Encryption Personal will fail to activate if a password is not created.
- 1 Go to the Windows Control Panel (**Start > Control Panel**).
 - 2 Click the **User Accounts** icon.
 - 3 Click **Create a password for your account**.
 - 4 Enter a new password and re-enter the password.
 - 5 Optionally enter a password hint.
 - 6 Click **Create Password**.
 - 7 Restart your computer.
- 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/upgrade.
 - Do not make changes to the computer, including inserting or removing external (USB) drives during installation/uninstallation/upgrade.
 - To reduce initial encryption time (as well as decryption time if uninstalling), run the Windows Disk Cleanup Wizard to remove temporary files and any other unnecessary data.
 - 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 master installer does not support upgrades from pre-v8.0 components. Extract the child installers from the master installer and upgrade the component individually. Should you have questions or concerns, contact Dell ProSupport.
 - The Encryption client now supports Audit Mode. Audit Mode allows administrators to deploy the Encryption client as part of the corporate image, rather than using a third-party SCCM or similar solutions to deploy the Encryption client. For instructions about how to install the Encryption client in a corporate image, see KB article [SLN304039](#).
 - The TPM is used for sealing the GPK. Therefore, if running the Encryption client, clear the TPM in the BIOS before installing a new operating system on the client computer.
 - 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 KB article [SLN288353](#) or [Contact Dell ProSupport](#) for help.

- Operating system re-install is not supported. To re-install the operating system, perform a backup of the target computer, wipe the computer, install the operating system, then recover the encrypted data following established recovery procedures.
- Be sure to periodically check www.dell.com/support for the most current documentation and Technical Advisories.

Encryption Client 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.

NOTE: .Net Framework 4.6 (or later) is required when running FIPS mode.

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](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>.

- The master installer installs the following prerequisites if not already installed on the computer. **When using the child installer**, you must install this component before installing the Encryption client.

Prerequisite

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

Visual C++ 2015 requires Windows Update [KB2999226](https://support.microsoft.com/kb/2999226) if installed on Windows 7.

Encryption Client Hardware

- The following table details the minimum supported computer hardware.

Hardware

- Intel Pentium or AMD Processor
- 110 MB of available disk space
- 512MB RAM

NOTE: Additional free disk space is required to encrypt the files on the endpoint. This size varies based on policies and size of drive.

- The following table details supported optional computer hardware.

Optional Embedded Hardware

- TPM 1.2 or 2.0

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
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro

Windows Operating Systems (32- and 64-bit)

- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)
- VMware Workstation 12.5 and higher

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

Operating Systems for Encryption External Media

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

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

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

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)

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

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

Encryption Client Localization

- The Encryption client is Multilingual User Interface (MUI) compliant and is localized in the following languages.

Language Support

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

SED Client

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

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

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

SED Client Hardware

- For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to KB article: [SLN296720](#).

Dell Computer Models Supported with UEFI

- The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support

– Latitude 5280	– Precision M3510	– Optiplex 3040 Micro, Mini Tower, Small Form Factor	– Venue Pro 11 (Models 5175/5179)
– Latitude 5480	– Precision M3520	– Optiplex 3046	– Venue Pro 11 (Model 7139)
– Latitude 5580	– Precision M4800	– OptiPlex 3050 All-In-One	
– Latitude 7370	– Precision M5510	– OptiPlex 3050 Tower, Small Form Factor, Micro	
– Latitude 7380	– Precision M5520	– Optiplex 5040 Mini Tower, Small Form Factor	
– Latitude E5250	– Precision M6800	– OptiPlex 5050 Tower, Small Form Factor, Micro	
– Latitude E5270	– Precision M7510	– OptiPlex 7020	
– Latitude E5285	– Precision M7520	– Optiplex 7040 Micro, Mini Tower, Small Form Factor	
– Latitude E5289 2-in-1	– Precision M7710	– OptiPlex 7050 Tower, Small Form Factor, Micro	
– Latitude E5450	– Precision M7720	– Optiplex 3240 All-In-One	
– Latitude E5470	– Precision D5720 All-in-One		
– Latitude E5550	– Precision T1700		
– Latitude E5570	– Precision T3420		
– Latitude E6440	– Precision T3620		

Dell Computer Models - UEFI Support

- Latitude E6540
- Latitude E7240
- Latitude E7250
- Latitude E7270
- Latitude E7280
- Latitude E7350
- Latitude 7389 2-in-1
- Latitude E7440
- Latitude E7450
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme (model 7414)
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 7212 Rugged Extreme Tablet
- Latitude 14 Rugged Extreme (model 7414)
- Latitude 14 Rugged (model 5414)
- Precision T5810
- Precision T7810
- Precision T7910
- XPS 13 9333
- XPS 13 9350
- XPS 15 9550
- XPS 15 9560
- Optiplex 5055 Ryzen CPU
- OptiPlex 5250 All-In-One
- Precision 5820 Tower
- Optiplex 7010
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- Precision 7820 Tower
- Precision 7920 Rack
- Optiplex 9010
- Optiplex 9020 Micro, Mini Tower, Small Form Factor
- Optiplex 9020 All-in-One
- Optiplex 9030 All-in-One
- Optiplex XE2

NOTE:

Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.

- For a list of docking stations and adapters supported with the SED client, see KB article [SLN296720](#).

SED Client International Keyboards

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

International Keyboard Support - UEFI

- DE-CH - Swiss German
- DE-FR - Swiss French

International Keyboard Support - Non-UEFI

- AR - Arabic (using Latin letters)
- DE-CH - Swiss German
- DE-FR - Swiss French

SED Client Localization

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

Language Support

- EN - English
- 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

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:

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

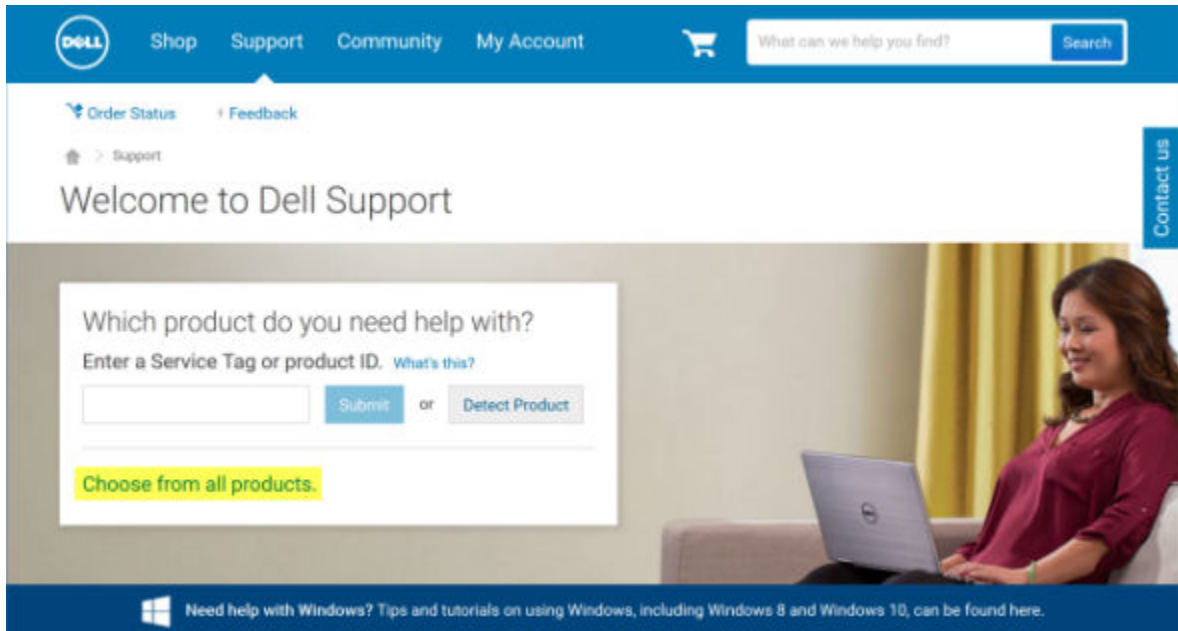
- Windows 8: Enterprise, Pro,
 - Windows 8.1: Enterprise, Pro
 - Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)
- Authentication features are available only when Preboot Authentication is enabled.

Download the Software

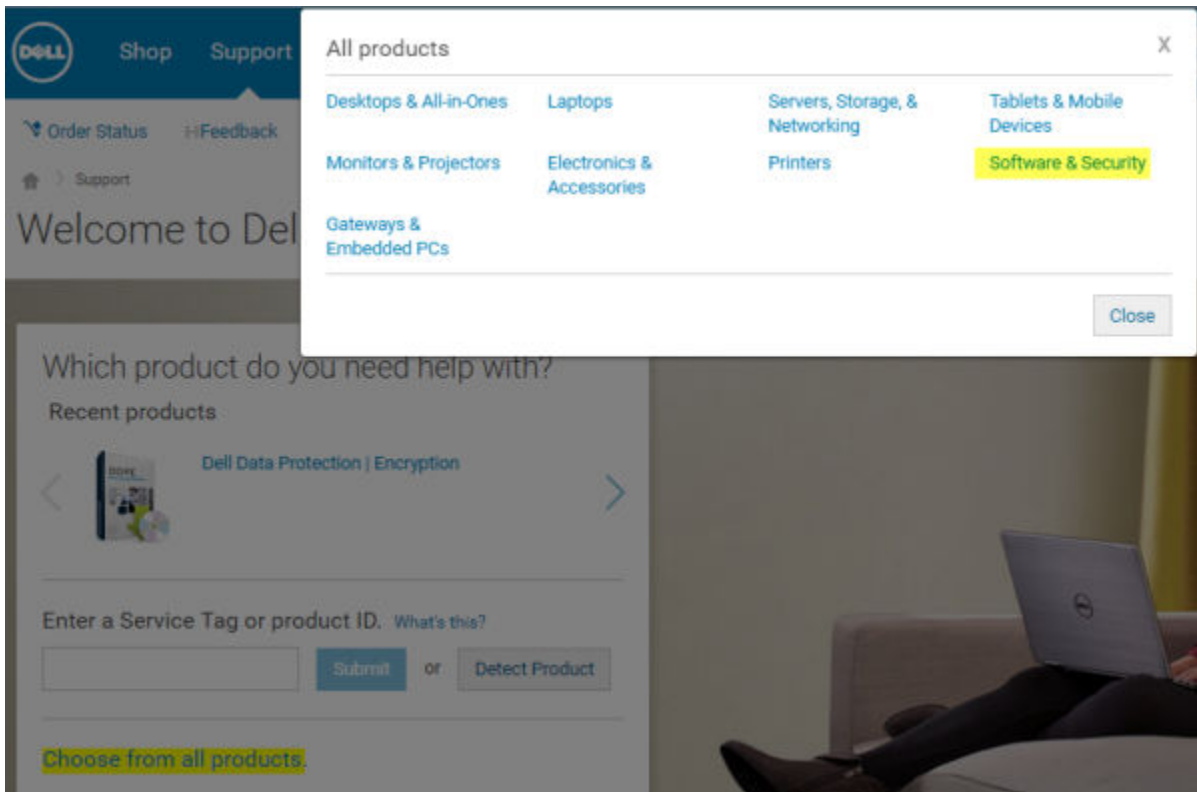
This section details obtaining the software from dell.com/support. If you already have the software, you can skip this section.

Go to dell.com/support to begin.

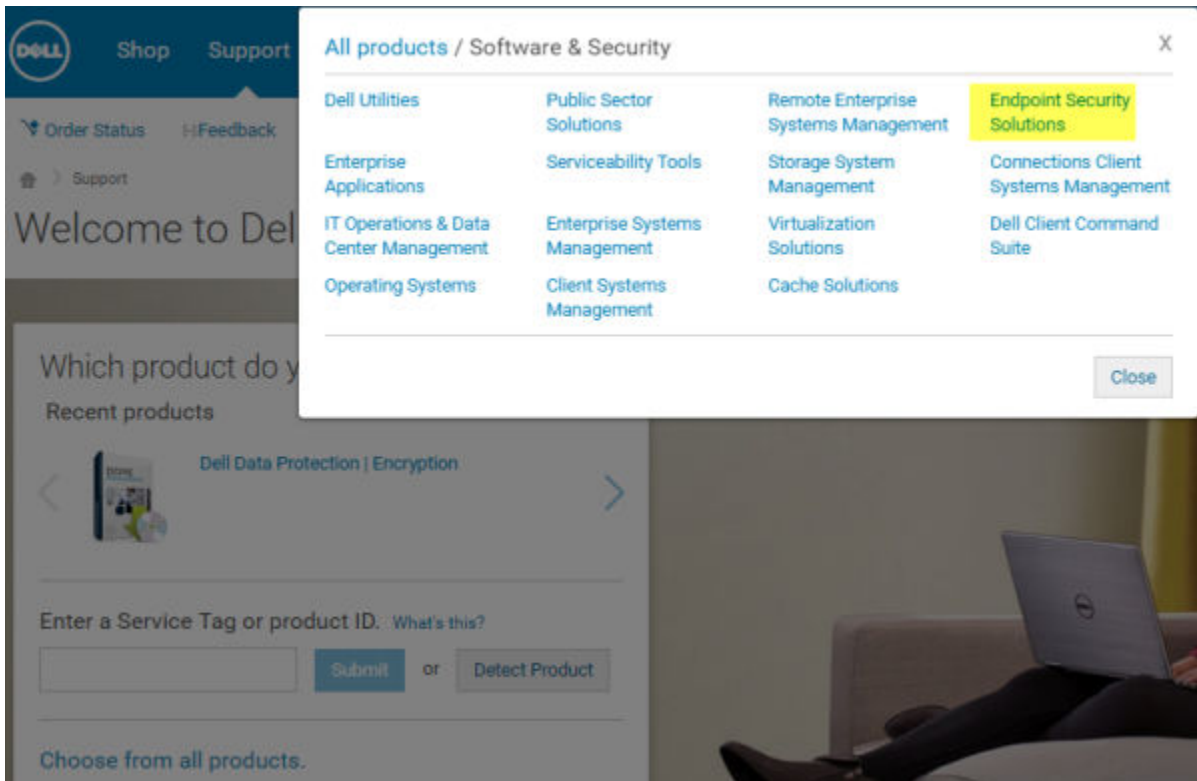
- 1 On the Dell Support webpage, select **Choose from all products**.



- 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 remembers.



- 4 Select the Dell product. Examples:

Dell Encryption Enterprise

Dell Endpoint Security Suite Enterprise

Dell Data Guardian

- 5 Select **Drivers & downloads**.
- 6 Select the desired client operating system type.
- 7 Select **Dell Data Security (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.

The screenshot shows the Dell Drivers & Downloads interface. On the left is a navigation menu with three items: 'Support topics & articles', 'Drivers & downloads' (highlighted in yellow), and 'Manuals'. The main content area has a header 'Optimize your system with drivers and updates.' followed by a sub-header 'View all available updates for Windows 10, 64-bit.' and a 'Change OS' button. Below this is a 'Refine your results:' section with two dropdown menus for 'Category' and 'Importance', and a 'More filters' link. A 'View by:' section offers options for 'Category', 'Importance', 'Release date', and 'Installation order', with 'Show All | Hide All' below. A single result is shown: 'Dell Data Protection (1 file)', highlighted in yellow. At the bottom, there are sections for 'More download options' (with links for 'My download lists', 'Update notifications', and 'Dell Download Center') and 'Drivers help and tutorials' (with a link for 'Driver Help and Tutorials').



- Support topics & articles
- Drivers & downloads
- Manuals

Optimize your system with drivers and updates. 1

Contact us

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 **Add to My Download List #XX**.



Proceed to [Install Encryption Personal](#).

Install Encryption Personal

You can install Encryption Personal using the master installer (recommended), or by extracting the child installers out of the master installer. Either way, Encryption Personal can be installed by user interface, command line or scripts, and using any push technology available to your organization.

Users should see the following help files for application assistance:

- See the *Dell Encrypt Help* to learn how to use the feature of the Encryption client. Access the help from `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- See the *Encryption External Media Help* to learn how the features of Encryption External Media. Access the help from `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
- See the *Encryption Personal Help* to learn how to use the features of Advanced Authentication. Access the help from `<Install dir>\Program Files\Dell\Dell Data Protection\Authentication\Help`.

Choose an Installation Method

There are two methods to install the client, select **one** of the following:

- [Install Encryption Personal Using the Master Installer - RECOMMENDED](#)
- [Install Encryption Personal Using the Child Installers](#)

Install Encryption Personal Using the Master Installer - RECOMMENDED

To install Encryption Personal, the installer must find the appropriate entitlement on the computer. If the appropriate entitlement is not found, Encryption Personal cannot be installed.

- The Dell Installer is commonly known as the Master Installer, as it installs multiple clients. In the case of Encryption Personal, it installs the Encryption client and the SED client.
- If installing using the master installer user interface, Encryption Personal can be installed on one computer at a time.
- Master installer log files are located at `C:\ProgramData\Dell\Dell Data Protection\Installer`.

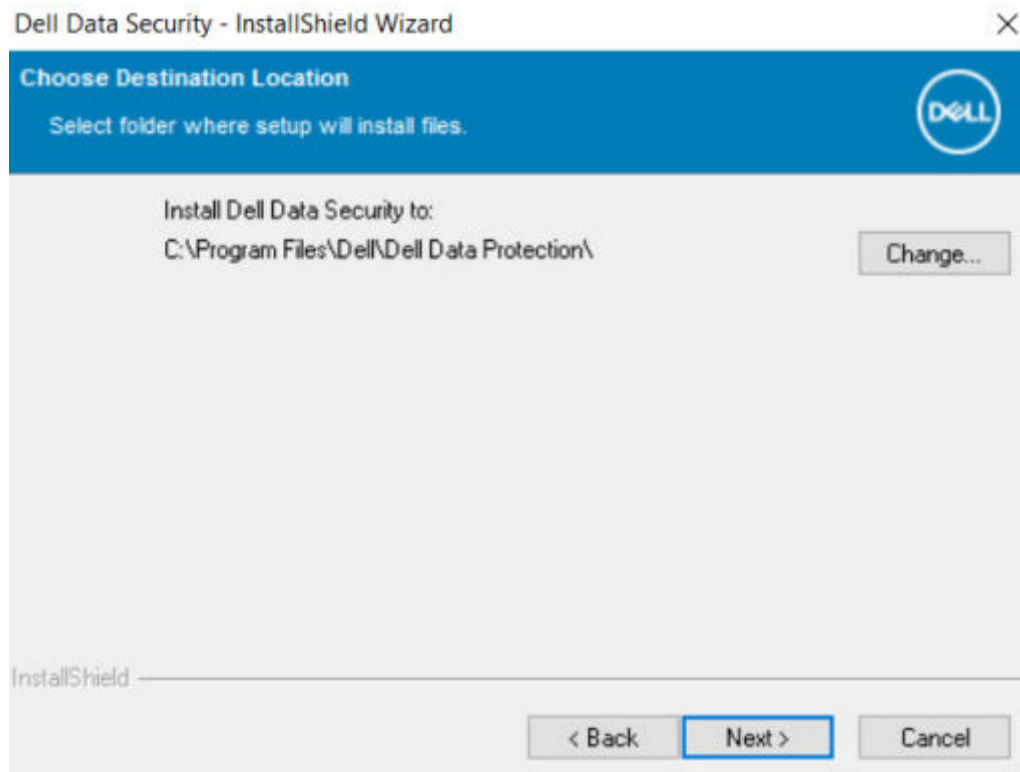
Select one method:

- [Installation Using the User Interface](#)
- [Installation Using the Command Line](#)

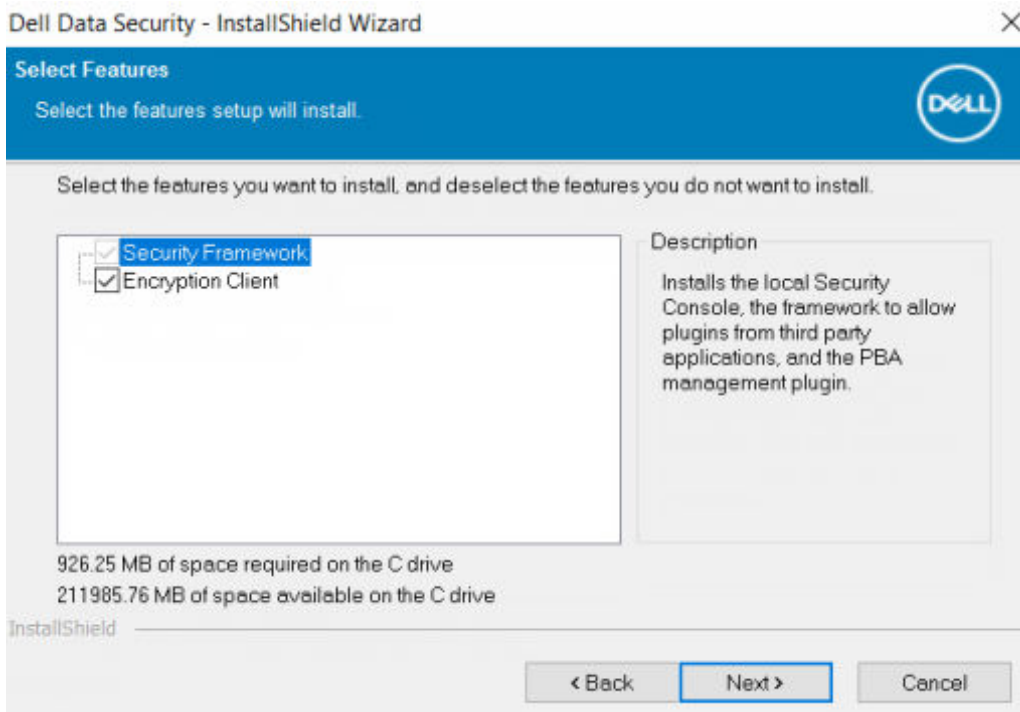
Installation Using the User Interface

- 1 Install the entitlement on the target computer if needed.
- 2 Copy DDSSetup.exe to the local computer.
- 3 Double-click DDSSetup.exe to launch the installer.
- 4 A dialog displays that alerts you to the status of installing the prerequisites. It takes a few minutes.
- 5 Click **Next** at the Welcome screen.
- 6 Read the license agreement, agree to the terms, and click **Next**.

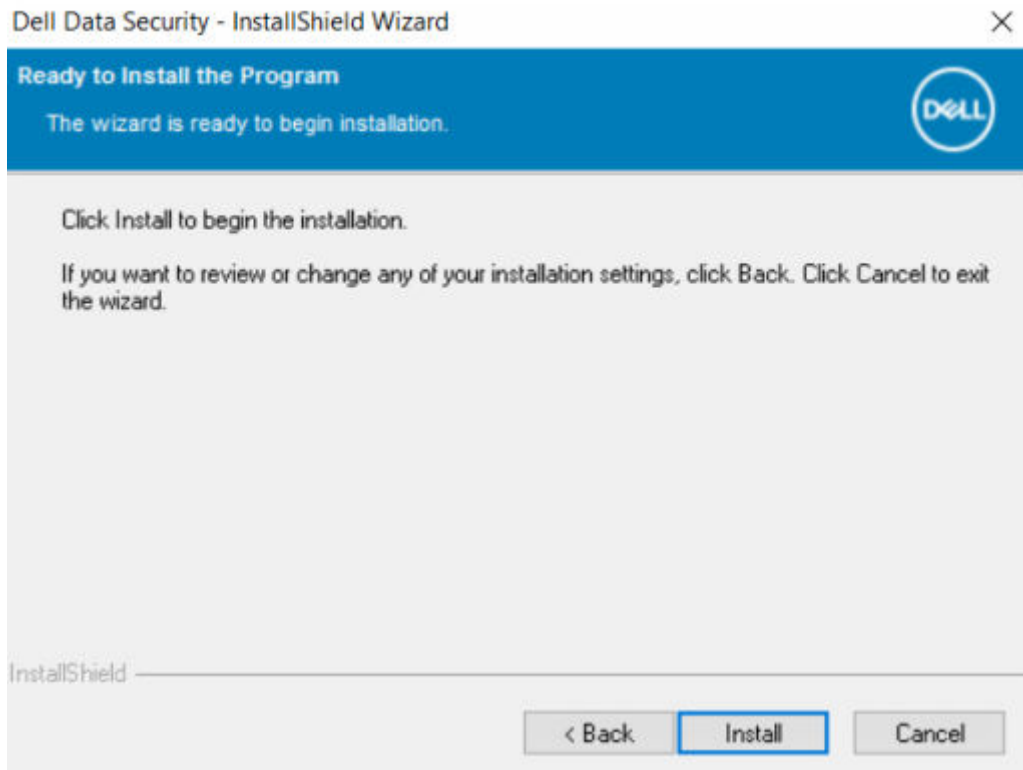
- 7 Click **Next** to install Encryption Personal in the default location of C:\Program Files\Dell\Dell Data Protection\.



