# Dell Data Protection | Encryption

## Enterprise Edition Advanced Installation Guide v8.13

## Notes, cautions, and warnings

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

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

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

**Enterprise Edition Advanced Installation Guide**

2017 - 05

Rev. A02

# Contents

**1 Introduction....................7**
Before You Begin....................7
Using This Guide....................8
Contact Dell ProSupport....................8

**2 Requirements....................9**
All Clients....................9
All Clients - Prerequisites....................9
All Clients - Hardware....................9
All Clients - Language Support....................10
Encryption Client....................10
Encryption Client Prerequisites....................11
Encryption Client Hardware....................11
Encryption Client Operating Systems....................11
External Media Shield (EMS) Operating Systems....................11
Server Encryption Client....................12
Server Encryption Client Prerequisites....................13
Server Encryption Client Hardware....................13
Server Encryption Client Operating Systems....................13
External Media Shield (EMS) Operating Systems....................14
SED Client....................15
OPAL Drivers....................15
SED Client Prerequisites....................15
SED Client Hardware....................16
SED Client Operating Systems....................17
Advanced Authentication Client....................17
Advanced Authentication Client Hardware....................17
Advanced Authentication Client Operating Systems....................18
BitLocker Manager Client....................19
BitLocker Manager Client Prerequisites....................19
BitLocker Manager Client Operating Systems....................19
Authentication Options....................19
Encryption Client....................20
SED Client....................21
BitLocker Manager....................22

**3 Registry Settings....................23**
Encryption Client Registry Settings....................23
SED Client Registry Settings....................27
Advanced Authentication Client Registry Settings....................28
BitLocker Manager Client Registry Settings....................29

**4 Install Using the Master Installer....................30**

Install Interactively Using the Master Installer....30
Install by Command Line Using the Master Installer....34

**5 Uninstall Using the Master Installer.... 36**
Uninstall the Master Installer....36
Command Line Uninstallation....36

**6 Install Using the Child Installers.... 37**
Install Drivers.... 38
Install Encryption Client....38
Command Line Installation....38
Install Server Encryption Client....41
Install Server Encryption Interactively.... 42
Install Server Encryption Using the Command Line.... 45
Activate Server Encryption....47
Install SED Management and Advanced Authentication Clients.... 50
Command Line Installation....50
Install BitLocker Manager Client.... 51
Command Line Installation....51

**7 Uninstall Using the Child Installers.... 53**
Uninstall Encryption and Server Encryption Client....54
Process....54
Command Line Uninstallation.... 54
Uninstall External Media Edition....56
Uninstall SED and Advanced Authentication Clients....56
Process.... 56
Deactivate the PBA.... 56
Uninstall SED Client and Advanced Authentication Clients.... 57
Uninstall BitLocker Manager Client....57
Command Line Uninstallation.... 57

**8 Commonly Used Scenarios.... 58**
Encryption Client and Advanced Authentication.... 59
SED Client (including Advanced Authentication) and Encryption Client.... 59
SED Client (including Advanced Authentication) and External Media Shield.... 60
BitLocker Manager and External Media Shield.... 60

**9 Download the Software....61**

**10 Pre-Installation Configuration for One-time Password, SED UEFI, and BitLocker....65**
Initialize the TPM.... 65
Pre-Installation Configuration for UEFI Computers....65
Enable Network Connectivity During UEFI Preboot Authentication....65
Disable Legacy Option ROMs....66
Pre-Installation Configuration to Set Up a BitLocker PBA Partition....66