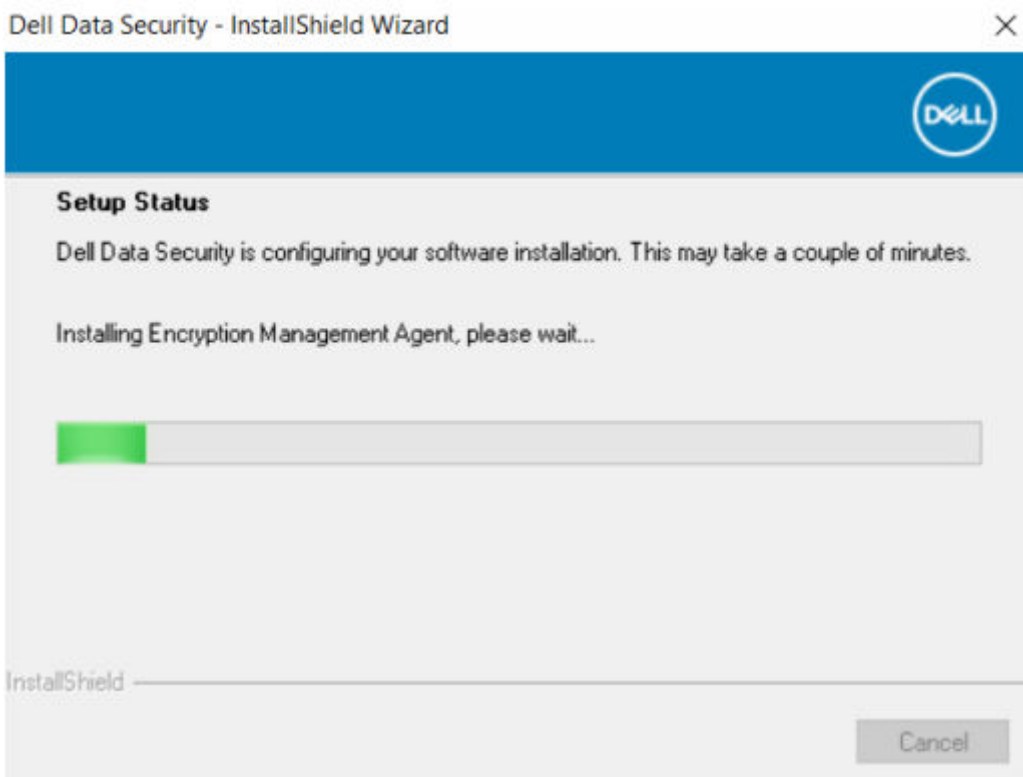
- 8 Authentication is installed by default and cannot be deselected. This is listed as Security Framework in the installer. Click **Next**.



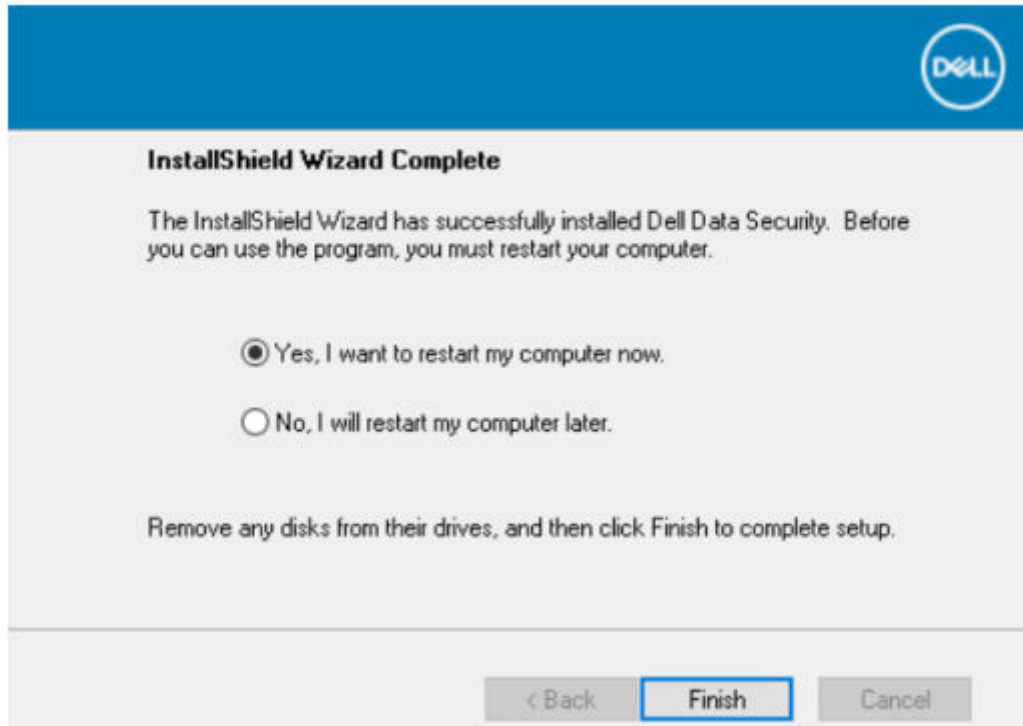
- 9 Click **Install** to begin the installation.



A status window displays. This takes several minutes.



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



11 Once the computer restarts, authenticate to Windows.

Installation of Encryption Personal + Advanced Authentication is complete.

Encryption Personal Setup Wizard and Configuration is covered separately.

Once the Encryption Personal Setup Wizard and Configuration is complete, launch the Encryption Personal Administrator Console.

The rest of this section details more installation tasks and may be skipped. Proceed to [Advanced Authentication and Encryption Personal Setup Wizards](#).

Installation Using the Command Line

- Install the entitlement on the target computer if needed.
- **NOTE: Dell Encryption logs do not specify if insufficient disk storage caused installation failure.**
- Switches:

For a command line installation, the switches must be specified first. The following table details the switches available for the installation.

Switch	Meaning
-y -gm2	Pass data to the self-extractor
/S	Silent mode
/z	Pass data to the InstallScript system variable CMDLINE

- Parameters:

The following table details the parameters available for the installation.

- Log files: Windows creates unique child installer installation 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 to create a log file by using **!*/v C:\<any directory>\<any log file name>.log**.

- All child installers use the same basic .msi switches and display options, except where noted, for command line installations. 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 *.exe
/s	Silent mode
/i	Install mode

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

Install Drivers

- Drivers and firmware for Dell ControlVault, fingerprint readers and smart cards 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 dell.com/support and selecting your computer model. Download the appropriate drivers and firmware based on your authentication hardware.
 - Dell 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.

- Then:

Encryption Management Agent

- Users log in to the PBA using their Windows credentials.
- Locate the file at **C:\extracted\Encryption Management Agent**.

Example Command Line Installation

\Encryption Management Agent

- The following example installs the Security Framework (silent installation, no reboot, and is installed in the default location of **C:\Program Files\Dell\Dell Data Protection**).

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

Then:

Install Encryption Client

- Review [Encryption Client](#) Requirements if your organization is using a certificate signed by a root authority, such as EnTrust or Verisign. A registry setting change is needed on the client computer to enable certificate validation.
- Locate the file at **C:\extracted\Encryption**.

Example Command Line Installation

- The following example installs Encryption Personal, Encrypt for Sharing, hides the overlay icons, no dialogue, no progress bar, and suppresses restart.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Once the computer is restarted, authenticate to Windows.

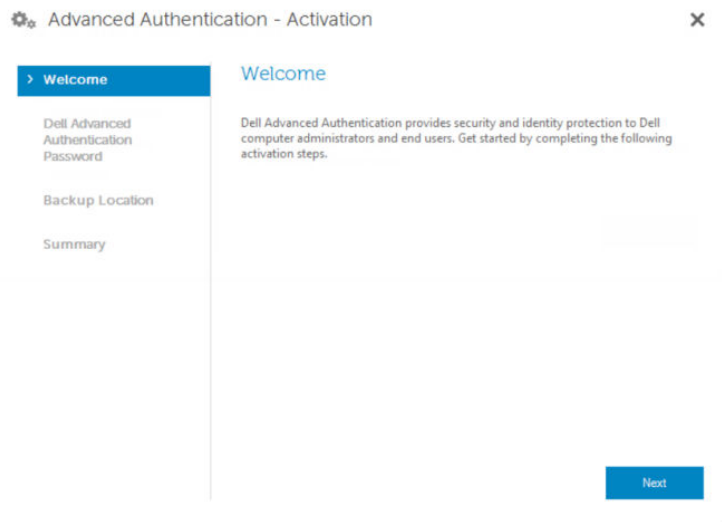
Installation of Encryption Personal is complete. Encryption Personal Setup Wizard and Configuration is covered separately.

Proceed to [Advanced Authentication and Encryption Personal Setup Wizards](#).

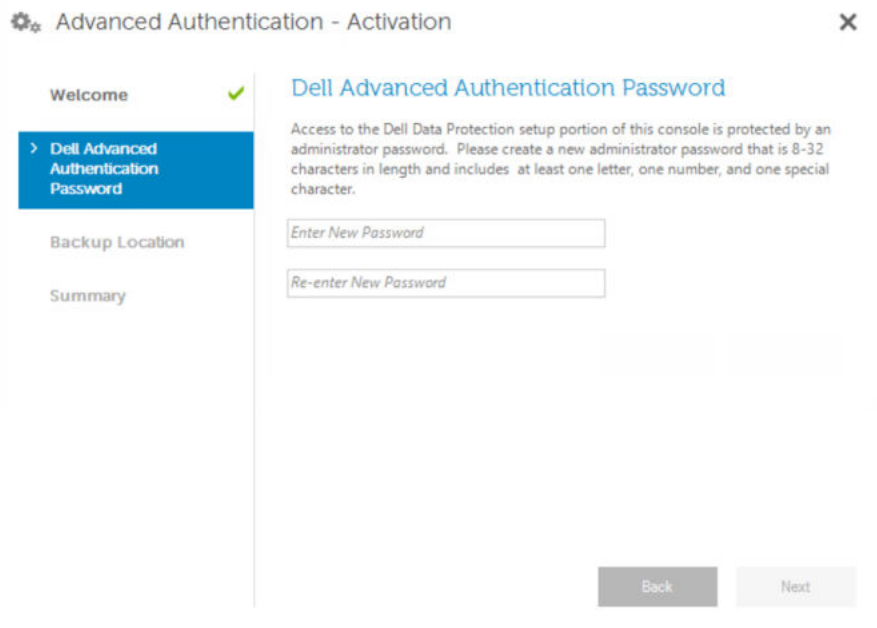
Advanced Authentication and Encryption Personal Setup Wizards

Log on with your Windows user name and password. You are seamlessly passed through to Windows. The interface may look different than you are accustomed to seeing.

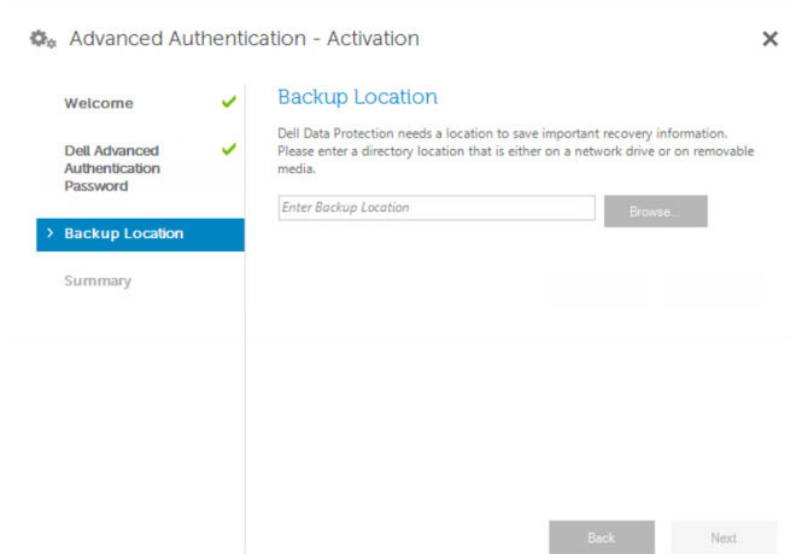
- 1 You may be prompted by UAC to run the application. If so, click Yes.
- 2 After the initial installation reboot, the Advanced Authentication activation wizard displays. Click **Next**.



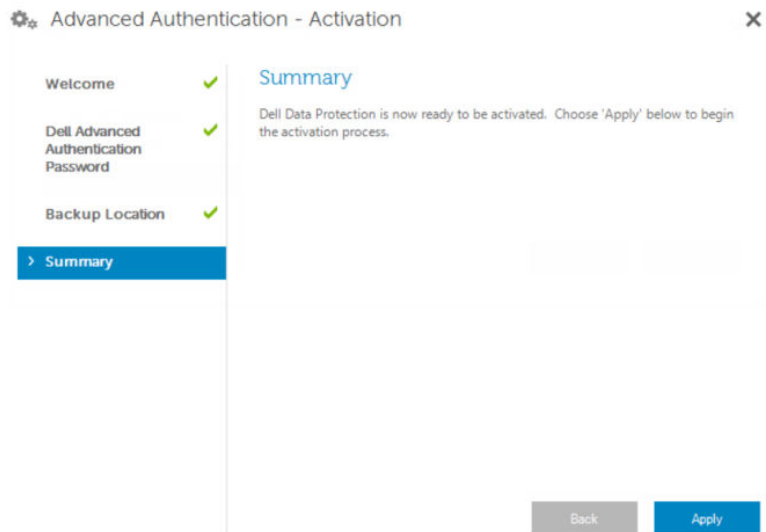
- 3 Type and re-enter a new Encryption Administrator Password (EAP). Click **Next**.



- 4 Enter a backup location on a network drive or removable media to store recovery information and click **Next**.



- 5 Click **Apply** to begin Advanced Authentication activation.



After the Advanced Authentication activation wizard is finished, proceed to the next step.

- 6 Launch the Encryption Personal setup wizard from the Dell Encryption icon in the notification area (it may launch on its own). This Setup Wizard helps you use encryption to protect the information on this computer. If this wizard is not completed, encryption cannot begin.

Read the Welcome screen and click **Next**.



- 7 Select a policy template. The policy template establishes the default policy settings for encryption. You can easily apply a different policy template or customize the selected template in the Local Management Console once initial configuration is complete.

Click **Next**.



- 8 Read and acknowledge the Windows password warning. If you wish to create a Windows password now, see [Requirements](#).
- 9 Create a 8-127 character Encryption Administrator Password (EAP) and confirm. The password should contain alphabetic, numeric, and special characters. This password can be the same as the EAP you set up for Advanced Authentication, but is not related to it. **Record and save this password in a safe place.** Click **Next**.



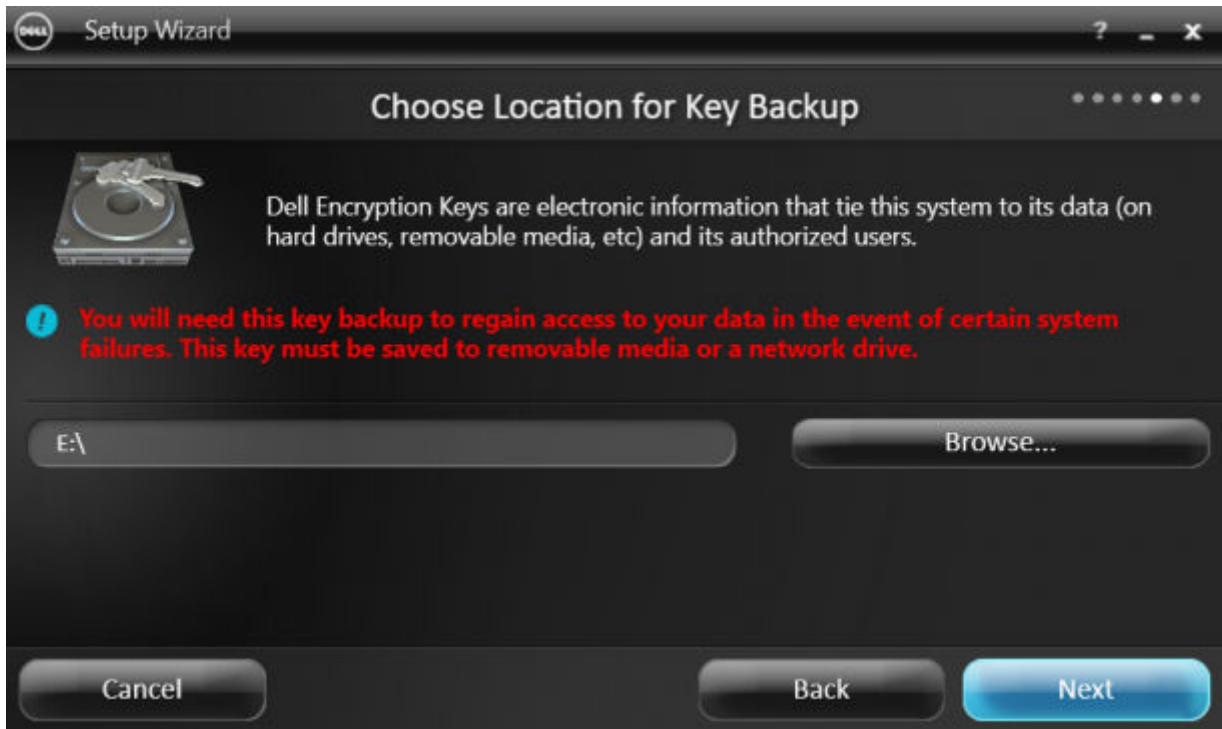
- 10 Click **Browse** to choose a network drive or removable storage to back up your encryption keys (which are wrapped in an application named LSARecovery_[hostname].exe).

In the event of certain computer failures, these keys are used to recover your data.

In addition, future policy changes sometimes require that your encryption keys get backed up again. If the network drive or removable storage is available, backing up of your encryption keys is done in the background. However, if the location is not available (such as the original removable storage device not being inserted into the computer), policy changes do not take effect until the encryption keys are manually backed up.

NOTE: To learn how to manually back up encryption keys, click "? > Help" in the upper right corner of the Local Management Console or click Start > Dell > Encryption Help.

Click **Next**.



- 11 On the Confirm Encryption Settings screen, a list of Encryption Settings display. Review the items and when satisfied with the settings, click **Confirm**.

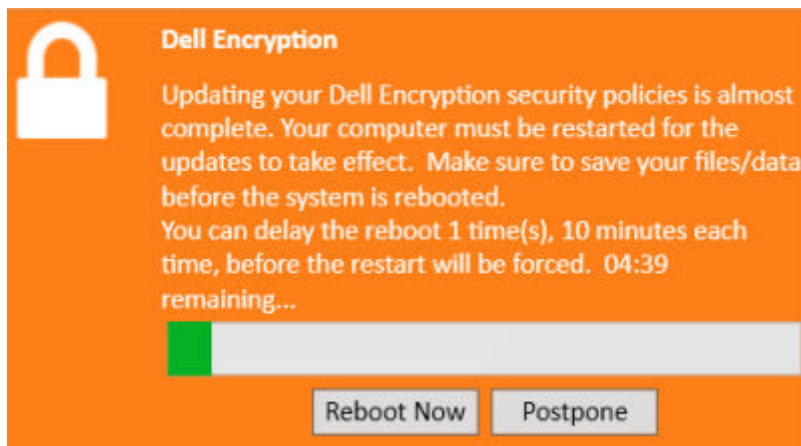


Configuration of the computer begins. A status bar informs you of the progress of configuration.

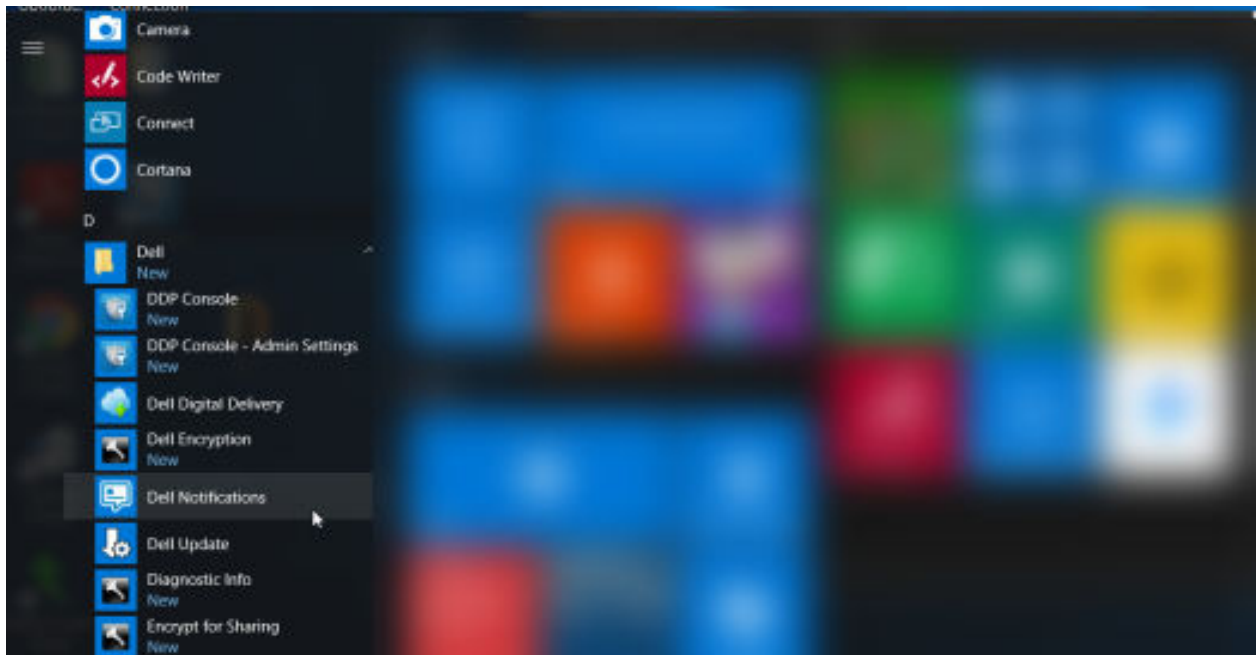
- 12 Click **Finish** to complete the configuration.



- 13 A reboot is required once the computer is configured for encryption. Click **Reboot Now** or you can postpone the reboot 5x20 minutes each.

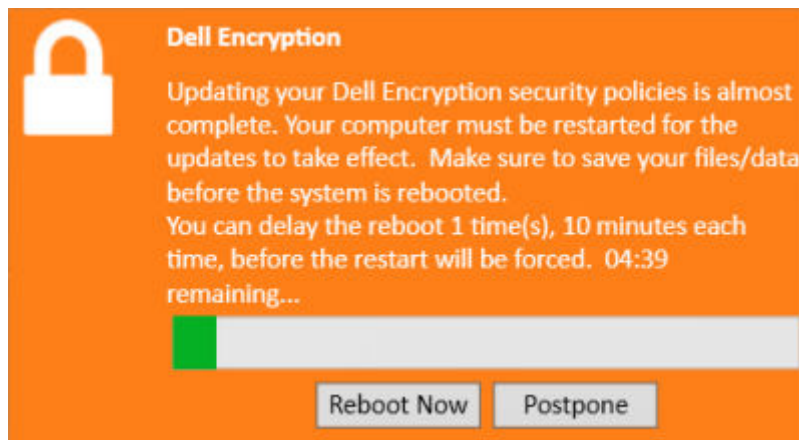


- 14 Once the computer is rebooted, open the Local Management Console from the Start menu to see the status of encryption.