**11 Set GPO on Domain Controller to Enable Entitlements.... 67**

**12 Extract the Child Installers from the Master Installer....70**

**13 Configure Key Server for Uninstallation of Encryption Client Activated Against EE Server.... 71**

Services Panel - Add Domain Account User.... 71

Key Server Config File - Add User for EE Server Communication.... 72

Sample Configuration File.... 73

Services Panel - Restart Key Server Service.... 73

Remote Management Console - Add Forensic Administrator.... 73

**14 Use the Administrative Download Utility (CMGAd)....75**

Use the Administrative Download Utility in Forensic Mode....75

Use the Administrative Download Utility in Admin Mode....77

**15 Configure Server Encryption.... 79**

Enable Server Encryption....79

Customize Activation Logon Dialog.... 79

Set Server Encryption EMS Policies.... 80

Suspend an Encrypted Server Instance....80

**16 Configure Deferred Activation.... 82**

Deferred Activation Customization....82

Prepare the Computer for Installation....83

Install the Encryption Client with Deferred Activation.... 83

Activate the Encryption Client with Deferred Activation....83

Troubleshoot Deferred Activation.... 84

Troubleshoot Activation....84

**17 Troubleshooting.... 87**

All Clients - Troubleshooting....87

Encryption and Server Encryption Client Troubleshooting.... 87

Upgrade to the Windows 10 Anniversary Update.... 87

Activation on a Server Operating System....87

(Optional) Create an Encryption Removal Agent Log File....90

Find TSS Version....91

EMS and PCS Interactions....91

Use WSScan.... 91

Use WSProbe....95

Check Encryption Removal Agent Status.... 96

SED Client Troubleshooting.... 97

Use the Initial Access Code Policy.... 97

Create a PBA Log File for Troubleshooting....98

Dell ControlVault Drivers....99

Update Dell ControlVault Drivers and Firmware....99

UEFI Computers....113

Troubleshoot Network Connection....113

TPM and BitLocker.... 113

TPM and BitLocker Error Codes.... 113

18 Glossary....................144

# 1

# Introduction

This guide details how to install and configure the Encryption client, SED management client, Advanced Authentication, and BitLocker Manager.

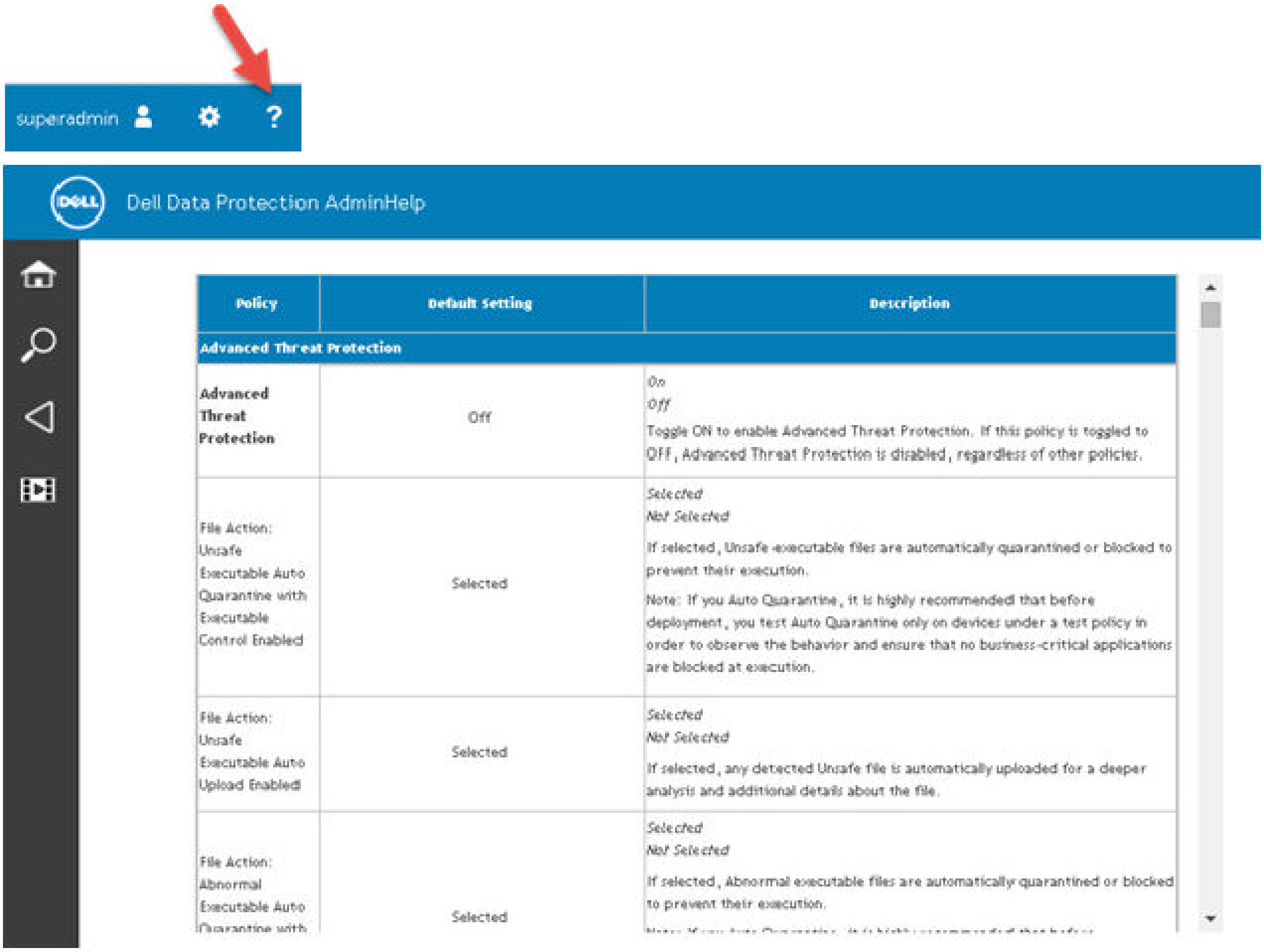
All policy information, and their descriptions are found in the AdminHelp.