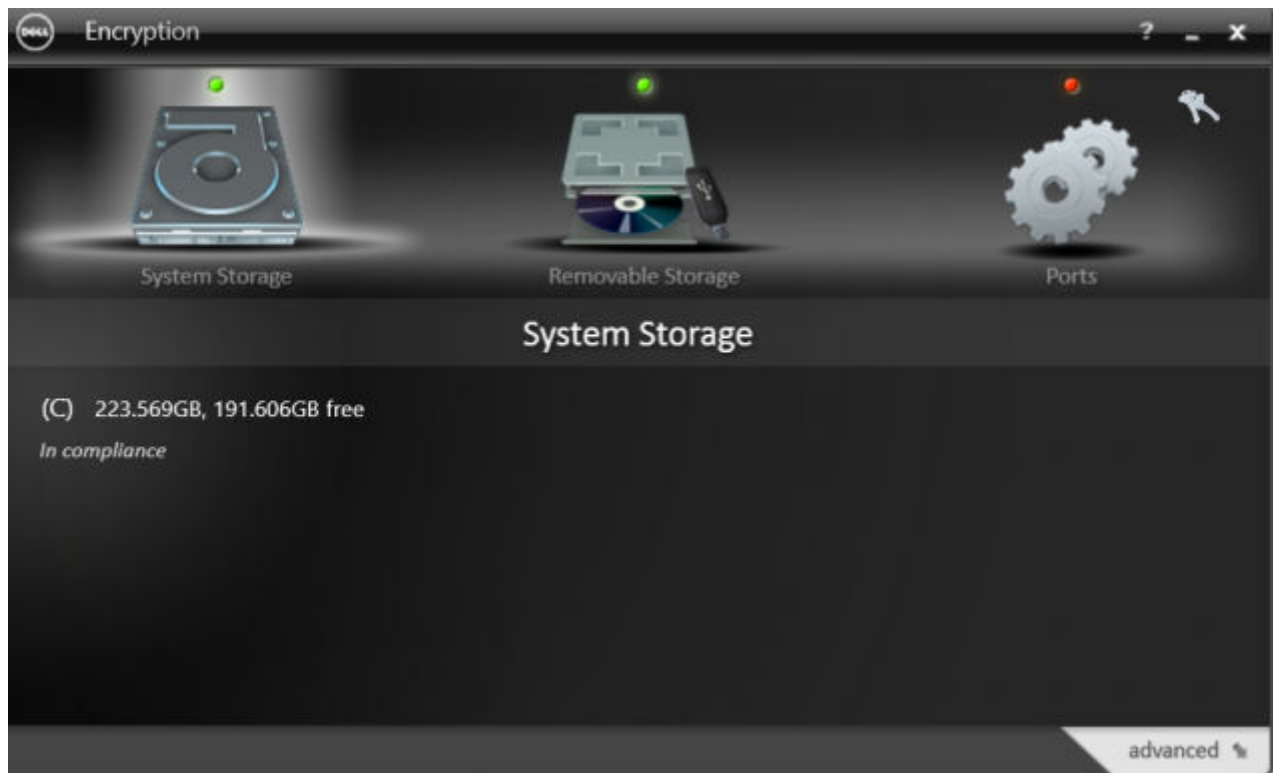


Encryption takes place in the background. The Local Management Console can be opened or closed. Either way, encryption of files progresses. You can continue to use your computer as usual while it is encrypting.

- 15 When the scan is complete, the computer reboots once more.



Once all encryption sweeps and reboots are complete, you can verify compliance status by launching the Local Management Console. The drive is0 labeled as "In Compliance".



Configure Dell Encryption Management Agent Settings

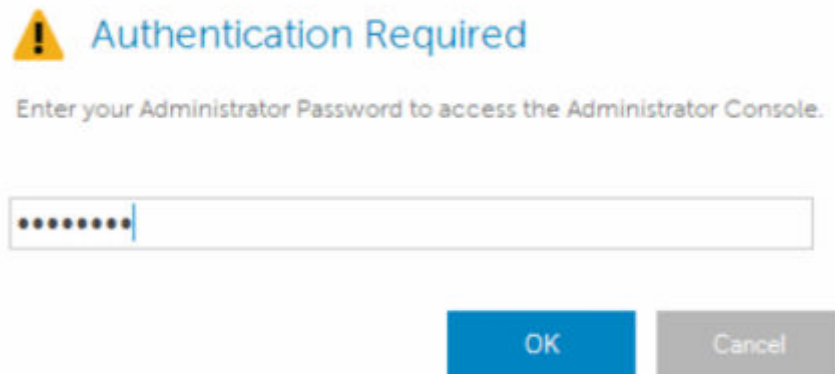
Default settings allow administrators and users to use advanced authentication immediately after activation, without additional configuration. Users are automatically added as advanced authentication users when they log on to the computer with their Windows passwords but, by default, multi-factor Windows authentication is not enabled.

To configure advanced authentication features, you must be an administrator on the computer.

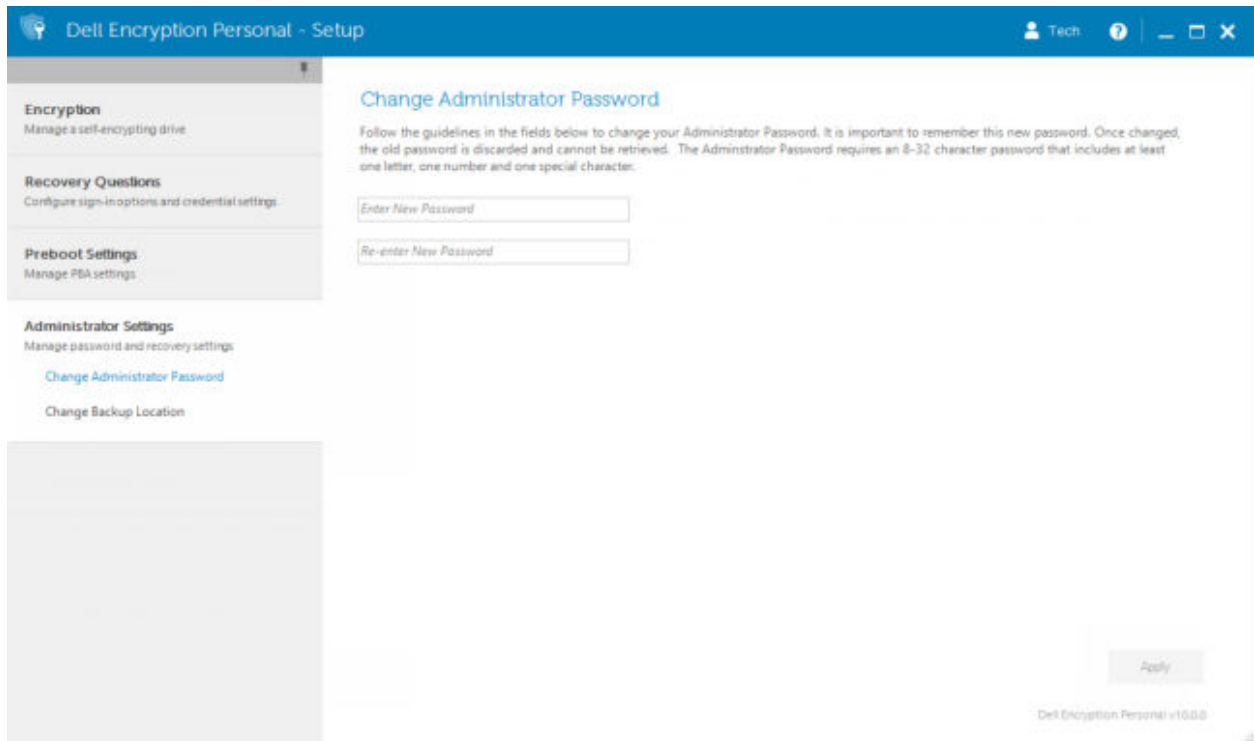
Change the Administrator Password and Backup Location

After advanced authentication activation, the administrator password and backup location can be changed, if necessary.

- 1 As an administrator, launch the Dell Data Security Console from the desktop shortcut.
- 2 Click the **Administrator Settings** tile.
- 3 In the Authentication dialog, enter the administrator password that was set up during activation, and click **OK**.

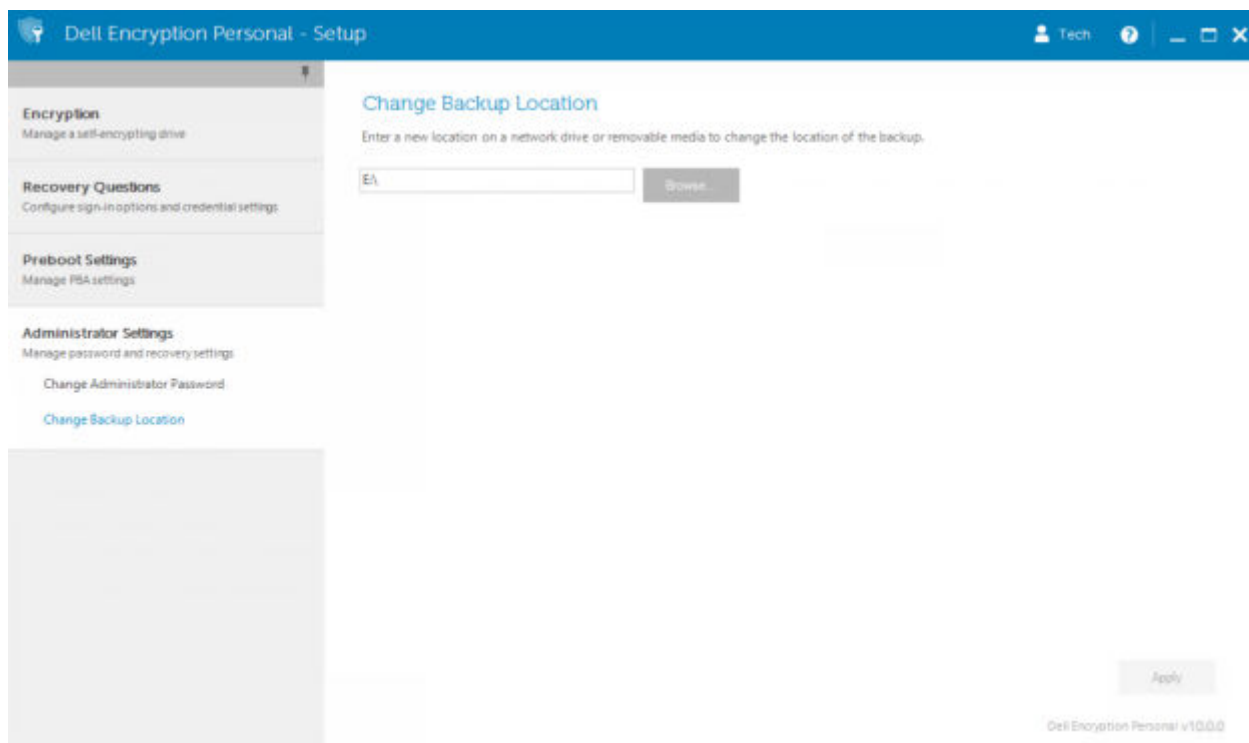


- 4 Click the **Administrator Settings** tab.
- 5 In the Change Administrator Password page, to change the password, enter a new password that is between 8-32 characters and includes at least one letter, one number, and one special character.



- 6 Enter the password a second time to confirm it, then click **Apply**.
 - 7 To change the location where the recovery key is stored, in the left pane, select **Change Backup Location**.
 - 8 Select a new location for the backup, and click **Apply**.
- The backup file must be saved either on a network drive or onto removable media. The backup file contains the keys that are needed to recover data on this computer. Dell ProSupport must have access to this file to help you recover data.

Recovery data is automatically backed up to the specified location. If the location is not available (for instance, if your backup USB drive is not inserted), Advanced Authentication prompts for a location to back up your data. Access to recovery data is required to begin encryption.



Configure Encryption and Preboot Authentication

Encryption and Preboot Authentication (PBA) are available if your computer is equipped with a self-encrypting drive (SED). Both are configured through the Encryption tab, which is visible only if your computer is equipped with a self-encrypting drive (SED). When you enable either encryption or PBA, the other is also enabled.

To configure encryption and Preboot Authentication:

- 1 In the Data Security Console, click the **Administrator Settings** tile.
- 2 Ensure that the backup location is accessible from the computer.

NOTE: If *Backup Location not found* displays and the backup location is on a USB drive, either your drive is not connected or is connected to a different slot than the one you used during backup. If the message displays, and the backup location is on a network drive, the network drive is inaccessible from the computer. If it is necessary to change the backup location, from the Administrator Settings tab, select **Change Backup Location** to change the location to the current slot or accessible drive. A few seconds after reassigning the location, the process of enabling encryption can proceed.

- 3 Click the **Encryption** tab and then click **Encrypt**.
- 4 At the Welcome page, click **Next**.
- 5 In the Preboot Policy page, change or confirm the following values, and click **Next**.

Attempts at non-cached user login	Number of times an unknown user can attempt to log in (a user that has not logged in to the computer before [no credentials have been cached]).
Attempts at cached user login	Number of times can a known user attempt to log in.
Attempts at answering recovery questions	Number of times the user can attempt to enter the correct answer.
Enable Crypto Erase Password	Select to enable.
Enter the Crypto Erase Password	A word or code of up to 100 characters used as a fail-safe security mechanism. Entering this word or code in the user name or password field during the PBA authentication

deletes the authentication tokens for all users and locks the SED. Afterward, only an administrator can forcibly unlock the device.

Leave this field blank if you do not want to have a crypto erase password available in case of emergency.

Remember Me

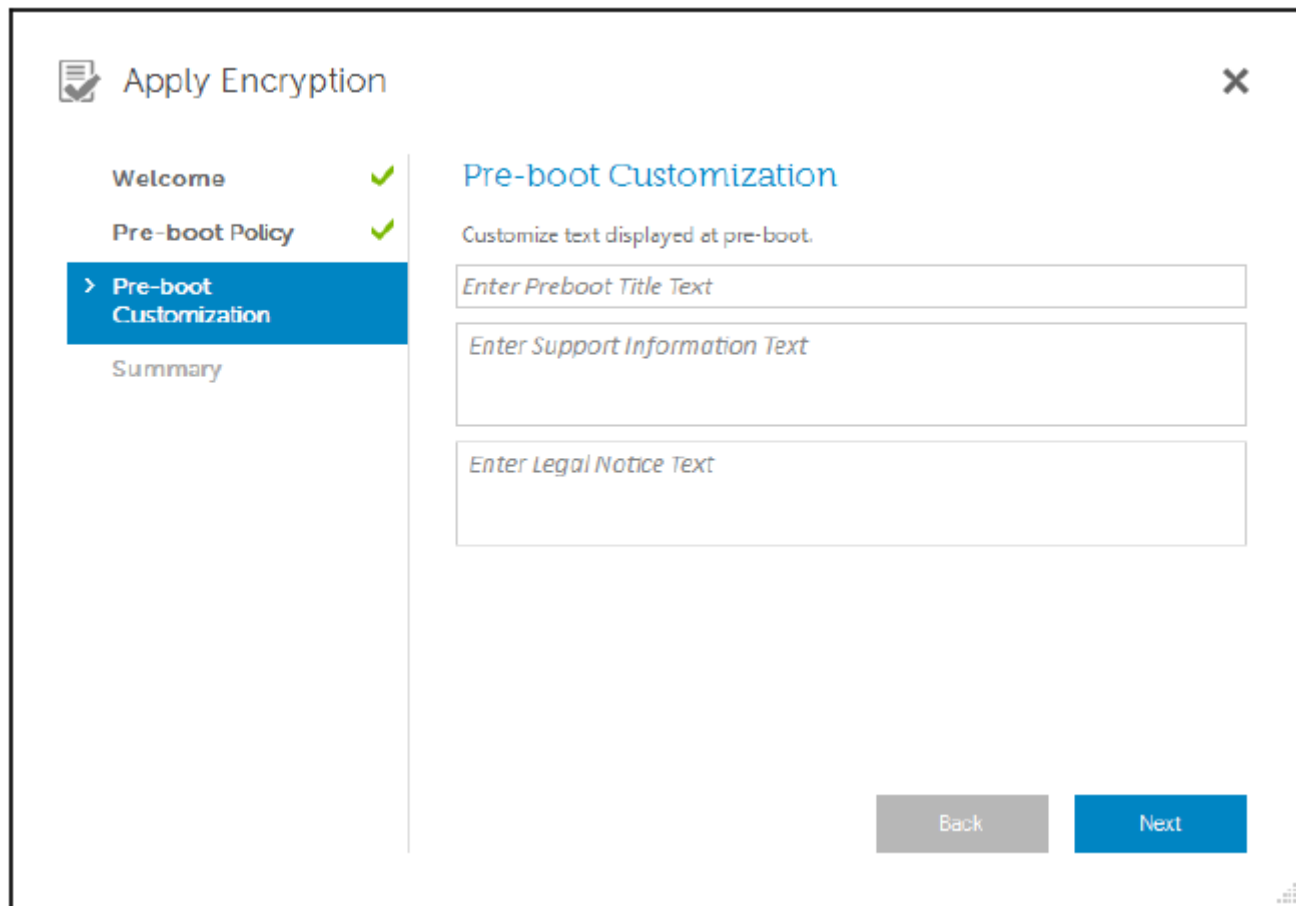
Enables or disables the ability for users to select Remember Me on the PBA login screen.

6 In the Preboot Customization page, enter customized text to display on the Preboot Authentication (PBA) screen, and click **Next**.

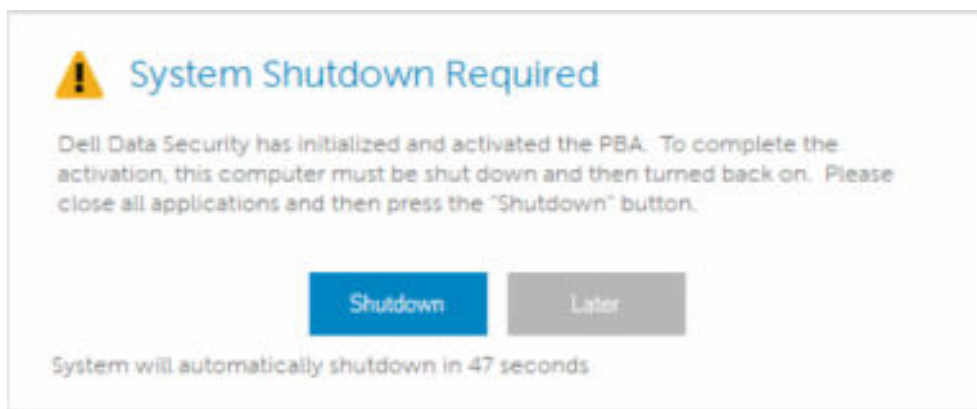
Preboot Title Text This text displays on the top of the PBA screen. If you leave this field blank, no title will be displayed. The text does not wrap, so entering more than 17 characters may result in the text being cut off.

Support Information Text This text displays on the PBA support information page. Dell recommends that you customize the message to include specific instructions about how to contact the help desk or security administrator. Not entering text in this field results in no support contact information being available for the user. Text wrapping occurs at the word level, not the character level. For instance, if you have a single word that is more than approximately 50 characters in length, it does not wrap and no scroll bar is present, therefore the text is truncated.

Legal Notice Text This text displays before the user is allowed to log on to the device. For example: "By clicking OK, you agree to abide by the acceptable computer use policy." Not entering text in this field results in no text or OK/Cancel buttons being displayed. Text wrapping occurs at the word level, not the character level. For instance, if you have a single word that is more than approximately 50 characters in length, it does not wrap and no scroll bar is present, therefore the text is truncated.



- 7 At the Summary page, click **Apply**.
- 8 When prompted, click **Shutdown**.
A full shutdown is required before encryption can begin.



- 9 After shutdown, restart the computer.
Authentication is now managed by the Encryption Management Agent. Users must log in at the Preboot Authentication screen with their Windows passwords.

Change Encryption and Preboot Authentication Settings

After you first enable encryption and configure Preboot Policy and Customization, the following actions are available from the Encryption tab:

- Change Preboot Policy or Customization - Click the **Encryption** tab and then click **Change**.
- Decrypt the SED, for example for uninstallation - Click **Decrypt**.

After you first enable encryption and configure Preboot Policy and Customization, the following actions are available from the Preboot Settings tab:

- Change Preboot Policy or Customization - Click the **Preboot Settings** tab and select either **Preboot Customization** or **Preboot Logon Policies**.

Manage Users' Authentication

Remove All of a User's Enrolled Credentials

- 1 Click the **Administrator Settings** tile and authenticate with your password.
- 2 Click the **Users** tab and find the user you want to remove.
- 3 Click **Remove**. (The Remove command appears in red at the bottom of the user's settings).
After removal, the user will not be able to log on to the computer unless they re-enroll.

Uninstall 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 another chapter that contains *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.

- 1 [Uninstall Encryption Client](#).
- 2 [Uninstall Encryption Management Agent](#).

The Driver package does not need to be uninstalled.

Proceed to [Choose an Uninstallation Method](#).

Choose an Uninstallation Method

There are two methods to uninstall the master installer, select **one** of the following:

- [Uninstall from Add/Remove Programs](#)
- [Uninstall from the Command Line](#)

Uninstall Interactively

- 1 Go to *Uninstall a Program* in the Windows Control Panel (in the search box on the taskbar, type **Control Panel**, then select Control Panel from the results).
- 2 Highlight **Dell Installer** and left-click **Change** to launch the Setup Wizard.
- 3 Read the Welcome screen and click **Next**.
- 4 Follow the prompts to uninstall and click **Finish**.
- 5 Restart your computer and log in to Windows.
The master installer is uninstalled.

Uninstall from the Command Line

- The following example silently uninstalls the master installer.

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

Reboot the computer when finished.

The master installer is uninstalled.

Proceed to [Uninstall Using the Child Installers](#).

Uninstall Using the Child Installers

- Dell recommends using the [Data Security Uninstaller](#) to remove Encryption Personal.
- The user performing decryption and uninstallation must be a local or domain administrator. If uninstalling by command line, domain administrator credentials are required.
- If you installed Encryption Personal with the master installer, the child executable files must first be extracted from the master installer before uninstallation, as shown in [Extract the Child Installers from the Master Installer](#).
- Ensure that the same version of clients is used for uninstallation as installation.
- 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 failures because of locked files.

Uninstall Encryption Client

- **Before beginning the uninstall process**, see [\(Optional\) Create an Encryption Removal Agent Log File](#). This log file is useful for troubleshooting an uninstall/decryption operation. If you do not intend to decrypt files during the uninstall process, you do not need to create an Encryption Removal Agent log file.
- Run WSScan to ensure that all data is decrypted after uninstallation is complete, but before restarting the computer. See [Use WSScan](#) for instructions.
- Periodically [Check Encryption Removal Agent Status](#). Data decryption is still in process if the Encryption Removal Agent Service still exists in the Services panel.

Choose an Uninstallation Method

There are two methods to uninstall the Encryption client, select **one** of the following:

- [Uninstall Interactively](#)
- [Uninstall from the Command Line](#)

Uninstall Using the User Interface

- 1 Go to *Uninstall a Program* in the Windows Control Panel (in the search box on the taskbar, type **Control Panel**, and then select **Control Panel** from the results).
- 2 Highlight **Dell Encryption XX-bit** and left-click **Change** to launch the Encryption Personal Setup Wizard.
- 3 Read the Welcome screen and click **Next**.
- 4 At the Encryption Removal Agent Installation screen, select either:

NOTE: The second option is enabled by default. If you wish to decrypt files, be sure you change the selection to option one.

- Encryption Removal Agent - Import Keys from a File

For SDE, User, or Common encryption, this option decrypts files and uninstalls the Encryption client. ***This is the recommended selection.***

- Do not install Encryption Removal Agent

This option uninstalls the Encryption client *but does not decrypt files*. This option should be used **only** for troubleshooting purposes, as directed by Dell ProSupport.

Click **Next**.

- 5 In *Backup File*, enter the path to the network drive or removable media location of the backup file or click **...** to browse to the location. The format of the file is LSARecovery_[hostname].exe.

Enter your Encryption Administrator Password. This is the password from Setup Wizard when the software was installed.

Click **Next**.

- 6 At *Dell Decryption Agent Service Logon As* select **Local System Account** and click **Finish**.
- 7 Click **Remove** at the Remove the Program screen.
- 8 Click **Finish** at the Configuration Complete screen.
- 9 Restart your computer and log on to Windows.

Decryption is now in progress.

The decryption process could take several hours, depending on the number of drives being decrypted and the amount of data on those drives. To check the decryption process, see [Check Encryption Removal Agent Status](#).

Uninstall from the Command Line

- 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 to create a log file by using **/I 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
/s	Silent mode
/x	Uninstall mode

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

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

- 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: 2 - Get keys using a forensic key bundle 0 - Do not install Encryption Removal Agent
CMGSILENTMODE	Property for silent uninstallation: 1 - Silent 0 - Not Silent
DA_KM_PW	The password for the domain administrator account.
DA_KM_PATH	Path to the key material bundle.

- The following example uninstalls the Encryption client without installing Encryption Removal Agent.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

- The following example uninstalls the Encryption client using a forensic key bundle. Copy the forensic key bundle to the local disk and then run this command.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Reboot the computer when finished.

The decryption process could take several hours, depending on the number of drives being decrypted and the amount of data on those drives. To check the decryption process, see [Check Encryption Removal Agent Status](#).

Uninstall Encryption Management Agent

Choose an Uninstallation Method

There are two methods to uninstall the Encryption client, select **one** of the following:

- [Uninstall Interactively](#)
- [Uninstall from the Command Line](#)

Uninstall Using the User Interface

- 1 Go to *Uninstall a Program* in the Windows Control Panel (in the search box on the taskbar, type **Control Panel**, and then select **Control Panel** from the results).
- 2 Highlight **Dell Encryption Management Agent** and left-click **Change** to launch the Setup Wizard.
- 3 Read the Welcome screen and click **Next**.
- 4 Follow the prompts to uninstall and click **Finish**.
- 5 Restart your computer and log on to Windows.

Client Security Framework is uninstalled.

Uninstall from the Command Line

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

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

Shut down and restart the computer when finished.

Data Security Uninstaller

Uninstall Encryption Personal

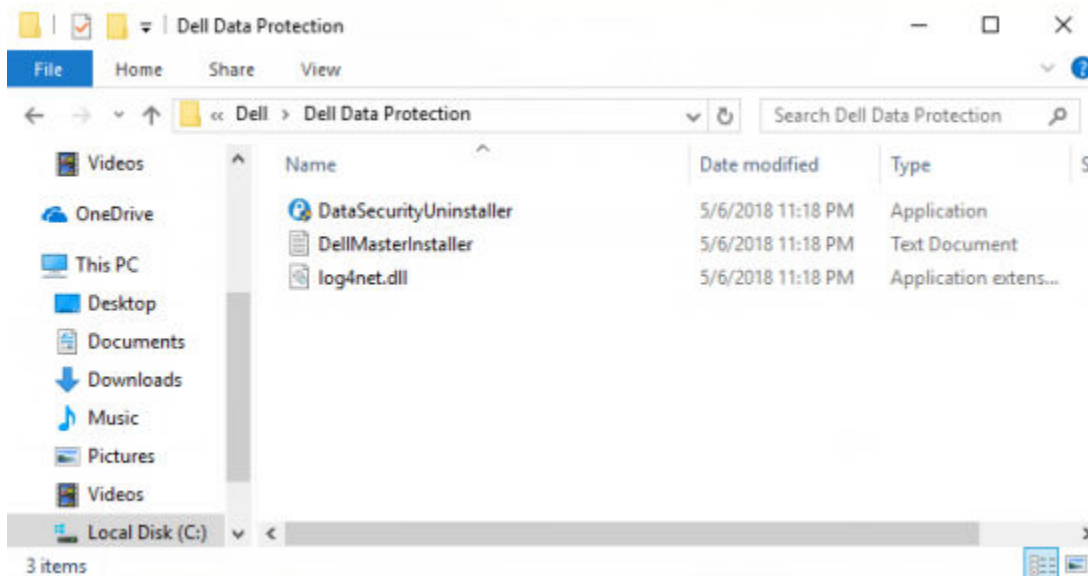
Dell provides the Data Security Uninstaller as a master uninstaller. This utility gathers the currently installed products and removes them in the appropriate order.

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

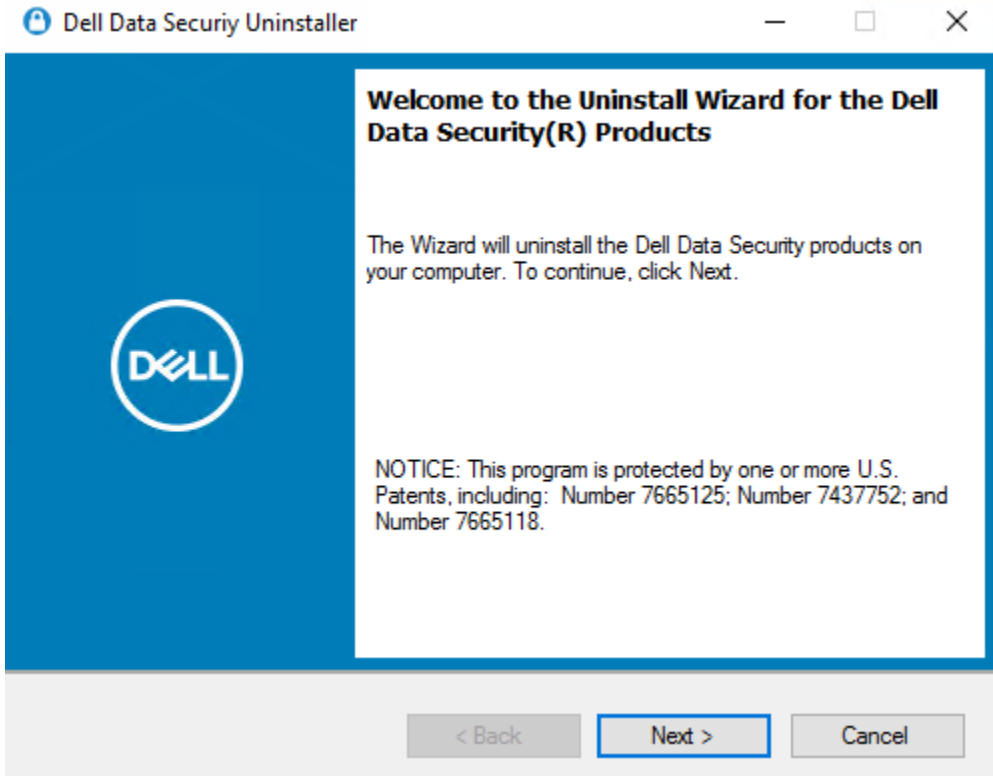
For more information or to use command line interface (CLI), see KB article [SLN307791](#).

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

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

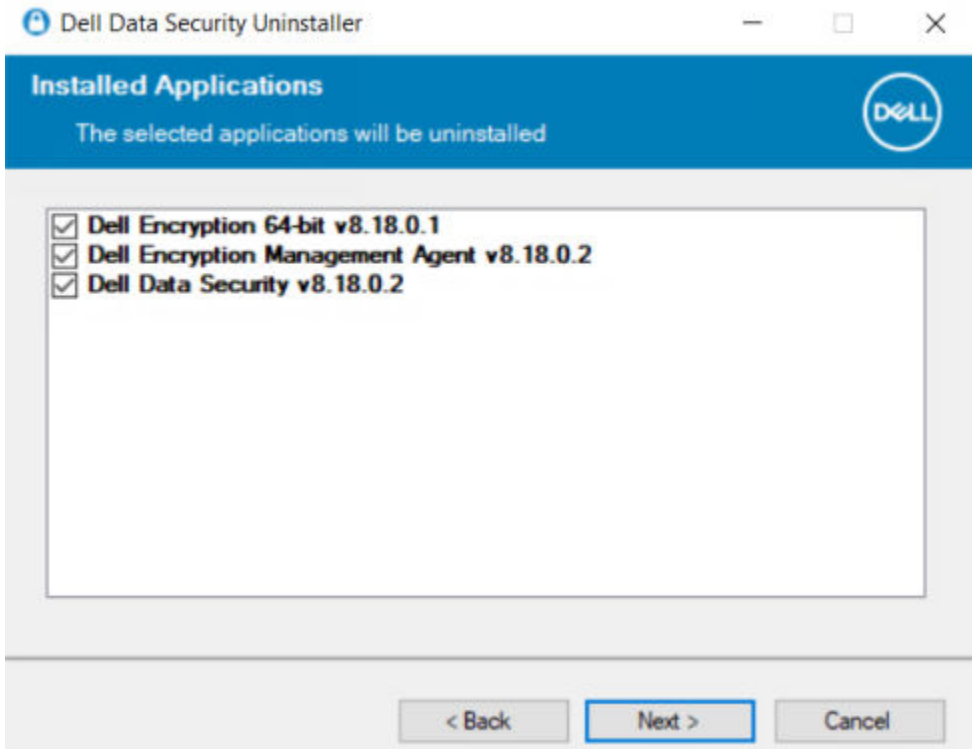


Click **Next**.

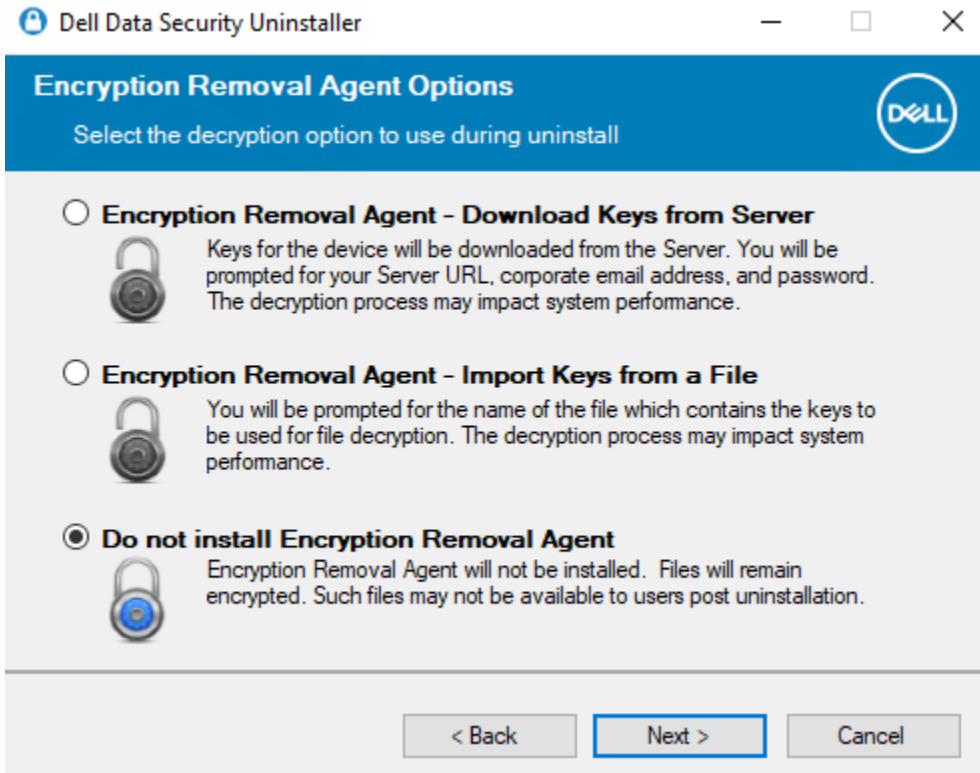


Optionally clear any application from removal and click **Next**.

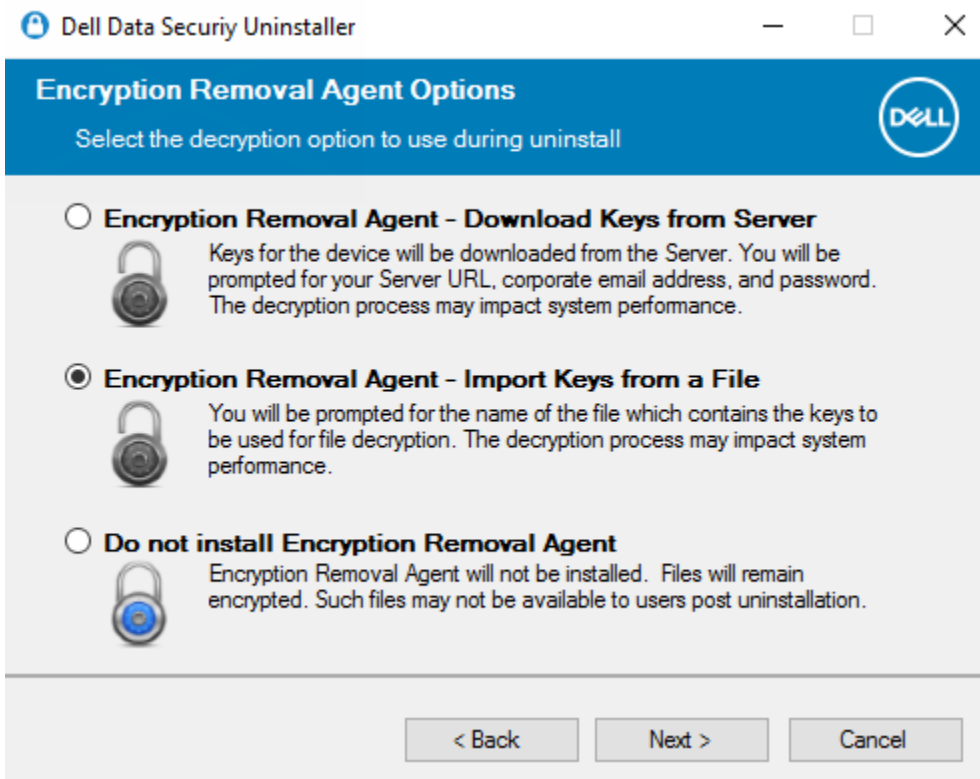
NOTE: Required dependencies are automatically selected or cleared.



To remove applications without installing the Encryption Removal Agent, choose **Do not install Encryption Removal Agent** and select **Next**.



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



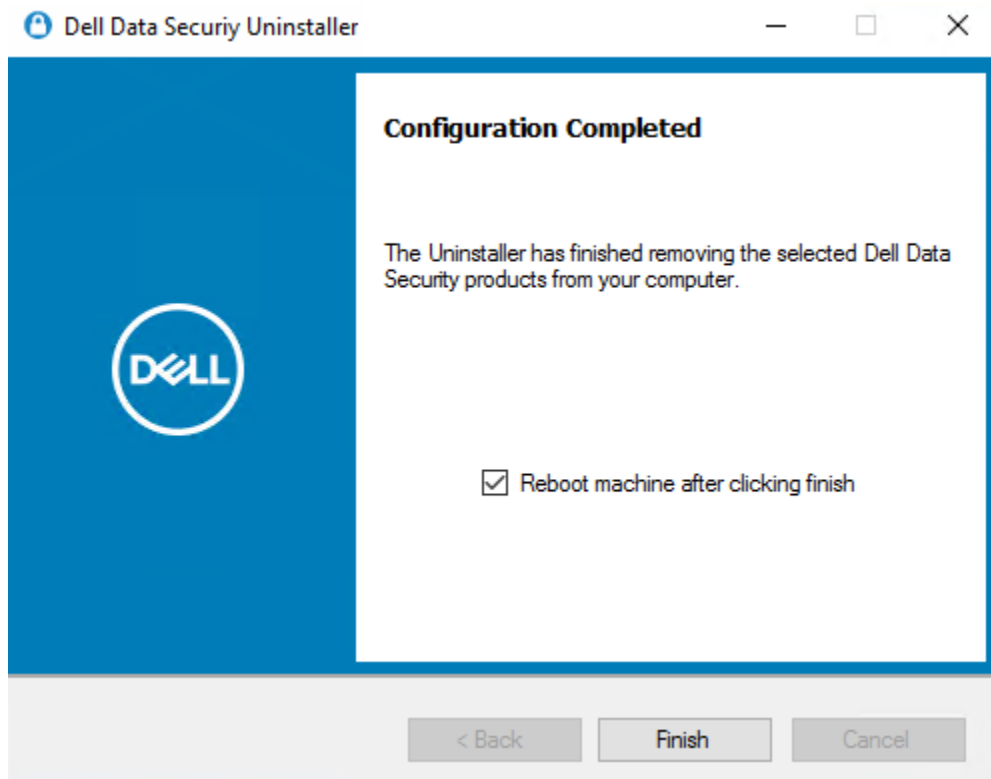
Browse to the location of the recovery keys and then enter the Passphrase for the file and click **Next**.

The screenshot shows a window titled "Dell Data Security Uninstaller" with a blue header bar. The header contains the text "User Encryption Key Information" and the Dell logo. Below the header, it says "Provide the information to download the forensic key files". The main area contains the text "Key files are downloaded from a server using an administrative tool, like CmgAd". There are two input fields: "Downloaded File:" with a text box containing "Location of BackUp File" and a browse button (three dots), and "Passphrase:" with a text box containing ten dots and a visibility toggle icon. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Select **Remove** to begin the uninstall.

The screenshot shows a window titled "Dell Data Security Uninstaller" with a blue header bar. The header contains the text "Remove the Applications" and the Dell logo. Below the header, it says "You have chosen to remove the Dell Data Security application(s)". The main area contains the text "Click Remove to remove Dell Data Security from your computer. After removal, this program(s) will no longer be available for use." and "If you want to review or change any settings, click Back.". At the bottom, there are three buttons: "< Back", "Remove", and "Cancel".

Click **Finish** to complete removal and reboot the computer. **Reboot machine after clicking finished** is selected by default.



Uninstallation and removal is complete.

Policies and Template Descriptions

Tooltips display when you hover your mouse over a policy in the Local Management Console.

Policies

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Fixed Storage Policies										
SDE Encryption Enabled	True								False	<p>This policy is the "master policy" for all other System Data Encryption (SDE) policies. If this policy is False, no SDE encryption takes place, regardless of other policy values.</p> <p>A True value means that all data not encrypted by other Intelligent Encryption policies is encrypted per the SDE Encryption Rules policy.</p> <p>Changing the value of this policy requires a reboot.</p>
SDE Encryption Algorithm	AES256									AES-256, AES-128, 3DES
SDE Encryption Rules										<p>Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders.</p> <p>Contact Dell ProSupport for guidance if you are unsure about changing the default values.</p>
General Settings Policies										
Encryption Enabled	True								False	<p>This policy is the "master policy" for all General Settings policies. A False value means</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										<p>that no encryption takes place, regardless of other policy values.</p> <p>A True value means that all encryption policies are enabled.</p> <p>Changing the value of this policy triggers a new sweep to encrypt/decrypt files.</p>
Common Encrypted Folders										<p>String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters)</p> <p>A list of folders on endpoint drives to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the endpoint.</p> <p>The available drive letters are:</p> <p>#: Refers to all drives</p> <p>f#: Refers to all fixed drives</p> <p>r#: Refers to all removable drives</p> <p>Important: Overriding directory protection can result in an unbootable computer and/or require reformatting drives.</p> <p>If the same folder is specified in both this policy and the User Encrypted Folders policy, this policy prevails.</p>
Common Encryption Algorithm	AES256									<p>AES-256, Rijndael 256, AES 128, Rijndael 128, 3DES</p> <p>System paging files are encrypted using AES-128.</p>
Application Data Encryption List	winword.exe excel.exe powerpnt.exe msaccess.exe									<p>String - maximum of 100 entries of 500 characters each</p> <p>Dell recommends not adding explorer.exe or iexplorer.exe to the ADE list, as unexpected or unintended results may occur.</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										<p>winproj.exe</p> <p>outlook.exe</p> <p>acrobat.exe</p> <p>visio.exe</p> <p>mspub.exe</p> <p>notepad.exe</p> <p>wordpad.exe</p> <p>winzip.exe</p> <p>winrar.exe</p> <p>onenote.exe</p> <p>onenotem.exe</p>
										<p>However, explorer.exe is the process used to create a new Notepad file on the desktop using the right-click menu. Setting encryption by file extension, instead of the ADE list, provides more comprehensive coverage.</p> <p>List process names of applications (without paths) whose new files you want encrypted, separated by carriage returns. Do not use wildcards.</p> <p>Dell recommends not listing applications/installers that write system-critical files. Doing so could result in encryption of important system files, which could make a computer unbootable.</p> <p>Common process names:</p> <p>outlook.exe, winword.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe</p> <p>The following hard-coded system and installer process names are ignored if specified in this policy:</p> <p>hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe</p>
Application Data Encryption Key	Common									<p>Common or User</p> <p>Choose a key to indicate who can access files encrypted by Application Data Encryption List, and where.</p> <p>Common for these files to be accessible to all managed users on the endpoint where they were created (the same level of access as Common Encrypted Folders), and</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										<p>encrypted with the Common encryption algorithm.</p> <p>User for these files to be accessible only to the user who created them, only on the endpoint where they were created (the same level of access as User Encrypted Folders), and encrypted with the User encryption algorithm.</p> <p>Changes to this policy do not affect files already encrypted because of this policy.</p>
Encrypt Outlook Personal Folders	True							False		True encrypts Outlook Personal Folders.
Encrypt Temporary Files	True							False		True encrypts the paths listed in the environment variables TEMP and TMP with the User data encryption key.
Encrypt Temporary Internet Files	True	False								<p>True encrypts the path listed in the environment variable CSIDL_INTERNET_CACHE with the User data encryption key.</p> <p>To reduce encryption sweep time, the client clears the contents of CSIDL_INTERNET_CACHE for initial encryption, as well as updates to this policy.</p> <p>This policy is applicable when using Microsoft Internet Explorer only.</p>
Encrypt User Profile Documents	True								False	<p>True encrypts:</p> <ul style="list-style-type: none"> · The users profile (C:\Users\jsmith) with the User data encryption key · \Users\Public with the Common encryption key
Encrypt Windows Paging File	True								False	True encrypts the Windows paging file. A change to this policy requires a reboot.

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Managed Services										<p>String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters)</p> <p>When a service is managed by this policy, the service is started only after the user is logged in and the client is unlocked. This policy also ensures that the service managed by this policy is stopped before the client is locked during logoff. This policy can also prevent a user logoff if a service is unresponsive.</p> <p>Syntax is one service name per line. Spaces in the service name are supported.</p> <p>Wildcards are not supported.</p> <p>Managed services are not started if an unmanaged user logs on.</p>
Secure Post-Encryption Cleanup	Three Pass Overwrite	Single Pass Overwrite							No Overwrite	<p>No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pass Overwrite</p> <p>Once folders specified via other policies in this category have been encrypted, this policy determines what happens to the unencrypted residue of the original files:</p> <ul style="list-style-type: none"> · No Overwrite deletes it. This value yields the fastest encryption processing. · Single-pass Overwrite overwrites it with random data. · Three-pass Overwrite overwrites it with a standard pattern of 1s and 0s, then with its complement, and then with random data. · Seven-pass Overwrite overwrites it with a standard

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										pattern of 1s and 0s, then with its complement, and then with random data five times. This value makes it most difficult to recover the original files from memory, and yields the most secure encryption processing.
Secure Windows Hibernation File	True					False		True	False	When enabled, the hibernation file is encrypted only when the computer enters hibernation. The client disengages protection when the computer comes out of hibernation, providing protection without impacting users or applications while the computer is in use.
Prevent Unsecured Hibernation	True					False		True	False	When enabled, the client does not allow computer hibernation if the client is unable to encrypt the hibernation data.
Workstation Scan Priority	High	Norm								Highest, High, Normal, Low, Lowest Specifies the relative Windows priority of encrypted folder scanning.
User Encrypted Folders										String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters) A list of folders on the endpoint hard drive to be encrypted with the User data encryption key or excluded from encryption. This policy applies to all drives classified by Windows as Hard Disk Drives. You cannot use this policy to encrypt drives or removable media whose type displays as Removable Disk, use EMS Encrypt External Media instead.
User Encryption Algorithm	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
User Data Encryption Key	User	Common		User	Common				User	<p>Encryption algorithm used to encrypt data at the individual user level. You can specify different values for different users of the same endpoint.</p> <p>Common or User</p> <p>Choose a key to indicate who can access files encrypted by the following policies, and where:</p> <ul style="list-style-type: none"> · User Encrypted Folders · Encrypt Outlook Personal folders · Encrypt Temporary Files (\Documents and Settings \username\Local Settings \Temp only) · Encrypt Temporary Internet Files · Encrypt User Profile Documents <p>Select:</p> <ul style="list-style-type: none"> · Common for User Encrypted Files/Folders to be accessible by all managed users on the endpoint where they were created (the same level of access as Common Encrypted Folders), and encrypted with the Common encryption algorithm. · User for these files to be accessible only to the user who created them, only on the endpoint where they were created (the same level of access as User Encrypted Folders), and encrypted with the User encryption algorithm. <p>If you elect to incorporate an encryption policy to encrypt entire disk partitions, it is recommended to use the default SDE encryption policy, rather than Common or User.</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										This ensures that any operating system files that are encrypted are accessible during states when the managed user is not logged in.
Hardware Crypto Accelerator (supported only with v8.3 through v8.9.1 Encryption clients)										
Hardware Crypto Accelerator (HCA)	False									<p>This policy is the “master policy” for all other Hardware Crypto Accelerator (HCA) policies. If this policy is False, no HCA encryption takes place, regardless of other policy values.</p> <p>HCA policies can only be used on computers equipped with a Hardware Crypto Accelerator.</p>
Volumes Targeted for Encryption	All Fixed Volumes									<p>All Fixed Volumes or System Volume Only</p> <p>Specify which volume(s) to target for encryption.</p>
Forensic Meta Data Available on Encrypted Drive	False									<p>True or False</p> <p>When True, forensics meta data is included on the drive to facilitate forensics. Meta data included:</p> <ul style="list-style-type: none"> Machine ID (MCID) of the current machine Device ID (DCID/SCID) of the current Encryption client installation <p>When False, forensics meta data is not included on the drive.</p> <p>Switching from False to True re-sweeps, based on the policies to add forensics.</p>
Allow User Approval of Secondary Drive Encryption	False									True allows users to decide if additional drives are encrypted.
Encryption Algorithm	AES256									AES-256 or AES-128

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Port Control Policies										
Port Control System	Disabled									<p>Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies.</p> <p>Note: PCS policies require a reboot before the policy takes effect.</p>
Port: Express Card Slot	Enabled									Enable, Disable, or Bypass ports exposed through the Express Card Slot.
Port: eSATA	Enabled									Enable, Disable, or Bypass port access to external SATA ports.
Port: PCMCIA	Enabled									Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled									Enable, Disable, or Bypass port access to external Firewire (1394) ports.
Port: SD	Enabled									Enable, Disable, or Bypass port access to SD card ports.
Subclass Storage: External Drive Control	Blocked	Read Only			Full Access			Read Only	Full Access	<p>CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy.</p> <p>This policy has interactions with PCS. See Encryption External Media and PCS Interactions.</p> <p>Full Access: External Drive port does not have read/write data restrictions applied</p> <p>Read Only: Allows read capability. Write data is disabled</p> <p>Blocked: Port is blocked from read/write capability</p> <p>This policy is endpoint-based and cannot be overridden by user policy.</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Port: Memory Transfer Device (MTD)	Enabled									Enable, Disable, or Bypass access to Memory Transfer Device (MTD) ports.
Class: Storage	Enabled									PARENT to the next 3 policies. Set this policy to Enabled to use the next 3 Subclass Storage policies. Setting this policy to Disabled disables all 3 Subclass Storage policies - no matter what their value.
Subclass Storage: Optical Drive Control	Read Only	UDF Only				Full Access	UDF Only	Full Access		<p>CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy.</p> <p>Full Access: Optical Drive port does not have read/write data restrictions applied</p> <p>UDF Only: Blocks all data writes that are not in the UDF format (CD/DVD burning, ISO burning). Read data is enabled.</p> <p>Read Only: Allows read capability. Write data is disabled</p> <p>Blocked: Port is blocked from read/write capability</p> <p>This policy is endpoint-based and cannot be overridden by user policy.</p> <p>Universal Disk Format (UDF) is an implementation of the specification known as ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system for computer data storage for a broad range of media.</p> <p>This policy has interactions with PCS. See Encryption External Media and PCS Interactions.</p>
Subclass Storage: Floppy	Blocked	Read Only				Full Access	Read Only	Full Access		CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy.