## Before You Begin

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

- *DDP Enterprise Server Installation and Migration Guide*
- *DDP Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide*

Verify that polices are set as desired. Browse through the AdminHelp, available from the **?** at the far right of the screen. The AdminHelp is page-level help designed to help you set and modify policy and understand your options with your EE Server/VE Server.



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

2 Thoroughly read the Requirements chapter of this document.

3 Deploy clients to end users.

# Using This Guide

Use this guide in the following order.

- See Requirements for client prerequisites, computer hardware and software information, limitations, and special registry modifications needed for features.
- If needed, see Pre-Installation Configuration for One-time Password, SED UEFI, and BitLocker.
- If your clients will be entitled using Dell Digital Delivery (DDD), see Set GPO on Domain Controller to Enable Entitlements.
- If installing clients using the master installer, see:
    - Install Interactively Using the Master Installer

      or
    - Install by Command Line Using the Master Installer
- If installing clients using the child installers, the child installer executable files must be extracted from the master installer. See Extract the Child Installers from the Master Installer, then return here.
    - Install Child Installers by Command line:
        - Install Drivers - Download the appropriate drivers and firmware based on your authentication hardware.
        - Install Encryption Client - use these instructions to install the Encryption client, which is the component that enforces security policy, whether a computer is connected to the network, disconnected from the network, lost, or stolen.
        - Install SED Management and Advanced Authentication Clients - use these instructions to install encryption software for SEDs. Although SEDs provide their own encryption, they lack a platform to manage their encryption and policies. With SED management, all policies, storage, and retrieval of encryption keys are available from a single console, reducing the risk that computers are unprotected in the event of loss or unauthorized access.

          The Advanced Authentication client manages multiple authentication methods, including PBA for SEDs, Single Sign-on (SSO), and user credentials such as fingerprints and passwords. In addition, it provides Advanced Authentication capabilities to access websites and applications.
        - Install BitLocker Manager Client - use these instructions to install the BitLocker Manager client, designed to improve the security of BitLocker deployments and to simplify and reduce the cost of ownership.

          > **NOTE:**
          > *Most* child installers can be installed interactively, but installations are not described in this guide.
- See Commonly Used Scenarios for scripts of our most commonly used scenarios.

# Contact Dell ProSupport

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

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

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

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

# Requirements

## All Clients

These requirements apply to all clients. Requirements listed in other sections apply to specific clients.

- IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.
- The user account performing the installation/upgrade/uninstallation must be a local or domain administrator user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or Dell KACE. A non-administrator user that has elevated privileges is not supported.
- Back up all important data before beginning installation/uninstallation.
- Do not make changes to the computer, including inserting or removing external (USB) drives during installation.
- Ensure that outbound port 443 is available to communicate with the EE Server/VE Server if your master installer clients will be entitled using Dell Digital Delivery (DDD). The entitlement functionality will not work if port 443 is blocked (for any reason). DDD is not used if installing using the child installers.
- Be sure to periodically check www.dell.com/support for the most current documentation and Technical Advisories.

## All Clients - Prerequisites

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

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

  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

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

## All Clients - Hardware

- The following table details supported computer hardware.

### Hardware

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

# All Clients - Language Support

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

### Language Support

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

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

### Language Support

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

# Encryption Client

- The client computer must have network connectivity to activate.
- To reduce initial encryption time, 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. See Extract the Child Installers from the Master Installer for extraction instructions.
- 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 http://www.dell.com/support/article/us/en/19/SLN304039.
- The Encryption client has been tested and is compatible with McAfee, the Symantec client, Kaspersky, and MalwareBytes. Hard-coded exclusions are in place in for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. The Encryption client has also been tested with the Microsoft Enhanced Mitigation Experience Toolkit.

  If your organization uses an anti-virus provider that is not listed, see http://www.dell.com/support/Article/us/en/19/SLN298707 or Contact Dell ProSupport for help.

- 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.
- In-place operating system upgrade is not supported with the Encryption client installed. Uninstall and decrypt the Encryption client, upgrade to the new operating system, and then re-install the Encryption client.

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

# Encryption Client Prerequisites

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

# Encryption Client Hardware

- The following table details supported 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<br>• Windows Embedded Standard 7 with Application Compatibility template (hardware encryption is not supported)<br>• Windows 8: Enterprise, Pro<br>• Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition<br>• Windows Embedded 8.1 Industry Enterprise (hardware encryption is not supported)<br>• Windows 10: Education, Enterprise, Pro<br>• VMware Workstation 5.5 and higher |

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

# External Media Shield (EMS) Operating Systems

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

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

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

### Windows Operating Systems Supported to Access EMS-Protected Media (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

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

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

# Server Encryption Client

Server Encryption is intended for use on computers running in server mode, particularly file servers.

- Server Encryption is compatible only with Enterprise Edition and Endpoint Security Suite Enterprise.
- Server Encryption provides the following:
  - Software encryption
  - Removable storage encryption
  - Port control

    ⓘ **NOTE:**
    The server must support port controls.

    Server Port Control System policies affect removable media on protected servers, for example, by controlling access and usage of the server's USB ports by USB devices.USB port policy applies to external USB ports. Internal USB port functionality is not affected by USB port policy. If USB port policy is disabled, the client USB keyboard and mouse will not work and the user will not be able to use the computer unless a Remote Desktop Connection is set up before the policy is applied.

**Server Encryption is for use on:**

- File servers with local drives
- Virtual Machine (VM) guests running a Server operating system or non-Server operating system as a simple file server
- Supported configurations:
  - Servers equipped with RAID 5 or 10 drives; RAID 0 (striping) and RAID 1 (mirroring) are supported independent of each other.
  - Servers equipped with Multi TB RAID drives
  - Servers equipped with drives that can be changed out without shutting down the computer
  - Server Encryption has been tested and is compatible with McAfee VirusScan, Symantec clients, Kaspersky Anti-Virus, and MalwareBytes Anti-Malware. Hard-coded exclusions are in place for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. If your organization uses an anti-virus provider that is not listed, see KB article SLN298707 or contact Dell ProSupport for help.

**Not Supported**

Server Encryption is not for use on:

- Dell Data Protection Server or servers running databases for Dell Data Protection Server
- Server Encryption is not compatible with Endpoint Security Suite, Personal Edition, or Security Tools.
- Server Encryption is not supported with SED Management or BitLocker Manager client.
- Migration to or from Server Encryption is not supported. Upgrades from External Media Edition to Server Encryption require that the previous product or products be uninstalled completely before installing Server Encryption.
- VM hosts (A VM Host typically contains multiple VM guests.)
- Domain Controllers
- Exchange Servers
- Servers hosting databases (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Servers using any of the following technologies:
    - Resilient file systems
    - Fluid file systems
    - Microsoft storage spaces
    - SAN/NAS network storage solutions
    - iSCSI connected devices
    - Deduplication software
    - Hardware deduplication
    - Split RAIDs (multiple volumes across a single RAID)
    - SED drives (RAIDs and NON-RAID)
    - Auto-logon (Windows OS 7, 8/8.1) for kiosks
    - Microsoft Storage Server 2012
- Server Encryption does not support dual boot configurations since it is possible to encrypt system files of the other operating system, which would interfere with its operation.
- In-place operating system upgrade is not supported with Server Encryption. To upgrade your operating system, uninstall and decrypt Server Encryption, upgrade to the new operating system, and then re-install Server Encryption.

  Additionally, operating system re-installs are not supported. If you want 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 by following recovery procedures. For more information about recovering encrypted data, refer to the *Recovery Guide*.

# Server Encryption Client Prerequisites

- You must install this component before installing the Server Encryption client.

| Prerequisite |
|---|
| • Visual C++ 2012 Update 4 or later Redistributable Package (x86 and x64) |

# Server Encryption Client Hardware

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

# Server Encryption Client Operating Systems

The following table details supported operating systems.

### Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Home, Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

### Supported Server Operating Systems

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition with and without Hyper-V, Enterprise Edition with and without Hyper-V, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition

### Operating Systems Supported with UEFI Mode

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

ⓘ **NOTE:**

On a supported UEFI computer, after selecting **Restart** from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture.

## External Media Shield (EMS) Operating Systems

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

ⓘ **NOTE:**

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

ⓘ **NOTE:**

Windows XP is supported when using EMS Explorer only.

### Windows Operating Systems Supported to Access EMS-Protected Media (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

### Supported Server Operating Systems

- Windows Server 2012 R2

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

- Mac OS X Yosemite 10.10.5

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

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

# SED Client

- The computer must have a wired network connection to successfully install SED management.
- IPv6 is not supported.
- Be prepared to shut down and restart the computer after you apply policies and are ready to begin enforcing them.
- Computers equipped with self-encrypting drives cannot be used with HCA cards. Incompatibilities exist that prevent the provisioning of the HCA. Dell does not sell computers with self-encrypting drives that support the HCA module. This unsupported configuration would be an after-market configuration.
- If the computer targeted for encryption is equipped with a self-encrypting drive, ensure that the Active Directory option, *User Must Change Password at Next Logon*, is disabled. Preboot Authentication does not support this Active Directory option.
- Dell recommends that you do not change the authentication method after the PBA has been activated. If you must switch to a different authentication method, you must either:

  - Remove all the users from the PBA.

  or

  - Deactivate the PBA, change the authentication method, and then re-activate the PBA.

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

- SED Management is not supported with Server Encryption.

# OPAL Drivers

- Supported OPAL compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support.

# SED Client Prerequisites

- The master installer installs Microsoft Visual C++2010 SP1 **and** Microsoft Visual C++ 2012 Update 4 if not already installed on the computer. **When using the child installer**, you must install these components before installing SED management.

  #### Prerequisites

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

# SED Client Hardware

### OPAL Compliant SEDs

- For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

### Dell Computer Models Supported with UEFI

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

**Dell Computer Models - UEFI Support**

- Latitude 5280
- Latitude 5480
- Latitude 5580
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7280
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M5520
- Precision M6800
- Precision M7510
- Precision M7520
- Precision M7710
- Precision M7720
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 Tower, Small Form Factor, Micro
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 5050 Tower, Small Form Factor, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- OptiPlex 7050 Tower, Small Form Factor, Micro
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

> **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.