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Drive Control										<p>Full Access: Floppy Drive port does not have read/write data restrictions applied</p> <p>Read Only: Allows read capability. Write data is disabled</p> <p>Blocked: Port is blocked from read/write capability</p> <p>This policy is endpoint-based and cannot be overridden by user policy.</p>
Class: Windows Portable Device (WPD)	Enabled									<p>PARENT to the next policy. Set this policy to Enabled to use the Subclass Windows Portable Device (WPD): Storage policy. Setting this policy to Disabled disables the Subclass Windows Portable Device (WPD): Storage policy - no matter what its value.</p> <p>Control access to all Windows Portable Devices.</p>
Subclass Windows Portable Device (WPD): Storage	Enabled									<p>CHILD of Class: Windows Portable Device (WPD)</p> <p>Class: Windows Portable Device (WPD) must be set to Enabled to use this policy.</p> <p>Full Access: Port does not have read/write data restrictions applied.</p> <p>Read Only: Allows read capability. Write data is disabled.</p> <p>Blocked: Port is blocked from read/write capability.</p>
Class: Human Interface Device (HID)	Enabled									<p>Control access to all Human Interface Devices (keyboards, mice).</p> <p>Note: USB port-level blocking and HID class-level blocking is only honored if the computer chassis type can be identified as a laptop/notebook form-factor. The computer's BIOS is</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										relied on for the identification of the chassis.
Class: Other	Enabled									Control access to all devices not covered by other Classes.
Removable Storage Policies										
EMS Encrypt External Media	True					False		True	False	<p>This policy is the "master policy" for all Removable Storage policies. A False value means that no encryption of removable storage takes place, regardless of other policy values.</p> <p>A True value means that all Removable Storage encryption policies are enabled.</p> <p>This policy has interactions with PCS. See Encryption External Media and PCS Interactions.</p>
EMS Exclude CD/DVD Encryption	False								True	<p>False encrypts CD/DVD devices.</p> <p>This policy has interactions with PCS. See Encryption External Media and PCS Interactions.</p>
EMS Access to unShielded Media	Block		Read only			Full Access		Read only	Full Access	<p>Block, Read Only, Full Access</p> <p>This policy has interactions with PCS. See Encryption External Media and PCS Interactions.</p> <p>When this policy is set to Block Access, you have no access to removable storage unless it is encrypted.</p> <p>Choosing either Read-Only or Full Access allows you to decide what removable storage to encrypt.</p> <p>If you choose not to encrypt removable storage and this policy is set to Full Access, you have full read/write access to removable storage.</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										If you choose not to encrypt removable storage and this policy is set to Read-Only, you cannot read or delete existing files on the unencrypted removable storage, but the client does not allow any files to be edited on, or added to, the removable storage unless it is encrypted.
EMS Encryption Algorithm	AES256									AES-256, Rijndael 256, AES-128, Rijndael 128, 3DES
EMS Scan External Media	True	False								True allows removable media to be scanned every time it is inserted. When this policy is False and the EMS Encrypt External Media policy is True, only new and changed files are encrypted. A scan occurs at every insertion so that any files added to the removable media without authenticating can be caught. Files can be added to the media if authentication is declined, but encrypted data cannot be accessed. The files added are not encrypted in this case, so the next time the media is authenticated (to work with encrypted data), any files that may have been added are scanned and encrypted.
EMS Access Encrypted Data on unShielded Device	True									True allows the user to access encrypted data on removable storage whether the endpoint is encrypted or not.
EMS Device Whitelist										This policy allows the specification of removable media devices to exclude from Encryption External Media. Any external media devices not on this list are protected. Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										<p>of 2048 total characters allowed.</p> <p>To find the PNPDeviceID for removable storage:</p> <ol style="list-style-type: none"> 1 Insert the removable storage device into a Encrypted computer. 2 Open the EMSService.log in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3 Find "PNPDeviceID=" <p>For example: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR \DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0</p> <p>Specify the following in the EMS Device Whitelist policy:</p> <p>VEN=Vendor (Ex: USBSTOR \DISK&VEN_SEAGATE)</p> <p>PROD=Product/Model Name (Ex: &PROD_USB); also excludes from EMS Encryption all of Seagate's USB drives; a VEN value (Ex: USBSTOR \DISK&VEN_SEAGATE) must precede this value</p> <p>REV=Firmware Revision (Ex: &REV_0409); also excludes the specific model being used; VEN and PROD values must precede this value</p> <p>Serial number (Ex: \2HC015KJ&0); excludes only this device; VEN, PROD, and REV values must precede this value</p> <p>Allowed Delimiters: Tabs, Commas, Semi colons, Hex character 0x1E (Record separator character)</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
EMS Alpha Characters Required in Password	True									True requires one or more letters in the password.
EMS Mixed Case Required in Password	True	False								True requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters Required in Password	8				6			8		1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	True	False								True requires one or more numeric characters in the password.
EMS Password Attempts Allowed	2	3			4			3		1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	True	False							True	True requires one or more special characters in the password.
EMS Cooldown Time Delay	30									0-5000 seconds Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	30	20			10	30	10			0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Encryption Rules										Encryption rules to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. Space and Enter

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
										characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored.
										Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both Encryption External Media and encryption rules to encrypt the device. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. See How to Encrypt an iPod with Encryption External Media .
EMS Block Access to UnShieldable Media	True								False	<p>Block access to any removable media that is less than 55 MB and thus has insufficient storage capacity to host Encryption External Media (such as a 1.44MB floppy disk).</p> <p>All access is blocked if EMS and this policy are both True. If EMS Encrypt External Media is True, but this policy is False, data can be read from the unencryptable media, but write access to the media is blocked.</p> <p>If EMS Encrypt External Media is False, then this policy has no effect and access to unencryptable media is not impacted.</p>
User Experience Control Policies										
Force Reboot on Update	True								False	Setting the value to True causes the computer to immediately reboot to allow processing of encryption or updates related to device-based policy, such as System Data Encryption (SDE).

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
Length of Each Reboot Delay	5	10				20		15		The number of minutes to delay when the user chooses to delay reboot for device-based policy.
Number of Reboot Delays Allowed	1					5		3		The number of times the user is allowed to delay reboot for device-based policy.
Suppress File Contention Notification	False									This policy controls whether users see notification pop-ups if an application attempts to access a file while the client is processing it.
Display Local Encryption Processing Control	False		True					False		Setting the value to True allows the user to see a menu option in the notification area icon that allows them to pause/resume encryption/decryption (depending on what the Encryption client is currently doing).
										<p>NOTE: Allowing a user to pause encryption could allow the user to prevent the Encryption client from fully encrypting or decrypting data per policy.</p>
Allow Encryption Processing Only When Screen is Locked	False		User-Optional					False		<p>True, False, User-Optional</p> <p>When True, there is no encryption or decryption of data while the user is actively working. The client only processes data when the screen is locked.</p> <p>User-Optional adds an option to the notification area icon allowing the user to turn this feature on or off.</p> <p>When False, encryption processing occurs any time, even while the user is working.</p> <p>Enabling this option significantly extends the amount of time it takes to</p>

Policy	Aggressive Protection for All Fixed Drives and External Drives	PCI Regulation	Data Breach Regulation	HIPAA Regulation	Basic Protection for All Fixed Drives and External Drives (Default)	Basic Protection for All Fixed Drives	Basic Protection for System Drive Only	Basic Protection for External Drives	Encryption Disabled	Description
--------	--	----------------	------------------------	------------------	---	---------------------------------------	--	--------------------------------------	---------------------	-------------

complete encryption or decryption.

Template Descriptions

Aggressive Protection for All Fixed Drives and External Drives

This policy template is designed for organizations with a primary goal of enforcing strong security and risk avoidance across the entire enterprise. It is best used when security is significantly more important than usability and the need for less secure policy exceptions for specific users, groups or devices is minimal.

This policy template:

- is a highly restricted configuration, providing greater protection.
- provides protection of the System Drive and all Fixed Drives.
- encrypts all data on removable media devices, and prevents the use of non-encrypted removable media devices.
- provides read-only optical drive control.

PCI Regulation Targeted

Payment Card Industry Data Security Standard (PCI DSS) is a multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to set the guidelines for organizations to proactively protect customer account data.

This policy template:

- provides protection of the System Drive and all Fixed Drives.
- prompts users to encrypt removable media devices.
- provides the ability to write only UDF CD/DVDs. Port control configuration allows read access to all optical drives.

Data Breach Regulation Targeted

The Sarbanes-Oxley Act requires adequate controls for financial information. Because much of this information resides in electronic format, encryption is a key control point when this data is stored or transferred. The Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act) guidelines do not require encryption. However, the Federal Financial Institutions Examination Council (FFIEC) recommends that, "Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit." California Senate Bill 1386 (California's Database Security Breach Notification Act) aims to protect California residents from identity theft by requiring organizations that have had computer security breaches to notify all affected individuals. The only way an organization can avoid notifying customers is to be able to prove all personal information was encrypted prior to a security breach.

This policy template:

- provides protection of the System Drive and all Fixed Drives.

- prompts users to encrypt removable media devices.
- provides the ability to write only UDF CD/DVDs. Port control configuration allows read access to all optical drives.

HIPAA Regulation Targeted

The Health Insurance Portability and Accountability Act (HIPAA) mandates that healthcare organizations implement a number of technical safeguards to protect the confidentiality and integrity of all individually identifiable health information.

This policy template:

- provides protection of the System Drive and all Fixed Drives.
- prompts users to encrypt removable media devices.
- provides the ability to write only UDF CD/DVDs. Port control configuration allows read access to all optical drives.

Basic Protection for All Fixed Drives and External Drives (Default)

This policy template provides the recommended configuration, which provides a high level of protection without significantly impacting system usability.

This policy template:

- provides protection of the System Drive and all Fixed Drives.
- prompts users to encrypt removable media devices.
- provides the ability to write only UDF CD/DVDs. Port control configuration allows read access to all optical drives.

Basic Protection for All Fixed Drives

This policy template:

- provides protection of the System Drive and all Fixed Drives.
- provides the ability to write CD/DVDs in any supported format. Port control configuration allows read access to all optical drives.

This policy template does not:

- provide encryption for removable media devices.

Basic Protection for System Drive Only

This policy template:

- provides protection of the System Drive, typically the C: drive, where the operating system is loaded.
- provides the ability to write CD/DVDs in any supported format. Port control configuration allows read access to all optical drives.

This policy template does not:

- provide encryption for removable media devices.

Basic Protection for External Drives

This policy template:

- provides protection of removable media devices.
- provides the ability to write only UDF CD/DVDs. Port control configuration allows read access to all optical drives.

This policy template does not:

- provide protection for the System Drive (typically the C: drive, where the operating system is loaded) or other Fixed Drives.

Encryption Disabled

This policy template does not provide encryption protection. Take additional measures to safeguard devices from loss and theft when using this template.

This template is useful for organizations that prefer to start with no active encryption to transition into security. As the organization becomes comfortable with their deployment, encryption can be enabled slowly by adjusting individual policies or by applying stronger templates for portions of or for the entire organization.

Extract Child Installers

- To install each client individually, extract the child executable files from the installer.
- If the master installer has been used to install, the clients must be uninstalled individually. Use this process to extract the clients from the master installer so that they can be used for uninstallation.

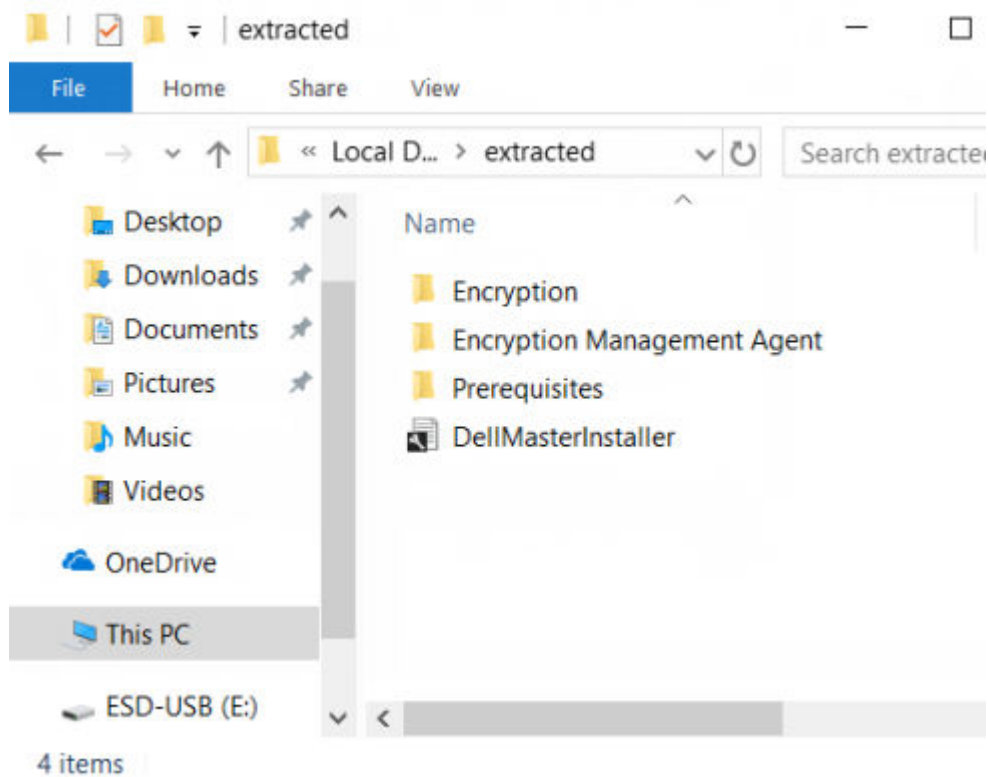
- 1 From the Dell installation media, copy the `DDSSetup.exe` file to the local computer.
- 2 Open a command prompt in the same location as the `DDSSetup.exe` file and enter:

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

The extraction path cannot exceed 63 characters.

Before you begin installation, ensure that all prerequisites have been met and all required software has been installed for each child installer that you plan to install. Refer to [Requirements](#) for details.

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



Proceed to [Troubleshooting](#).

Troubleshooting

Upgrading to the Windows 10 April 2018 Update

Computers installed with Encryption must use a specially configured Windows 10 Upgrade package to upgrade to the Windows 10 April 2018 Update. The configured version of the upgrade package ensures that Dell Encryption can manage access to your encrypted files to protect them from harm during the upgrade process.

To upgrade to the Windows 10 April 2018 Update, follow the instructions in the following article:

<http://www.dell.com/support/article/us/en/19/SLN298382>

Encryption Client Troubleshooting

Upgrade to the Windows 10 Creators Update

To upgrade to the Windows 10 April 2018 Update version, follow the instructions in the following article: <http://www.dell.com/support/article/us/en/19/SLN298382>.

(Optional) Create an Encryption Removal Agent Log File

- Before beginning the uninstall process, you can optionally create an Encryption Removal Agent log file. This log file is useful for troubleshooting an uninstall/decryption operation. If you do not intend to decrypt files during the uninstall process, you do not need to create this log file.
- The Encryption Removal Agent log file is not created until after the Encryption Removal Agent service runs, which does not happen until the computer is restarted. Once the client is successfully uninstalled and the computer is fully decrypted, the log file is permanently deleted.
- The log file path is **C:\ProgramData\Dell\Dell Data Protection\Encryption**.
- Create the following registry entry on the computer targeted for decryption.

```
[HKLM\Software\Credant\DecryptionAgent]
```

```
"LogVerbosity"=DWORD:2
```

0: no logging

1: logs errors that prevent the service from running

2: logs errors that prevent complete data decryption (recommended level)

3: logs information about all decrypting volumes and files

5: logs debugging information

Find TSS Version

- TSS is a component that interfaces with the TPM. To find the TSS version, go to (default location) `C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe`. Right-click the file and select **Properties**. Verify the file version on the **Details** tab.

Encryption External Media and PCS Interactions

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

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

To Encrypt Data Written to CD/DVD

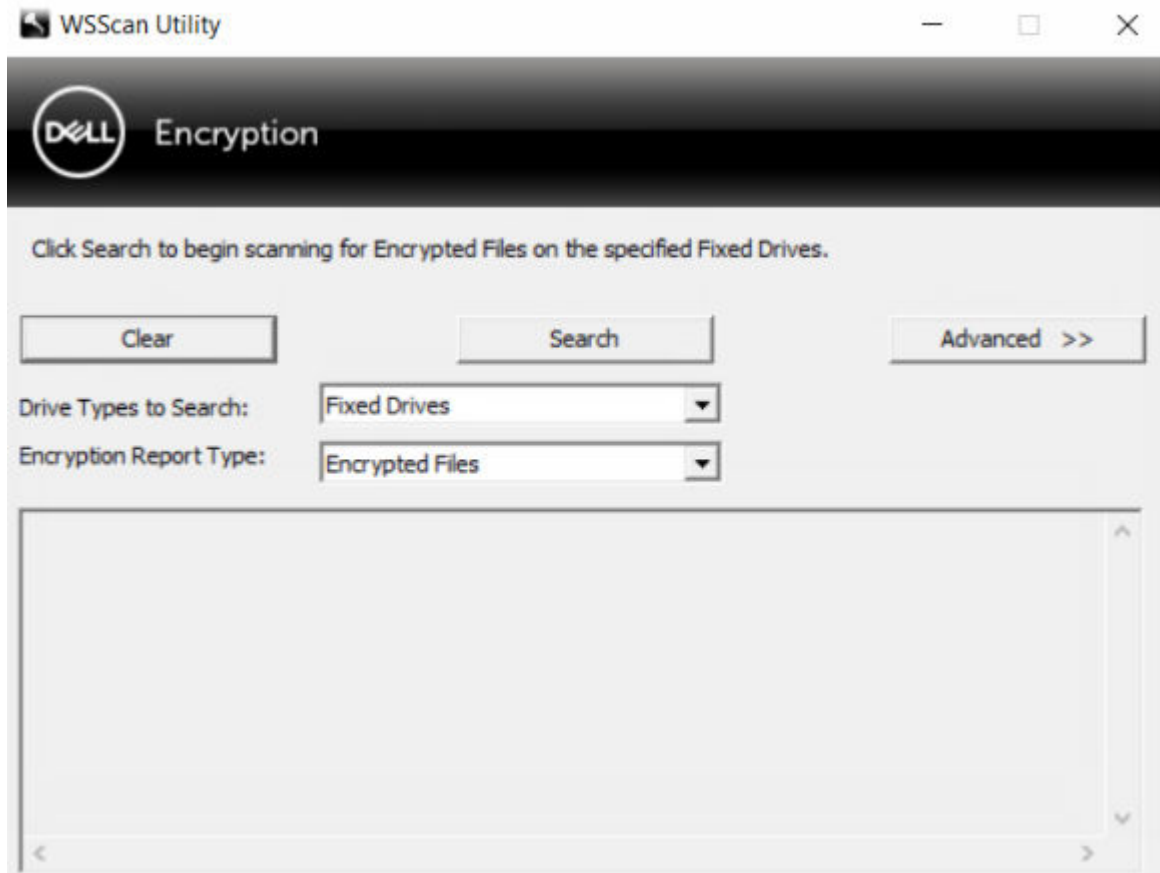
- Set Windows Media Encryption = On.
- Set EMS Exclude CD/DVD Encryption = not selected.
- Set Subclass Storage: Optical Drive Control = UDF Only.

Use WSScan

- WSScan allows you to ensure that all data is decrypted when uninstalling 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

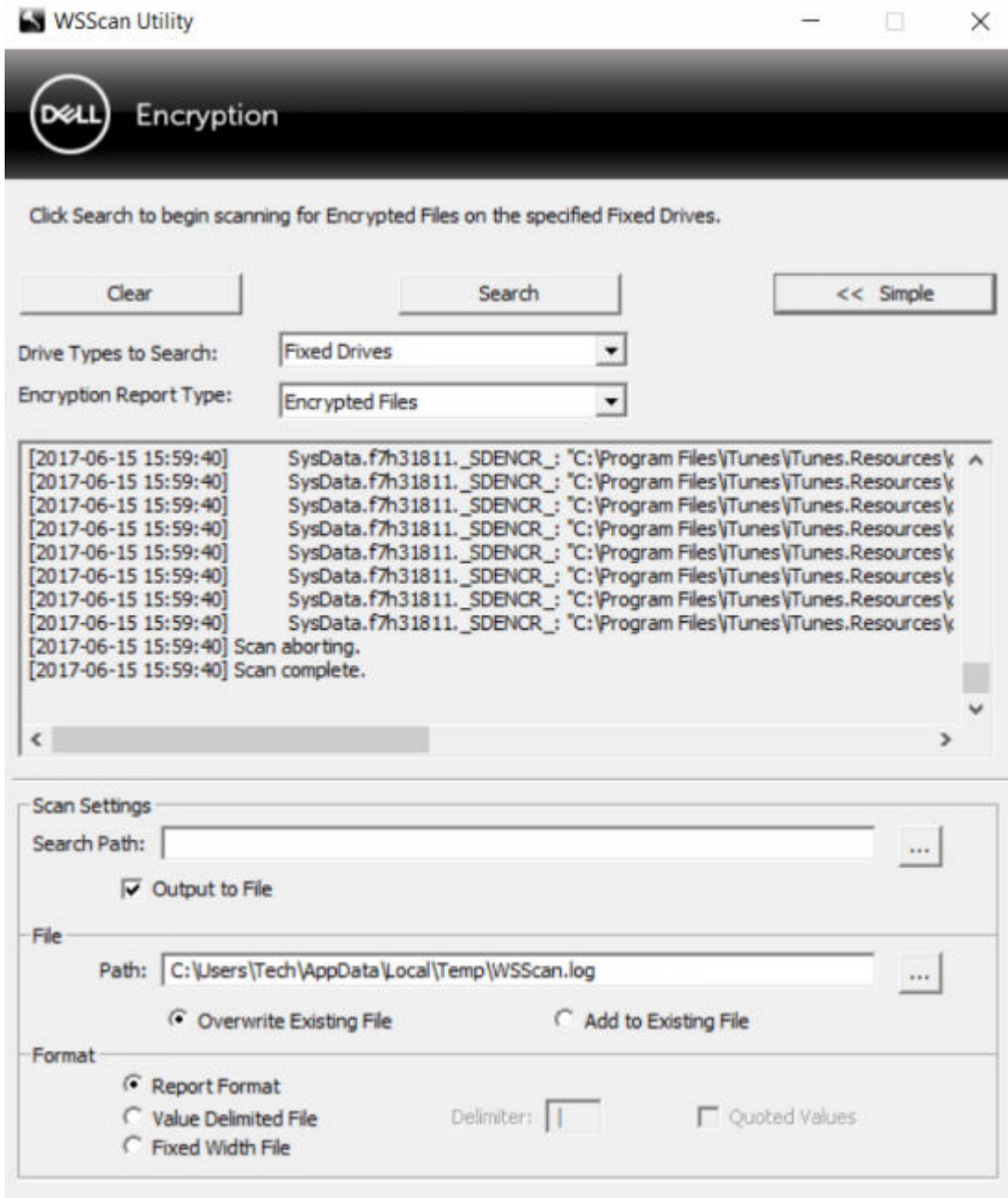
- 1 From the Dell installation media, copy `WSScan.exe` to the Windows computer to scan.
- 2 Launch a command line at the location above and enter **wsscan.exe** at the command prompt. WSScan launches.
- 3 Click **Advanced**.
- 4 Select the type of drive to scan: *All Drives*, *Fixed Drives*, *Removable Drives*, or *CDROMs/ DVDROMs*.
- 5 Select the Encryption Report Type: *Encrypted Files*, *Unencrypted Files*, *All Files*, or *Unencrypted Files in Violation*:
 - *Encrypted Files* - To ensure that all data is decrypted when uninstalling 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**.



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 menu 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 file name in *Path*, if desired.
- 5 Select **Add to Existing File** if you do not want to overwrite any existing WSScan output files.
- 6 Choose the output format:
 - Select Report Format for a report style list of scanned output. This is the default format.
 - Select Value Delimited File for output that can be imported into a spreadsheet application. The default delimiter is "|", although it can be changed to up to 9 alphanumeric, space, or keyboard punctuation characters.
 - Select the Quoted Values option to enclose each value in double quotation marks.
 - Select Fixed Width File for non-delimited output containing a continuous line of fixed-length information about each encrypted file.
- 7 Click **Search**.

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



WSScan Output

WSScan information about encrypted files contains the following information.

Example Output:

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

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

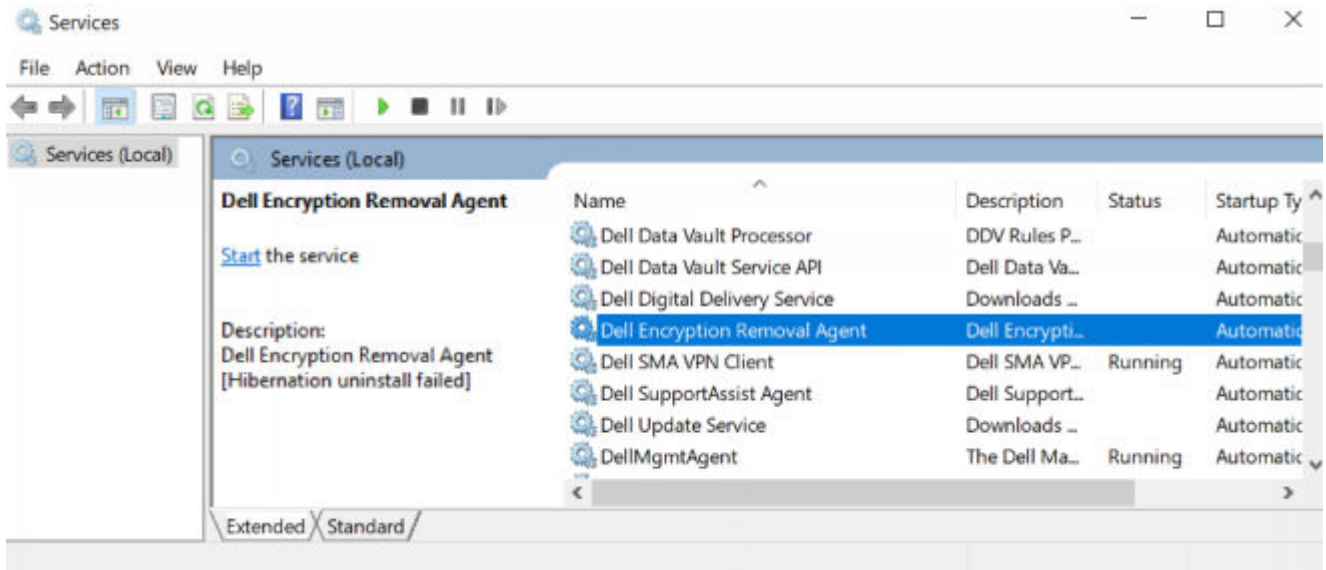
Output	Meaning
	<p>User: User encryption key.</p> <p>Common: Common encryption key.</p> <p>WSScan does not report files encrypted using Encrypt for Sharing.</p>
KCID	<p>The Key Computer ID.</p> <p>As shown in the example above, "7vdlxrsb"</p> <p>If you are scanning a mapped network drive, the scanning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

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.



How to Encrypt an iPod with Encryption External Media

These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules.

- We do not recommend the use of the iPod Shuffle, as unexpected results may occur.
- As iPods change, this information could also change, so caution is advised when allowing the use of iPods on Encryption External Media-enabled computers.
- Because folder names on iPods are dependent on the model of the iPod, we recommend creating an exclusion policy which covers all folder names, across all iPod models.
- To ensure encrypting an iPod via Encryption External Media does not make the device unusable, enter the following rules in the Encryption External Media Encryption Rules policy:

-R#:\Calendars

-R#:\Contacts

-R#:\iPod_Control

-R#:\Notes

-R#:\Photos

- You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories *excluded* from encryption via the previous rules:

^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos:

^R#:\;ppt.doc.xls.pptx.docx.xlsx

- Rules have been tested against these iPods:

iPod Video 30gb fifth generation

iPod Nano 2gb second generation

iPod Mini 4gb second generation

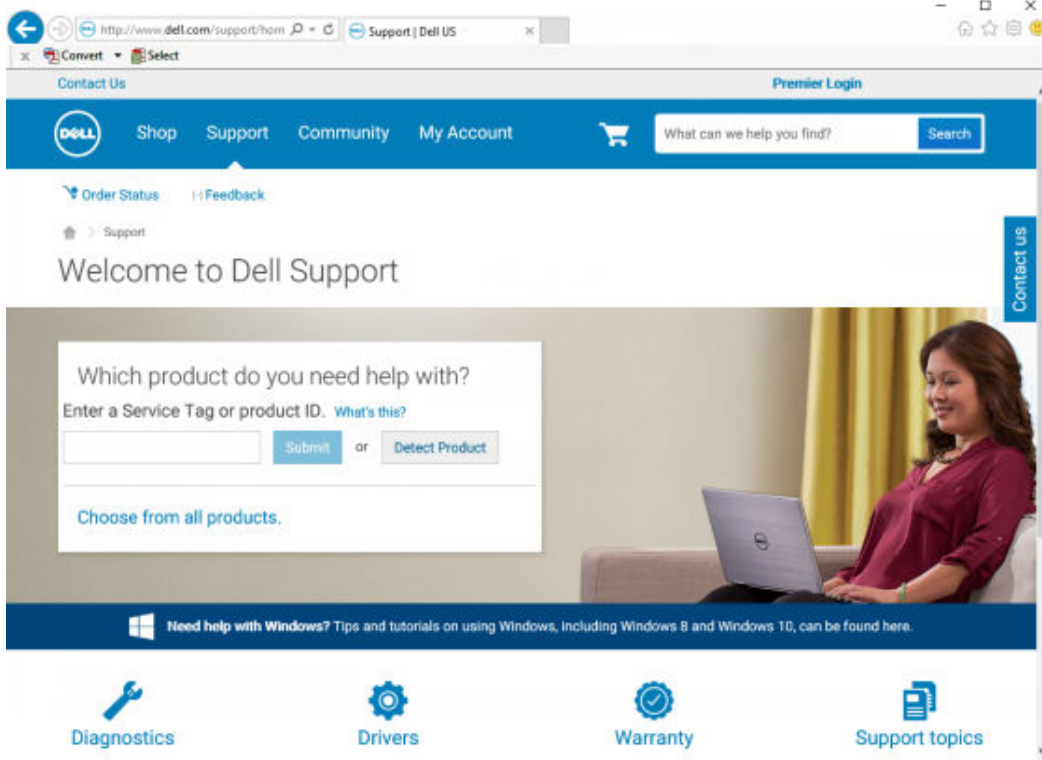
Dell ControlVault Drivers

Update Dell ControlVault Drivers and Firmware

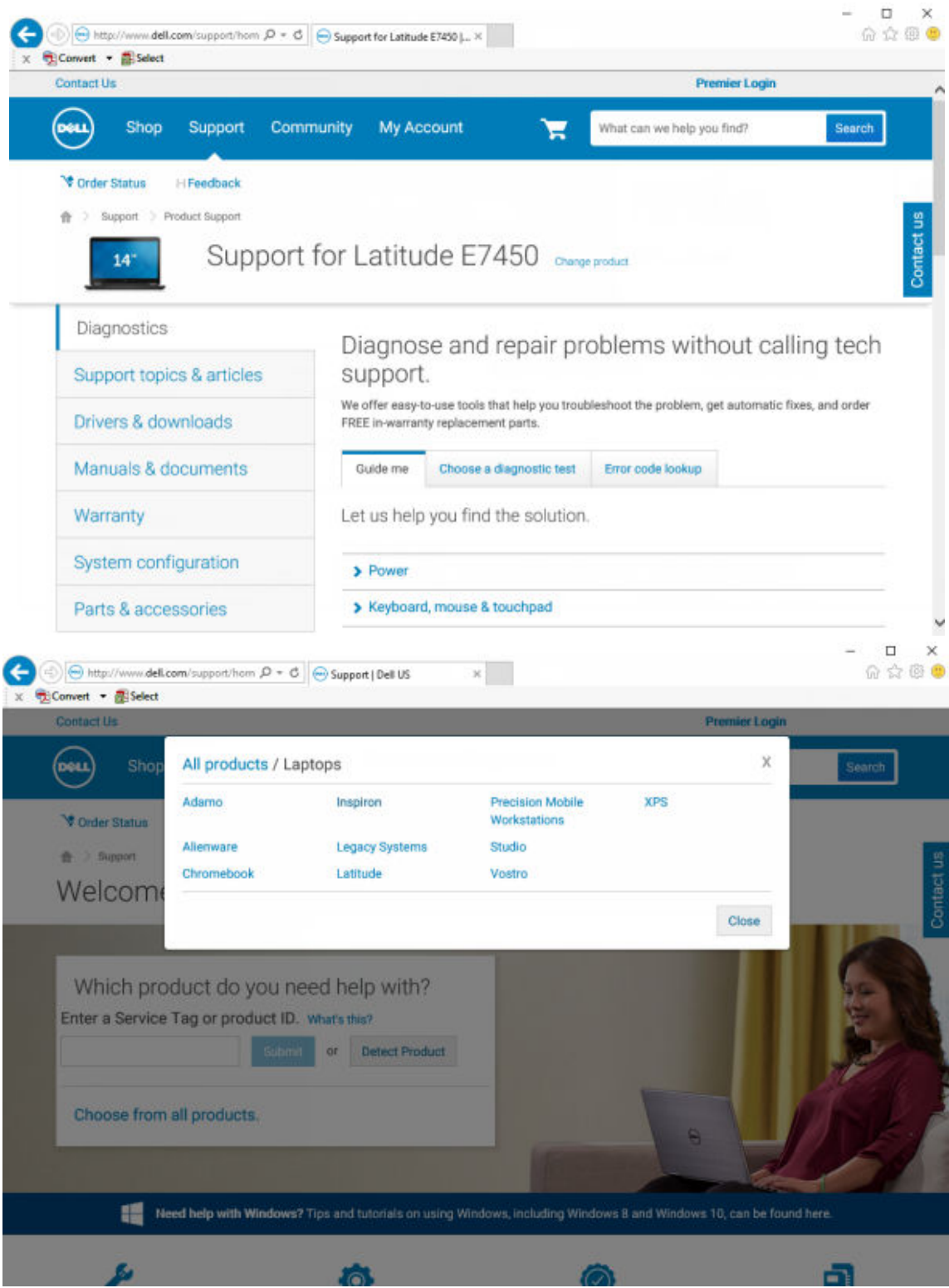
- Dell ControlVault drivers and firmware that are installed on Dell computers at the factory are outdated and should be updated by following this procedure, in this order.
- If an error message is received during client installation prompting you to exit the installer to update Dell ControlVault drivers,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

Download Latest Drivers

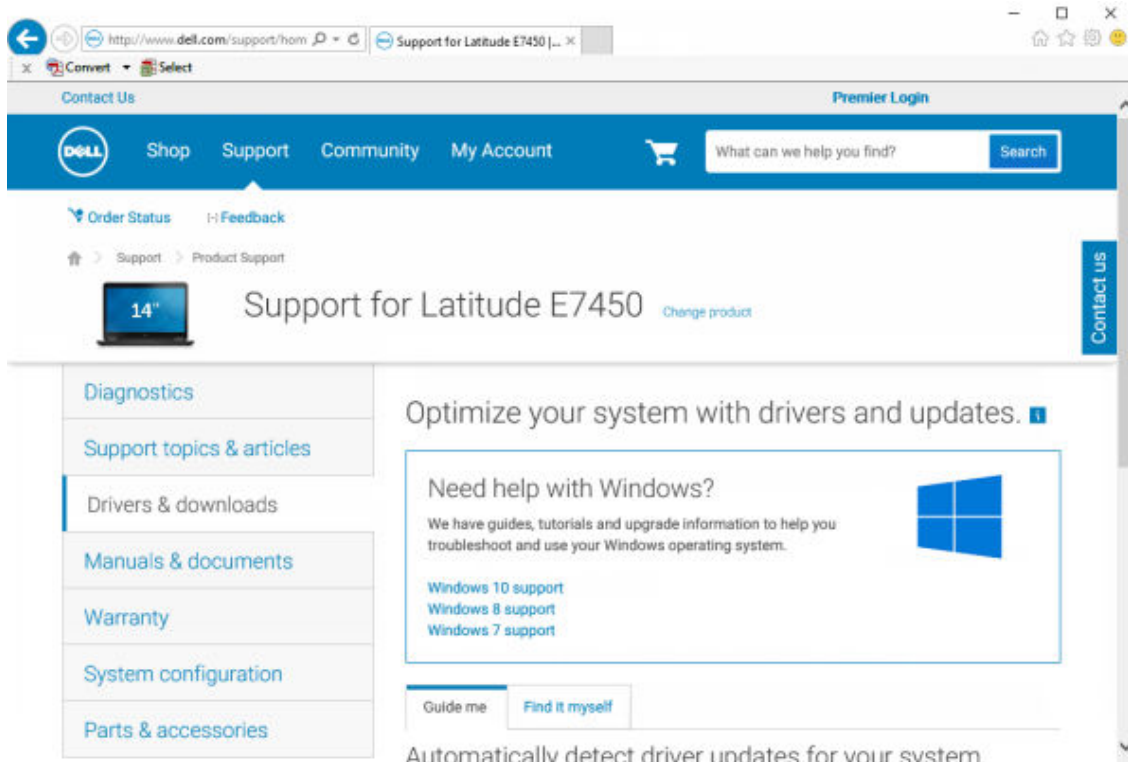
- 1 Go to support.dell.com.



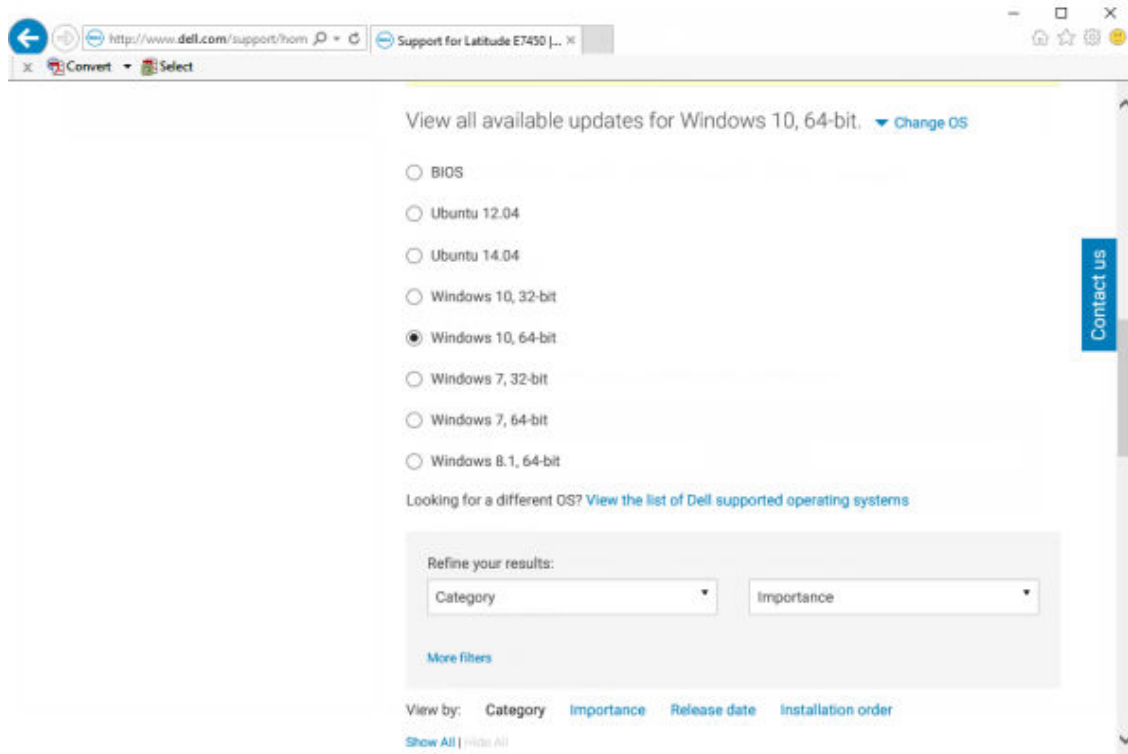
- 2 Select your computer model.



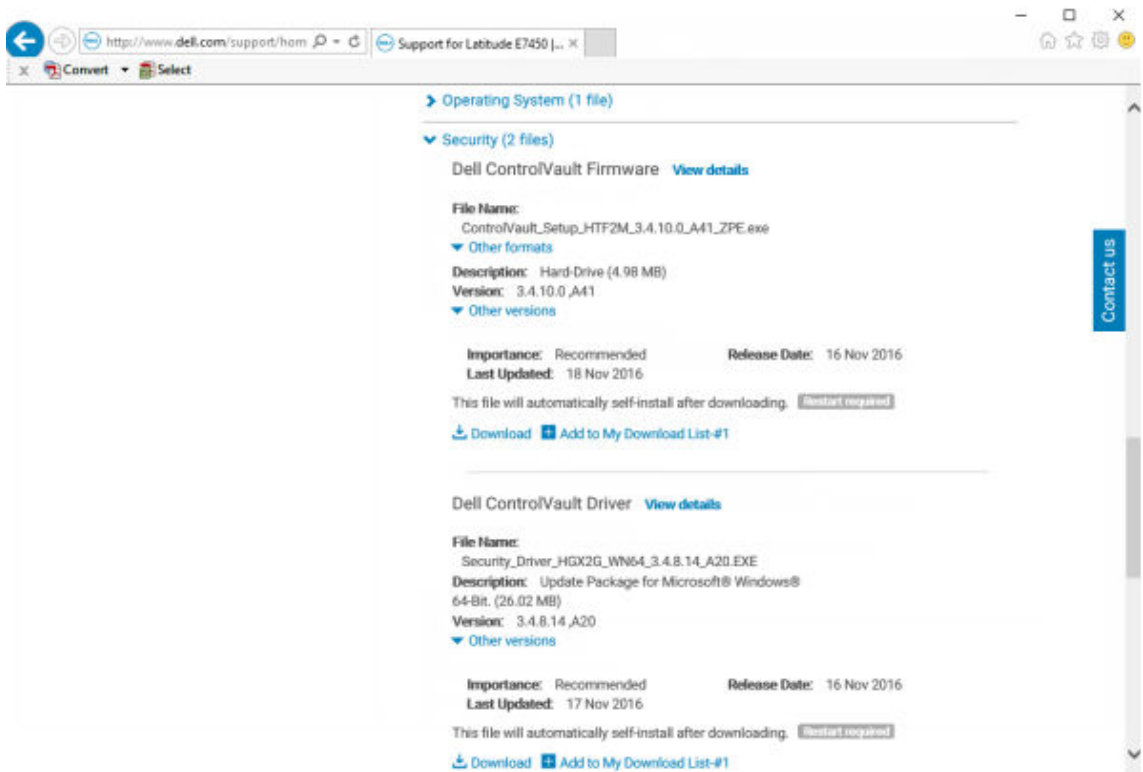
3 Select **Drivers & Downloads**.



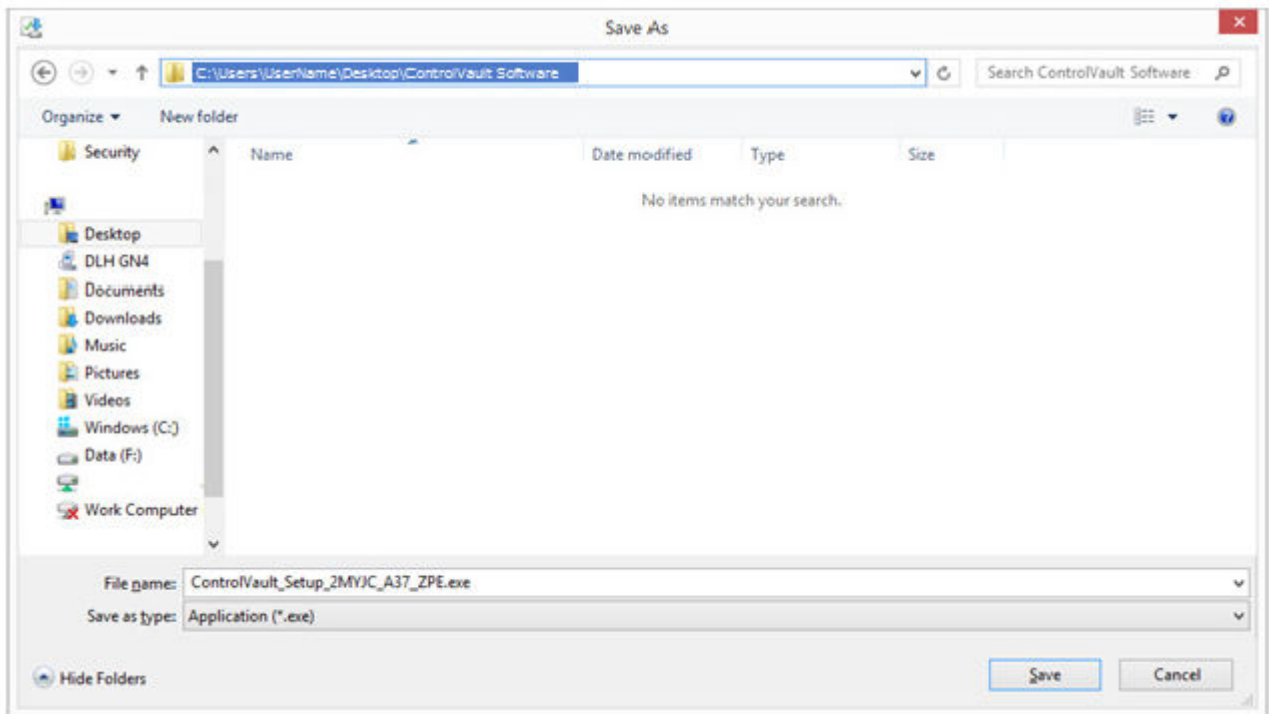
4 Select the **Operating System** of the target computer.