### International Keyboards

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

**International Keyboard Support - UEFI**

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

### International Keyboard Support - Non-UEFI

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

# SED Client Operating Systems

- The following table details the supported operating systems.

### Windows Operating Systems (32- and 64-bit)

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

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

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

# Advanced Authentication Client

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

  To continue using the Microsoft Operating System to manage user credentials, do not install Security Tools or uninstall it.
- The Security Tools One-time Password (OTP) feature requires that a TPM is present, enabled, and owned. OTP is not supported with TPM 2.0. To clear and set ownership of the TPM, see https://technet.microsoft.com.
- An SED does not require a TPM to provide Advanced Authentication or encryption.

# Advanced Authentication Client Hardware

- The following table details supported authentication hardware.

### Fingerprint and Smart Card Readers

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

### Contactless Cards

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

### Smart Cards

- PKCS #11 Smart Cards using the ActivIdentity client

### Smart Cards

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

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

- The following table details Dell computer models supported with SIPR Net cards.

### Dell Computer Models - Class B/SIPR Net Card Support

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

# Advanced Authentication Client Operating Systems

### Windows Operating Systems

- The following table details supported operating systems.

### Windows Operating Systems (32- and 64-bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

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

### Mobile Device Operating Systems

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

### Android Operating Systems

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

### iOS Operating Systems

- iOS 7.x
- iOS 8.x

### Windows Phone Operating Systems

- Windows Phone 8.1
- Windows 10 Mobile

# BitLocker Manager Client

- Consider reviewing Microsoft BitLocker requirements if BitLocker is not yet deployed in your environment,
- Ensure that the PBA partition is already set up. If BitLocker Manager is installed before the PBA partition is set up, BitLocker cannot be enabled and BitLocker Manager will not be operational. See Pre-Installation Configuration to Set Up a BitLocker PBA Partition.
- The keyboard, mouse, and video components must be directly connected to the computer. Do not use a KVM switch to manage peripherals as the KVM switch can interfere with the computer's ability to properly identify hardware.
- Turn on and enable the TPM. BitLocker Manager will take ownership of the TPM and will not require a reboot. However, if a TPM ownership already exists, BitLocker Manager will begin the encryption setup process (no restart is required). The point is that the TPM must be "owned" and enabled.
- The BitLocker Manager client will use the approved AES FIPS validated algorithms if FIPS mode is enabled for the GPO security setting "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" on the device and you manage that device via our product. We do not force this mode as default for BitLocker-encrypted clients because Microsoft now suggests customers not use their FIPS validated encryption due to numerous issues with application compatibility, recovery, and media encryption: http://blogs.technet.com.
- BitLocker Manager is not supported with Server Encryption.

# BitLocker Manager Client Prerequisites

- The master installer installs Microsoft Visual C++2010 SP1 **and** Microsoft Visual C++ 2012 Update 4 if not already installed on the computer. **When using the child installer**, you must install these components before installing BitLocker Manager.

**Prerequisites**

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

# BitLocker Manager Client Operating Systems

- The following table details supported operating systems.

**Windows Operating Systems**

- Windows 7 SP0-SP1: Enterprise, Ultimate (32- and 64-bit)
- Windows 8: Enterprise (64-bit)
- Windows 8.1: Enterprise Edition, Pro Edition (64-bit)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64-bit)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64-bit)
- Windows Server 2016

# Authentication Options

- The following authentication options require specific hardware: Fingerprints, Smart Cards, Contactless Cards, Class B/SIPR Net Cards, and authentication on UEFI computers. The following options require configurations: smart cards with Windows Authentication, smart cards with Preboot Authentication, and One-time Password. The following tables show authentication options available by operating system, when hardware and configuration requirements are met.