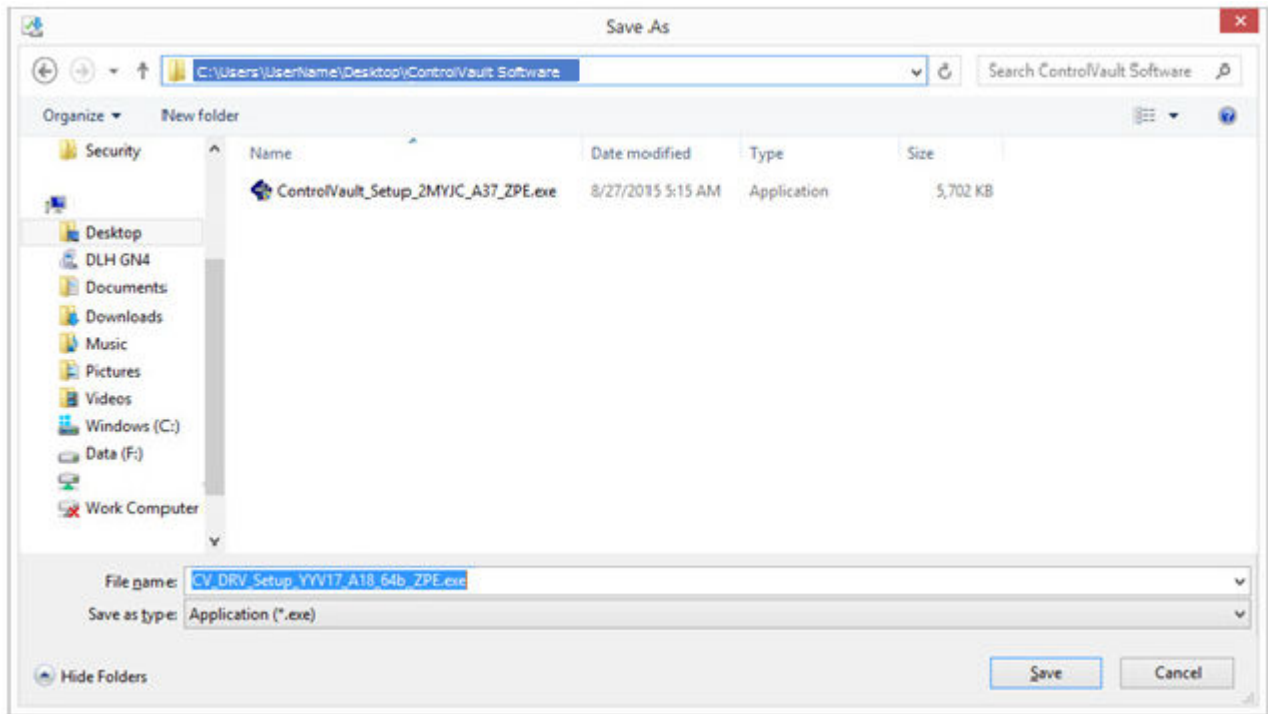
5 Expand the **Security** category.



6 Download and save the Dell ControlVault Drivers.



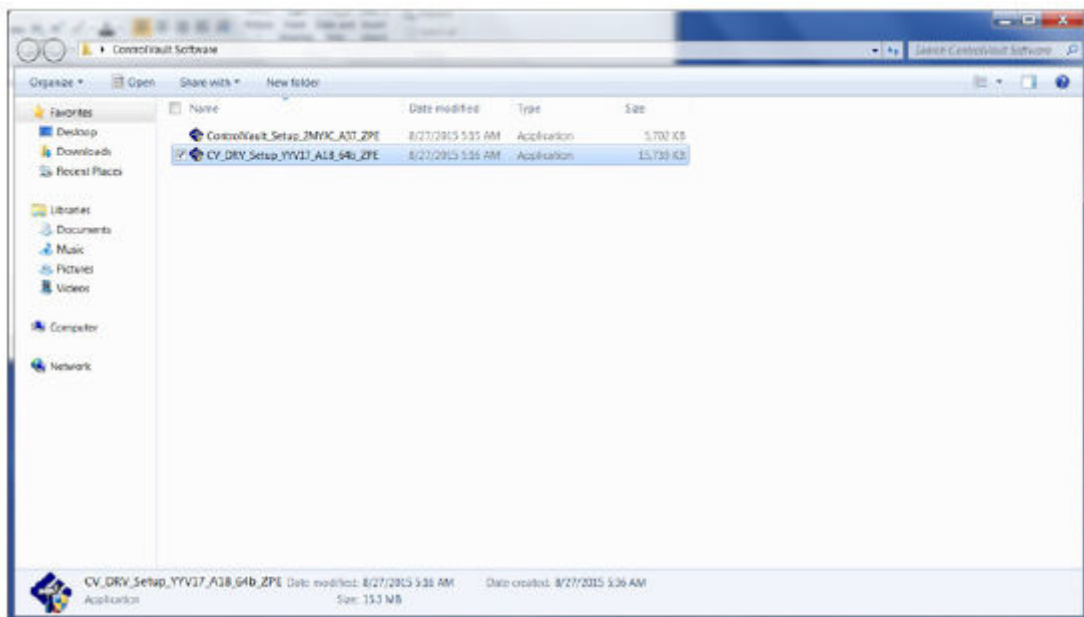
7 Download and save the Dell ControlVault Firmware.



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

Install Dell ControlVault Driver

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



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

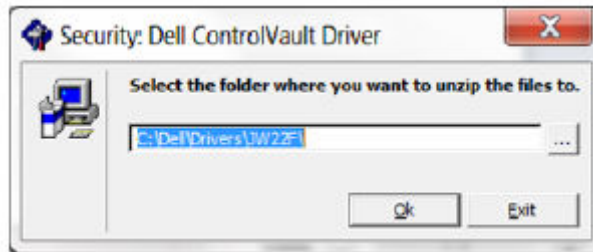
TIP:

Be sure to install the driver first. The file name of the driver *at the time of this document creation* is ControlVault_Setup_2MYJC_A37_ZPE.exe.

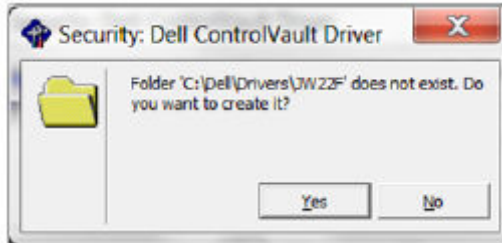
- 3 Click **Continue** to begin.



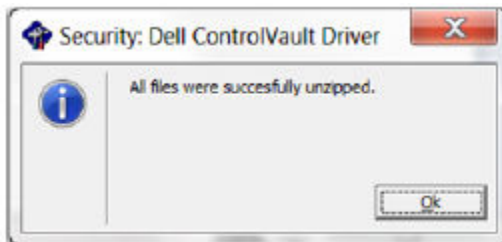
- 4 Click **Ok** to unzip the driver files in the default location of C:\Dell\Drivers**<New Folder>**.



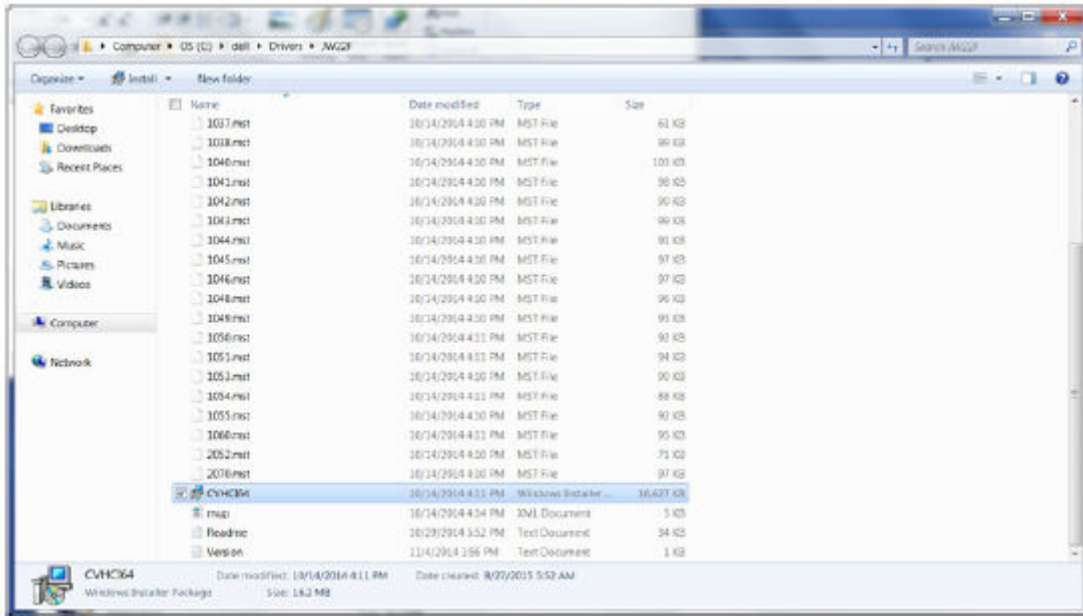
- 5 Click **Yes** to allow the creation of a new folder.



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



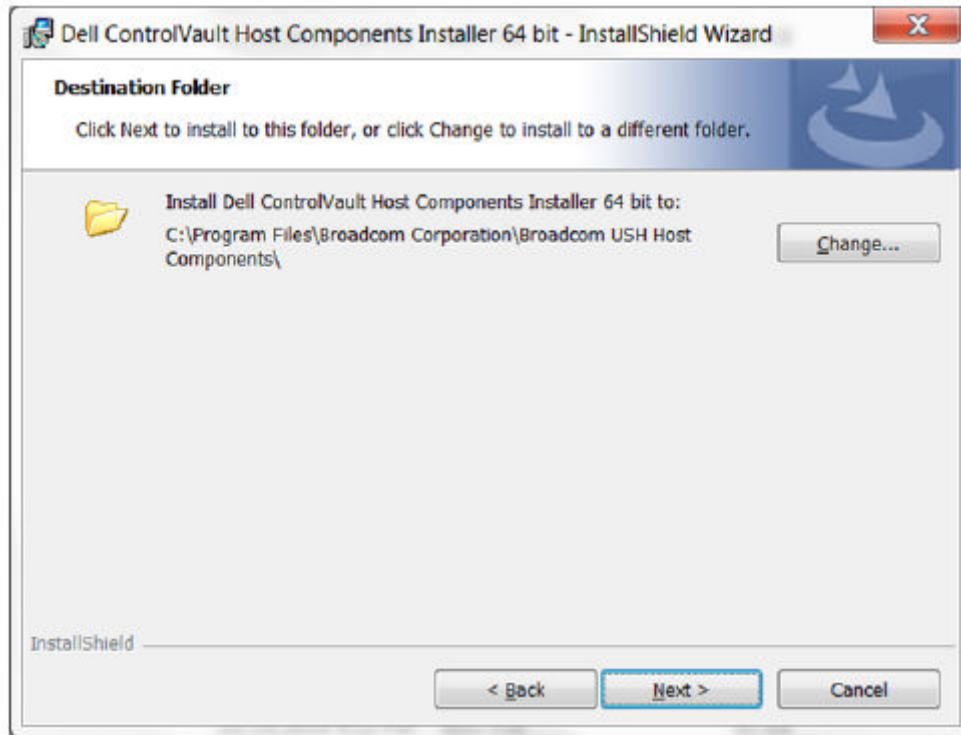
- 7 The folder which contains the files should display after extraction. If not, navigate to the folder to which you extracted the files. In this case, the folder is **JW22F**.



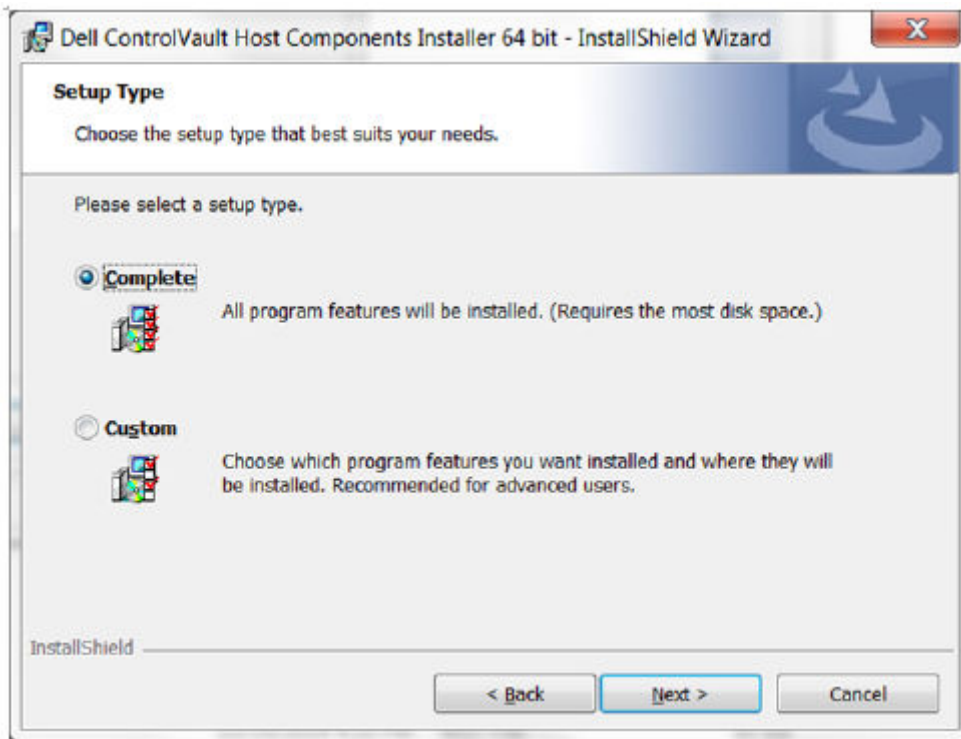
- 8 Double-click **CVHCI64.MSI** to launch the driver installer. [this example is **CVHCI64.MSI** in this example (CVHCI for a 32-bit computer)].
- 9 Click **Next** at the Welcome screen.



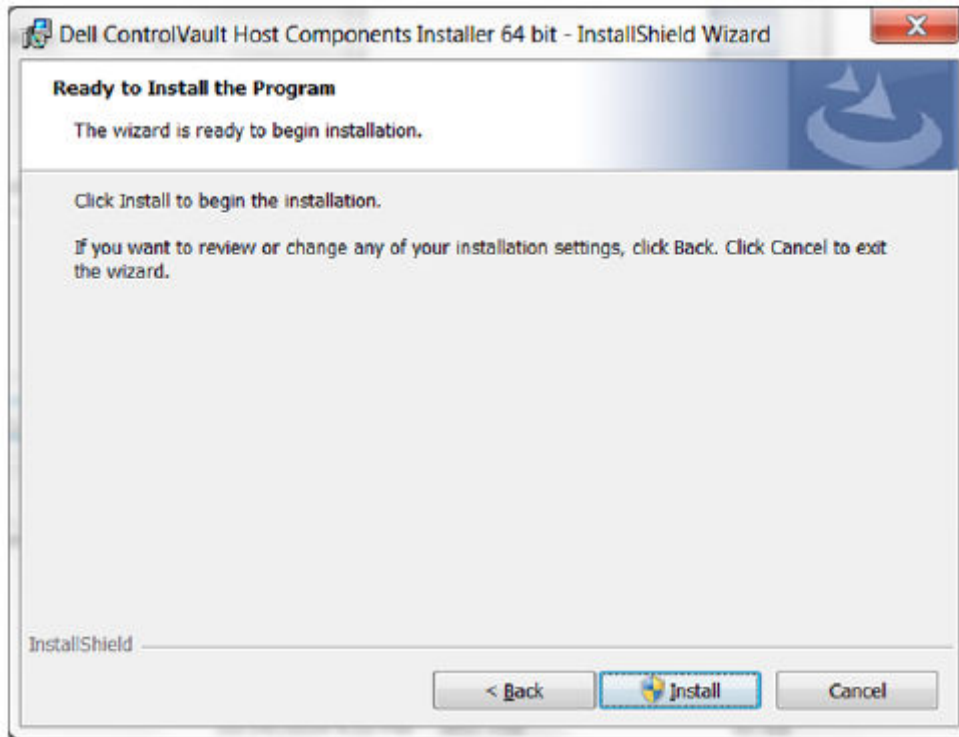
- 10 Click **Next** to install the drivers in the default location of C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.



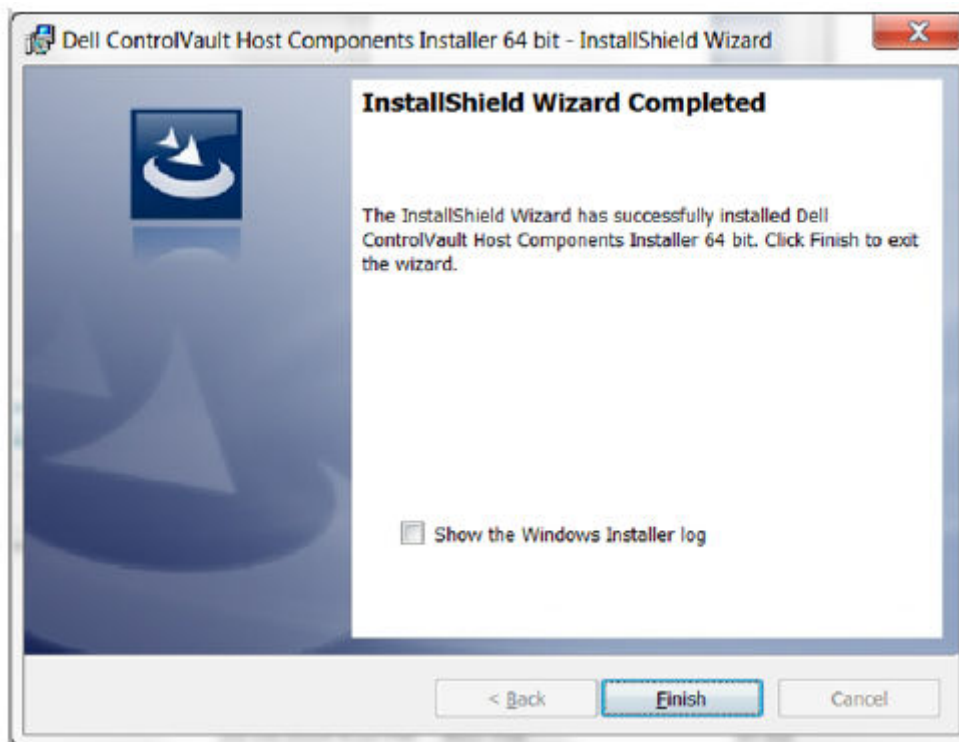
11 Select the **Complete** option and click **Next**.



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



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

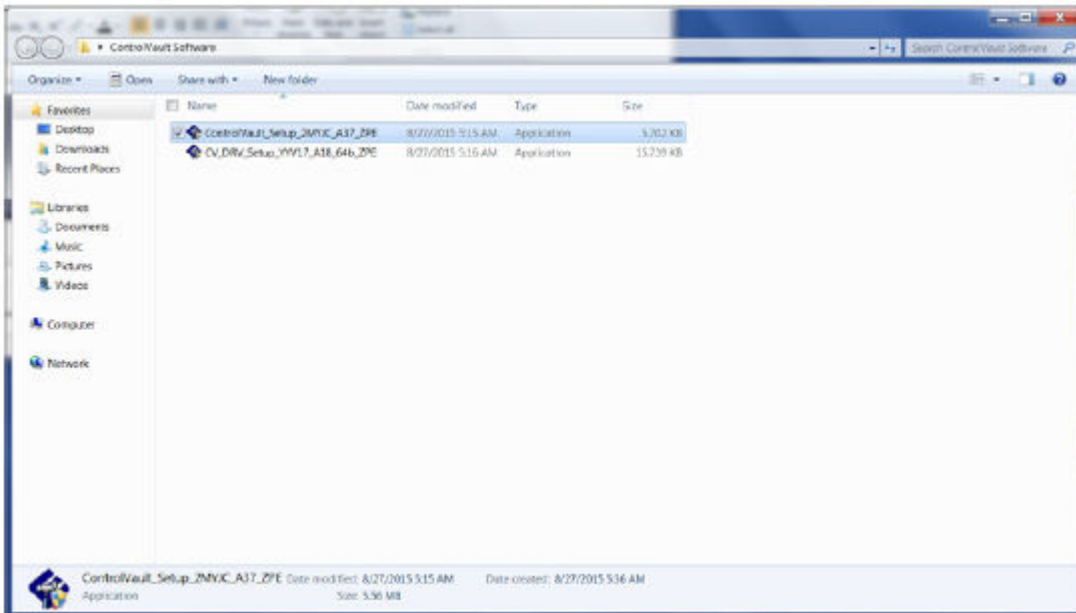


Verify Driver Installation

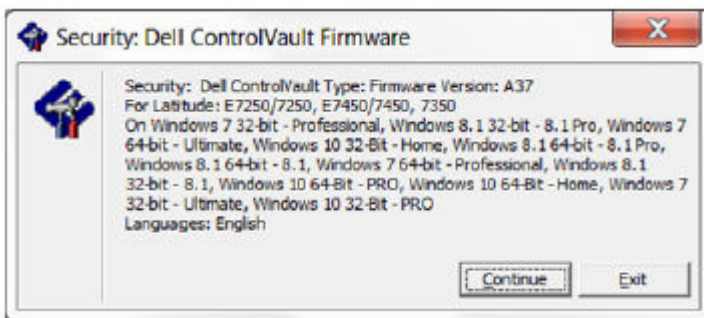
- The Device Manager will have a Dell ControlVault device (and other devices) depending on the operating system and hardware configuration.

Install Dell ControlVault Firmware

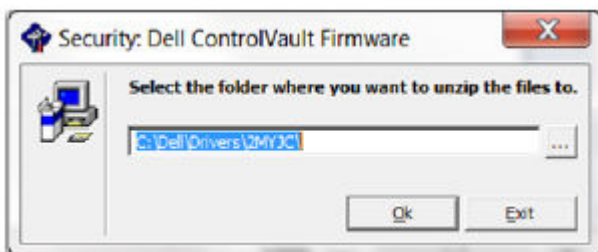
- 1 Navigate to the folder which you downloaded the firmware installation file.



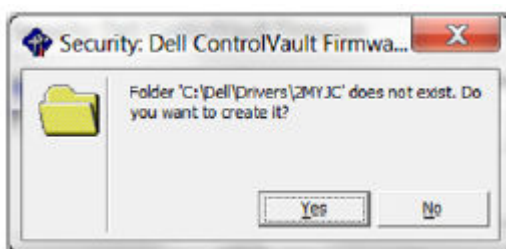
- 2 Double-click the Dell ControlVault firmware to launch the self-extracting executable file.
- 3 Click **Continue** to begin.