# Encryption Client

**Non-UEFI**

| | **PBA** | | | | | **Windows Authentication** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Password** | **Fingerprint** | **Contacted Smart card** | **OTP** | **SIPR Card** | **Password** | **Fingerprint** | **Smart card** | **OTP** | **SIPR Card** |
| Windows 7 SP0-SP1 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8.1 Update 0-1 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 10 | | | | | | X | X[2] | X[2] | X[1] | X[2] |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

**UEFI**

| | **PBA - on supported Dell computers** | | | | | **Windows Authentication** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Password** | **Fingerprint** | **Contacted Smart card** | **OTP** | **SIPR Card** | **Password** | **Fingerprint** | **Smart card** | **OTP** | **SIPR Card** |
| Windows 7 SP0-SP1 | | | | | | | | | | |
| Windows 8 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8.1 Update 0-1 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 10 | | | | | | X | X[2] | X[2] | X[1] | X[2] |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

# SED Client

### Non-UEFI

| | PBA | | | | | Windows Authentication | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Password** | **Fingerprint** | **Contacted Smart card** | **OTP** | **SIPR Card** | **Password** | **Fingerprint** | **Smart card** | **OTP** | **SIPR Card** |
| Windows 7 SP0-SP1 | X[2] | | X[2,3] | | | X | X[3] | X[3] | X[1] | X[3] |
| Windows 8 | X[2] | | X[2,3] | | | X | X[3] | X[3] | X[1] | X[3] |
| Windows 8.1 | X[2] | | X[2,3] | | | X | X[3] | X[3] | X[1] | X[3] |
| Windows 10 | X[2] | | X[2,3] | | | X | X[3] | X[3] | X[1] | X[3] |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

3. Available with a supported OPAL SED.

### UEFI

| | PBA - on supported Dell computers | | | | | Windows Authentication | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Password** | **Fingerprint** | **Contacted Smart card** | **OTP** | **SIPR Card** | **Password** | **Fingerprint** | **Smart card** | **OTP** | **SIPR Card** |
| Windows 7 | | | | | | | | | | |
| Windows 8 | X[4] | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8.1 | X[4] | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 10 | X[4] | | | | | X | X[2] | X[2] | X[1] | X[2] |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

4. Available with a supported OPAL SED on supported UEFI computers.

# BitLocker Manager

| | Non-UEFI | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PBA [5] | | | | | Windows Authentication | | | | |
| | Password | Fingerprint | Contacted Smart card | OTP | SIPR Card | Password | Fingerprint | Smart card | OTP | SIPR Card |
| Windows 7 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8.1 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 10 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows Server 2008 R2 (64-bit) | | | | | | X | | X[2] | | |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

5. BitLocker Preboot PIN is managed through Microsoft functionality.

**UEFI**

| | PBA[5] - on supported Dell computers | | | | | Windows Authentication | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Password | Fingerprint | Contacted Smart card | OTP | SIPR Card | Password | Fingerprint | Smart card | OTP | SIPR Card |
| Windows 7 | | | | | | | | | | |
| Windows 8 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 8.1 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows 10 | | | | | | X | X[2] | X[2] | X[1] | X[2] |
| Windows Server 2008 R2 (64-bit) | | | | | | X | | X[2] | | |

1. Available when installed with the master installer or with Advanced Authentication package when using the child installers.

2. Available when authentication drivers are downloaded from support.dell.com.

5. BitLocker Preboot PIN is managed through Microsoft functionality.

# 3

# Registry Settings

- This section details all Dell ProSupport approved registry settings for local **client** computers, regardless of the reason for the registry setting. If a registry setting overlaps two products, it will be listed in each category.
- These registry changes should be done by Administrators only and may not be appropriate or work in all scenarios.

## Encryption Client Registry Settings

- If a self-signed certificate is used on the Dell Server for Enterprise Edition for Windows, certificate trust validation must remain disabled on the client computer (trust validation is *disabled* by default with Enterprise Edition for Windows). Before *enabling* trust validation on the client computer, the following requirements must be met.
  - A certificate signed by a root authority, such as EnTrust or Verisign, must be imported into EE Server/VE Server.
  - The full chain of trust of the certificate must be stored in the Microsoft keystore on the client computer.
  - To *enable* trust validation for EE for Windows, change the value of the following registry entry to 0 on the client computer.