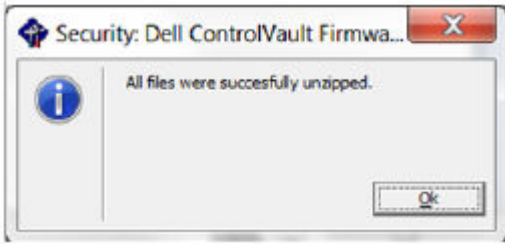
- 4 Click **Ok** to unzip the driver files in the default location of C:\Dell\Drivers\



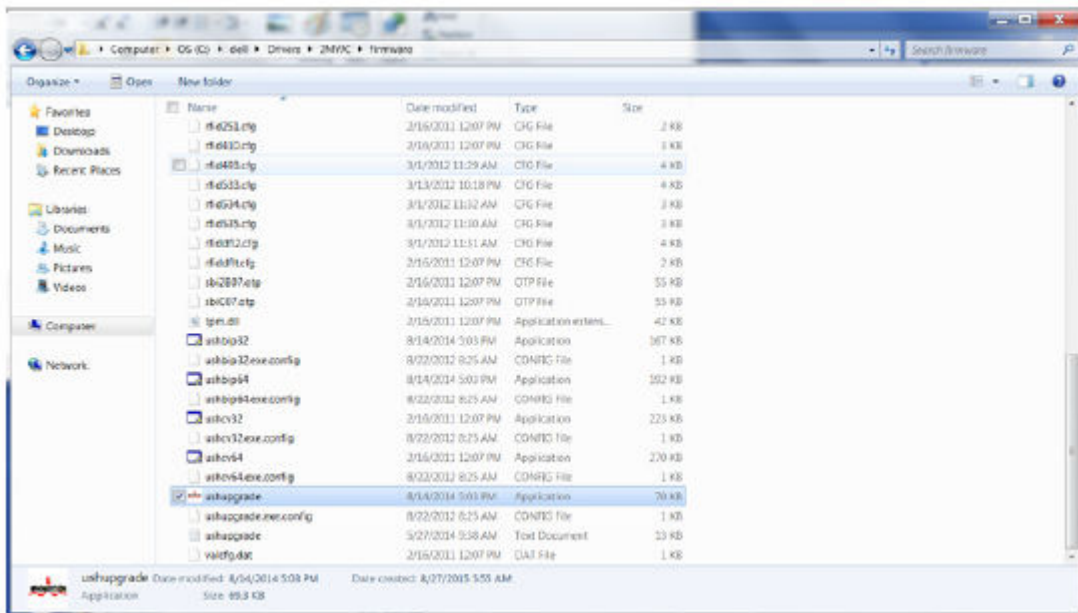
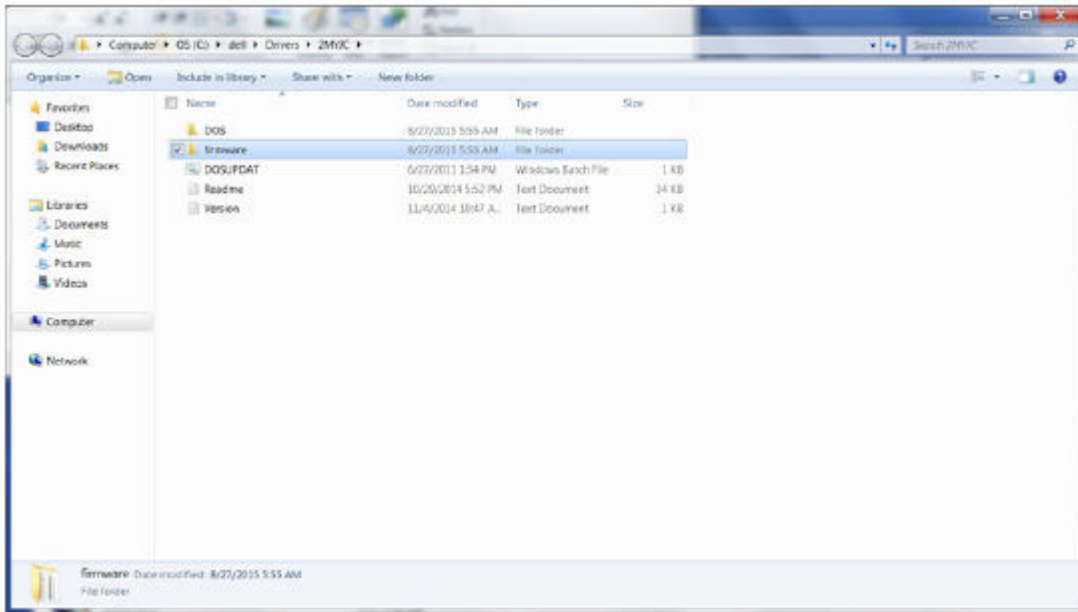
- 5 Click **Yes** to allow the creation of a new folder.



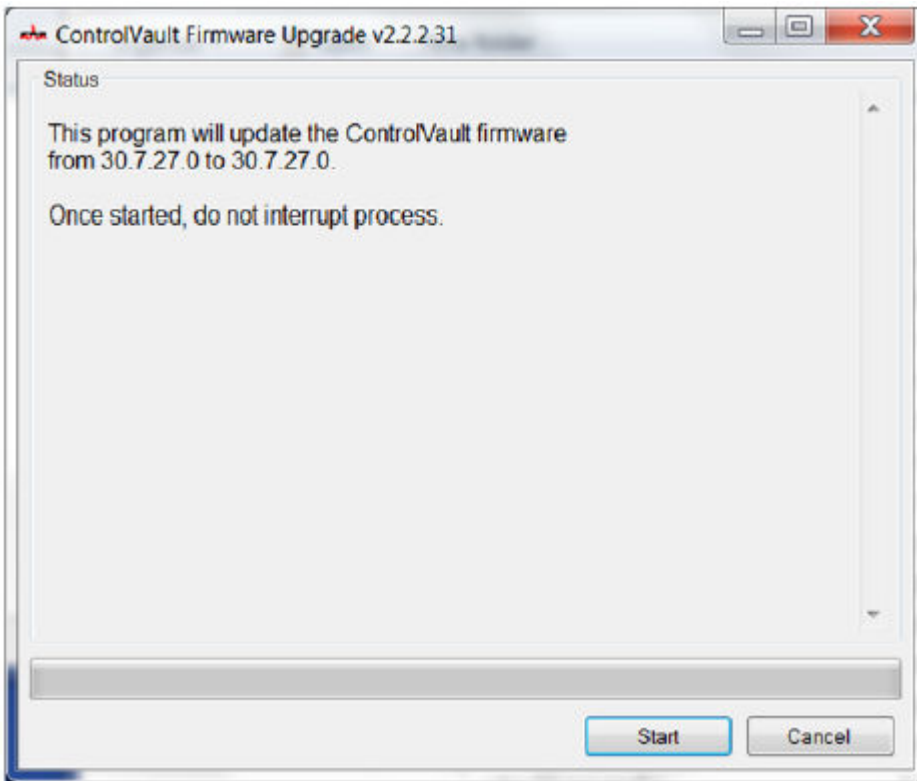
- 6 Click **Ok** when the successfully unzipped message displays.



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



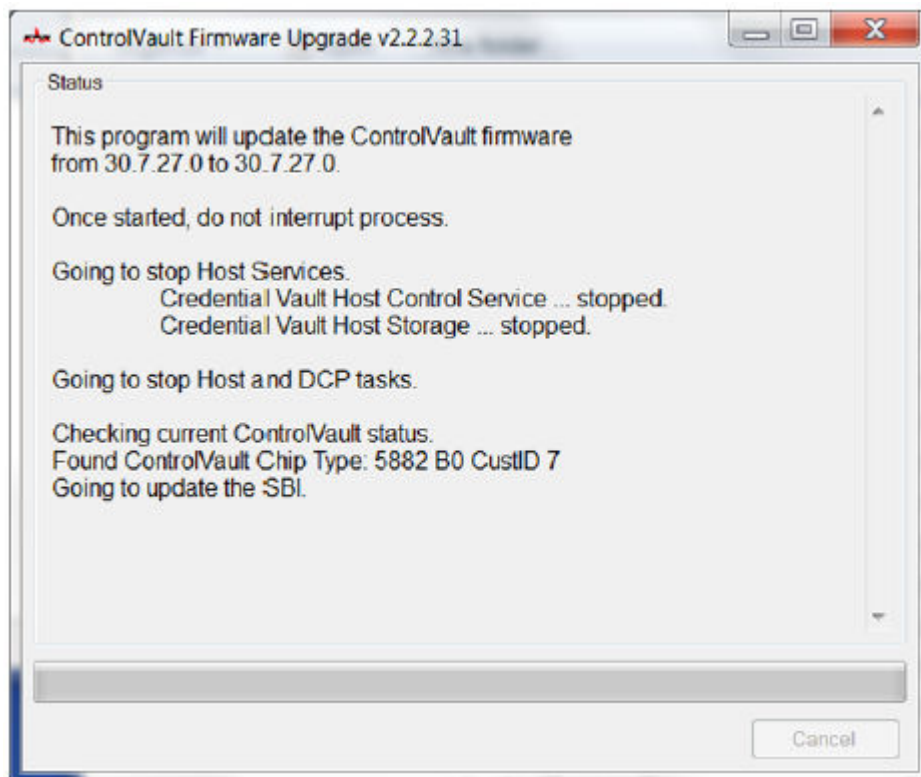
- 8 Double-click **ushupgrade.exe** to launch the firmware installer.
- 9 Click **Start** to begin the firmware upgrade.

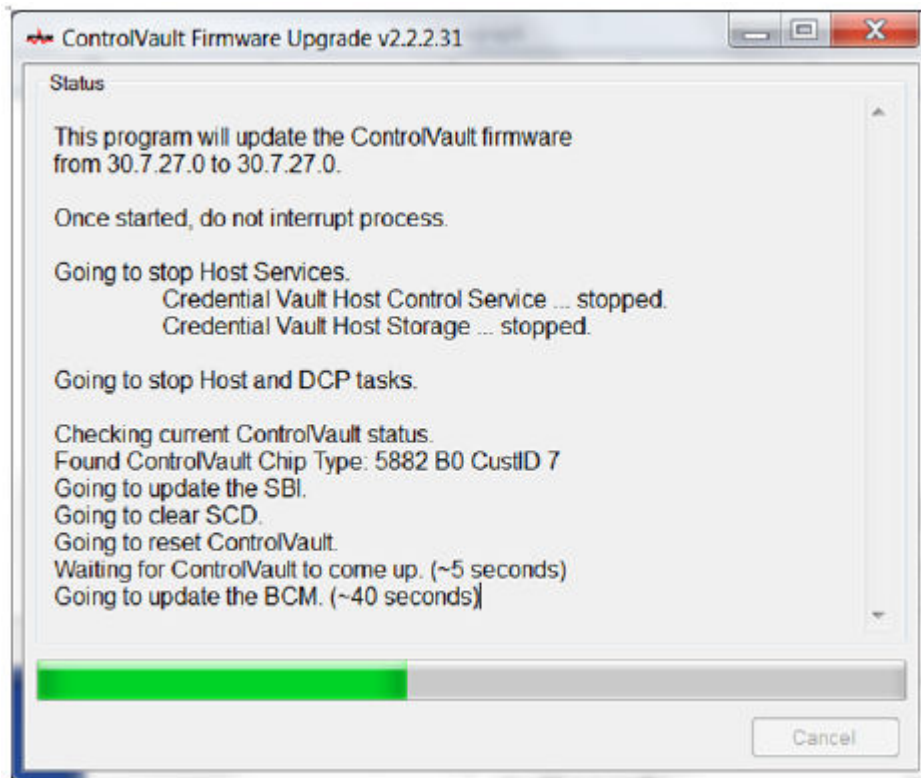
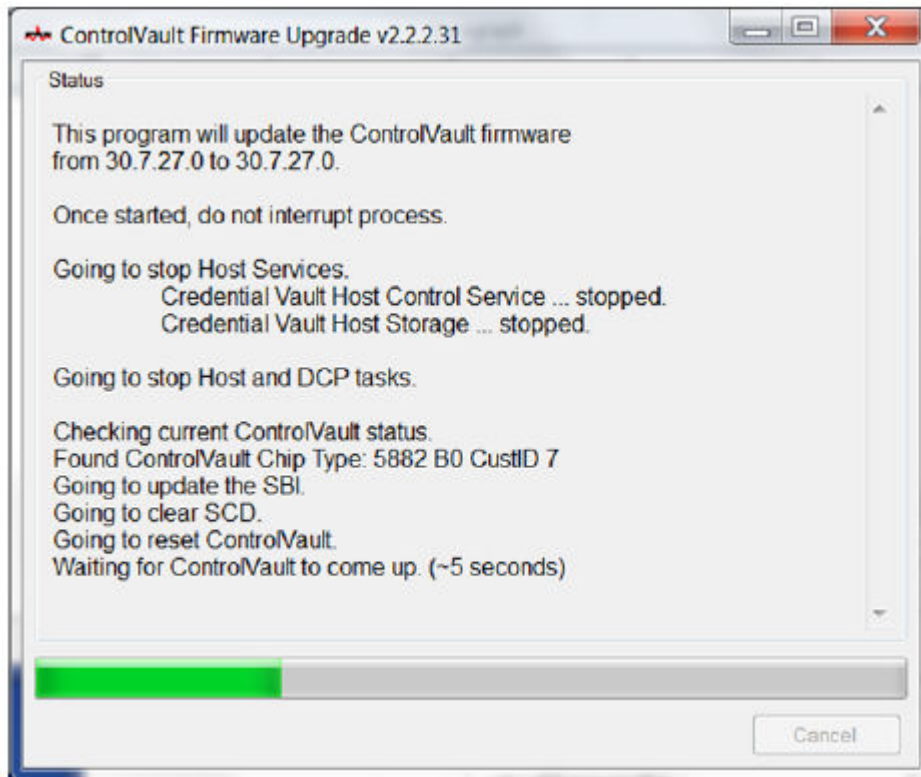


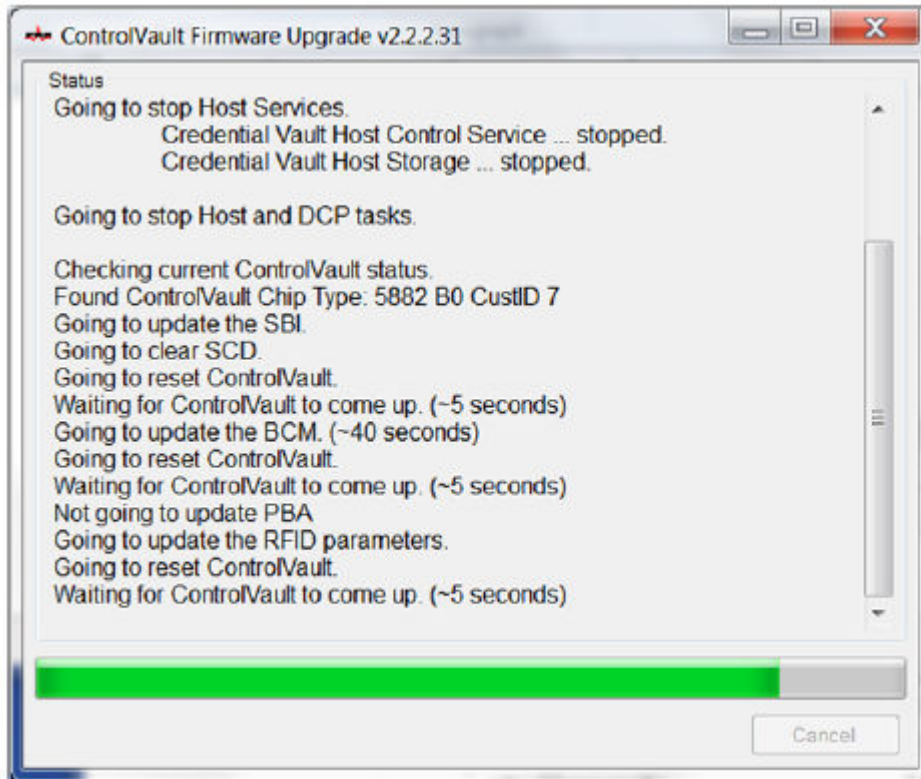
IMPORTANT:

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

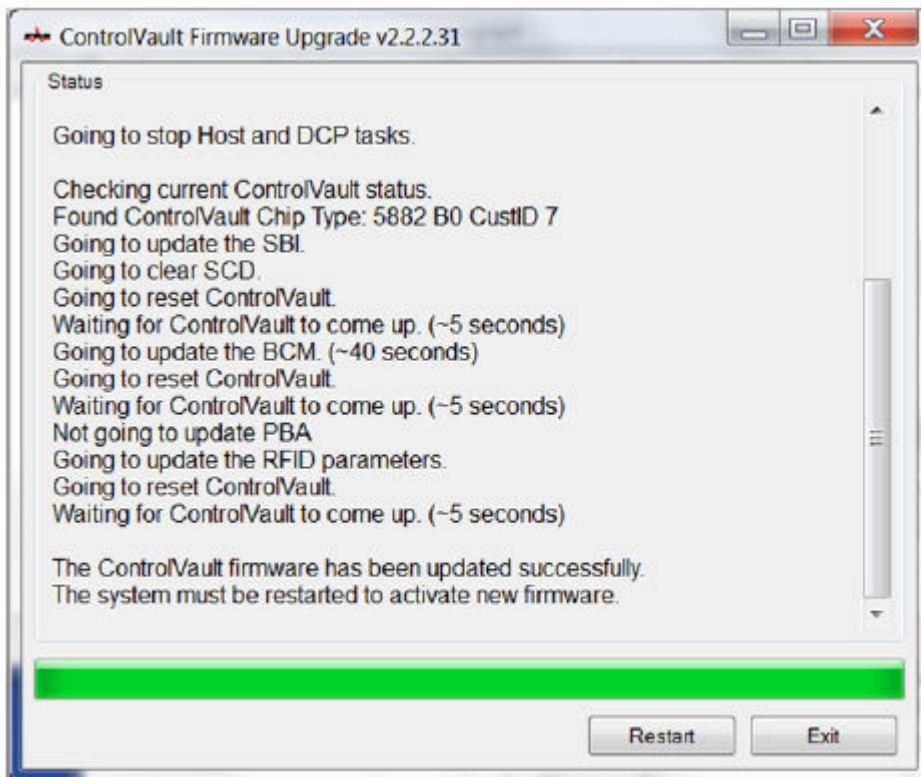
Several status messages display.







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



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

Registry Settings

This section details all Dell ProSupport approved registry settings for local client computers.

Encryption Client

(Optional) Create an Encryption Removal Agent Log File

- Before beginning the uninstall process, you can optionally create an Encryption Removal Agent log file. This log file is useful for troubleshooting an uninstall/decryption operation. If you do not intend to decrypt files during the uninstall process, you do not need to create this log file.
- The Encryption Removal Agent log file is not created until after the Encryption Removal Agent service runs, which does not happen until the computer is restarted. Once the client is successfully uninstalled and the computer is fully decrypted, the log file is permanently deleted.
- The log file path is **C:\ProgramData\Dell\Dell Data Protection\Encryption**.
- Create the following registry entry on the computer targeted for decryption.

```
[HKLM\Software\Credant\DecryptionAgent]
```

```
"LogVerbosity"=DWORD:2
```

0: no logging

1: logs errors that prevent the service from running

2: logs errors that prevent complete data decryption (recommended level)

3: logs information about all decrypting volumes and files

5: logs debugging information

Use Smart Cards with Windows Log On

- To determine if a smart card is present and active, ensure the following value is set:

```
HKLM\SOFTWARE\Dell\Dell Data Protection\
```

```
"SmartcardEnabled"=DWORD:1
```

If SmartcardEnabled is missing or has a value of zero, the Credential Provider will display only Password for authentication.

If SmartcardEnabled has a non-zero value, the Credential Provider will display options for Password and smart card authentication.

- The following registry value indicates whether Winlogon should generate a notification for logon events from smart cards.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
```

```
"SmartCardLogonNotify"=DWORD:1
```

0 = Disabled

1 = Enabled

Preserve Temp Files During Installation

- By default, all temporary files in the c:\windows\temp directory are automatically deleted during installation. Deletion of temporary files speeds initial encryption and occurs before the initial encryption sweep.

However, if your organization uses a third-party application that requires the file structure within the \temp directory to be preserved, you should prevent this deletion.

To disable temporary file deletion, create or modify the registry setting as follows:

```
[HKLM\SOFTWARE\CREDANT\CMGShield]
```

```
"DeleteTempFiles"=REG_DWORD:0
```

Not deleting temporary files increases initial encryption time.

Change the Default Behavior of the User Prompt to Begin or Delay Encryption

- The Encryption client displays the *length of each policy update delay* prompt for five minutes each time. If the user does not respond to the prompt, the next delay begins. The final delay prompt includes a countdown and progress bar, and it displays until the user responds, or the final delay expires and the required logoff/reboot occurs.

You can change the behavior of the user prompt to begin or delay encryption, to prevent encryption processing following no user response to the prompt. To do this, set the registry the following registry value:

```
[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]
```

```
"SnoozeBeforeSweep"=DWORD:1
```

Any non-zero value changes the default behavior to snooze. With no user interaction, encryption processing is delayed up to the number of configurable allowed delays. Encryption processing begins when the final delay expires.

Calculate the maximum possible delay as follows (a maximum delay would involve the user never responding to a delay prompt, each of which displays for 5 minutes):

(NUMBER OF POLICY UPDATE DELAYS ALLOWED × LENGTH OF EACH POLICY UPDATE DELAY) + (5 MINUTES × [NUMBER OF POLICY UPDATE DELAYS ALLOWED - 1])

Change the Default Use of SDUser Key

- System Data Encryption (SDE) is enforced based on the policy value for SDE Encryption Rules. Additional directories are protected by default when the SDE Encryption Enabled policy is Selected. For more information, search "SDE Encryption Rules" in AdminHelp. When the Encryption client is processing a policy update that includes an active SDE policy, the current user profile directory is encrypted by default with the SDUser key (a User key) rather than the SDE key (a Device key). The SDUser key is also used to encrypt files or folders that are copied (not moved) into a user directory that is not a encrypted with SDE.

To disable the SDUser key and use the SDE key to encrypt these user directories, create the following registry entry on the computer:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]
```

```
"EnableSDUserKeyUsage"=DWORD:00000000
```

If this registry key is not present or is set to anything other than 0, the SDUser key is used to encrypt these user directories.

Authentication

Disable Smart Card and Biometric Services (Optional)

If you do not want Advanced Authentication to change the services associated with smart cards and biometric devices to a startup type of "automatic", you can disable the service startup feature.

When disabled, Authentication does not attempt to start these three services:

- SCardSvr - Manages access to smart cards read by the computer. If this service is stopped, this computer is unable to read smart cards. If this service is disabled, any services that explicitly depend on it fail to start.

- SCPolicySvc - Allows the system to be configured to lock the user desktop upon smart card removal.
- WbioSvc - The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

Disabling this feature also suppresses warnings associated with the required services not running.

- By default, if the registry key does not exist or the value is set to 0, this feature is enabled.

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Set to 0 to Enable.

Set to 1 to Disable

Use Smart Cards with Windows Log On

- To determine if the PBA is activated, ensure that the following value is set:

[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

"PBAIsActivated"=DWORD (32-bit):1

A value of 1 means that the PBA is activated. A value of 0 means the PBA is not activated.

NOTE: Manually deleting this key can create unintended results for users syncing with the PBA resulting in the need for manual recovery.

- To determine if a smart card is present and active, ensure the following value is set:

HKLM\SOFTWARE\Dell\Dell Data Protection\

"SmartcardEnabled"=DWORD:1

If SmartcardEnabled is missing or has a value of zero, the Credential Provider will display only Password for authentication.

If SmartcardEnabled has a non-zero value, the Credential Provider will display options for Password and smart card authentication.

- The following registry value indicates whether Winlogon should generate a notification for logon events from smart cards.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

"SmartCardLogonNotify"=DWORD:1

0 = Disabled

1 = Enabled

Proceed to [Glossary](#).

Glossary

Advanced Authentication - The Advanced Authentication product provides smart card reader options. Advanced Authentication helps manage these multiple authentication methods, supports login with self-encrypting drives, SSO, and manages user credentials and passwords.

Encryption Administrator Password (EAP) - The EAP is an administrative password that is unique to each computer. Most configuration changes made in the Local Management Console require this password. This password is also the same password that is required if you have to use your LSARecovery_[hostname].exe file to recover your data. Record and save this password in a safe place.

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.

Encryption Keys - In most cases, the Encryption client uses the User key plus two additional encryption keys. However, there are exceptions: All SDE policies and the Secure Windows Credentials policy use the SDE key. The Encrypt Windows Paging File policy and Secure Windows Hibernation File policy use their own key, the General Purpose Key (GPK). The Common key makes files accessible to all managed users on the device where they were created. The User key makes files accessible only to the user who created them, only on the device where they were created. The User Roaming key makes files accessible only to the user who created them, on any Dell-encrypted Windows (or Mac) device.

Encryption Sweep - An encryption sweep is the process of scanning the folders to be encrypted on an Dell-encrypted 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 occurs upon initial receipt of a policy that has encryption enabled. This can occur immediately after activation if your policy has encryption enabled. - If the Scan Workstation on Logon policy is enabled, folders specified for encryption is swept on each user logon. - A sweep can be re-triggered under certain subsequent policy changes. Any policy change related to the definition of the encryption folders, encryption algorithms, encryption key usage (common verses user), triggers a sweep. In addition, toggling between encryption enabled and disabled triggers an encryption sweep.

Preboot Authentication (PBA) - Preboot Authentication serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system as a trusted authentication layer. The PBA prevents anything being read from the hard disk, such as the operating system, until the user has confirmed they have the correct credentials.

Single Sign-On (SSO) - SSO simplifies the logon process when multi-factor authentication is enabled at both preboot and Windows logon. If enabled, authentication is required at preboot only, and users are automatically logged on to Windows. If not enabled, authentication may be required multiple times.

System Data Encryption (SDE) - SDE is designed to encrypt the operating system and program files. To accomplish this purpose, SDE must be able to open its key while the operating system is booting. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password to unlock encryption keys. SDE policies do not encrypt the files needed by the operating system to start the boot process. SDE policies do not require preboot authentication or interfere with the Master Boot Record in any way. When the computer boots up, the encrypted files are available before any user logs in (to enable patch management, SMS, backup and recovery tools). Disabling SDE encryption triggers automatic decryption of all SDE encrypted files and directories for the relevant users, regardless of other SDE policies, such as SDE Encryption Rules.

Trusted Platform Module (TPM) - TPM is a security chip with three major functions: secure storage, measurement, and attestation. The Encryption client uses TPM for its secure storage function. The TPM can also provide encrypted containers for the software vault.