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "IgnoreCertErrors"=dword:00000000

    0 = Fail if a certificate error is encountered

    1= Ignores errors
- To use smart cards with Windows Authentication, the following registry value must be set on the client computer.

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1
- To create an Encryption Removal Agent log file, create the following registry entry on the computer targeted for decryption. See (Optional) Create an Encryption Removal Agent Log File.

  [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
- By default, during installation, the system tray icon is displayed. Use the following registry setting to hide the system tray icon for all managed users on a computer after the original installation. Create or modify the registry setting as follows:

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=dword:1

- 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.
- 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 will change the default behavior to snooze. With no user interaction, encryption processing will be 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])
- Use the following registry setting to have the Encryption client poll the EE Server/VE Server for a forced policy update. Create or modify the registry setting as follows:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  The registry setting will automatically disappear when done.
- Use the following registry settings to either allow the Encryption client to send an optimized inventory to the EE Server/VE Server, send a full inventory to the EE Server/VE Server, or to send a full inventory for all activated users to the EE Server/VE Server.
  - Send Optimized Inventory to EE Server/VE Server:

    Create or modify the registry setting as follows:

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "OnlySendInvChanges"=REG_DWORD:1

    If no entry is present, optimized inventory is sent to the EE Server/VE Server.
  - Send Full Inventory to EE Server/VE Server:

    Create or modify the registry setting as follows:

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "OnlySendInvChanges"=REG_DWORD:0

If no entry is present, optimized inventory is sent to the EE Server/VE Server.

- Send Full Inventory for All Activated Users

  [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

  "RefreshInventory"=REG_DWORD:1

  This entry is deleted from the registry as soon as it is processed. The value is saved in the vault, so even if the computer is rebooted before the inventory upload takes place, the Encryption client still honors this request the next successful inventory upload.

  This entry supersedes the OnlySendInvChanges registry value.

- Slotted Activation is a feature that allows you to spread activations of clients over a set time period in order to ease EE Server/VE Server load during a mass deployment. Activations are delayed based on algorithmically generated time slots to provide a smooth distribution of activation times.

  For users requiring activation through VPN, a slotted activation configuration for the client may be required, to delay initial activation for long enough to allow time for the VPN client to establish a network connection.

  > ⓘ **IMPORTANT:**
  > Configure Slotted Activation only with the assistance of Dell ProSupport. Improper time slot configuration could result in large numbers of clients attempting to activate against an EE Server/VE Server at once, creating potentially severe performance issues.

  These registry entries require a restart of the computer for the updates to take effect.

  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\SlottedActivation]

    Enables or disables Slotted Activation

    Disabled=0 (default)

    Enabled=1

  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat]

    The time period in seconds that the activation slot interval occurs. Use this setting to override the time period in seconds that the activation slot interval occurs. 25200 seconds are available for slotting activations during a seven-hour period. The default setting is 86400 seconds, which represents a daily repeat.

  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals]

    The interval within the repeat, ACTIVATION_SLOT_CALREPEAT, when all activation time slots occur. Only one interval is allowed. This setting should be 0,<CalRepeat>. An offset from 0 could yield unexpected results. The default setting is 0,86400. To set a seven-hour repeat, use the setting 0,25200. CALREPEAT is activated when a user logs in.

  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold]

    The number of activation slots that can be missed before the computer attempts to activate upon the next login of the user whose activation has been slotted. If activation fails during this immediate attempt, the client resumes slotted activation attempts. If activation fails due to a network failure, activation is attempted upon network reconnection, even if the value in MISSTHRESHOLD has not been exceeded. If a user logs out before the activation slot time is reached, a new slot is assigned upon next login.

  - [HKCU/Software/CREDANT/ActivationSlot] (per-user data)

    Deferred time to attempt the slotted activation, which is set when the user logs onto the network for the first time after slotted activation is enabled. The activation slot is recalculated for each activation attempt.

  - [HKCU/Software/CREDANT/SlotAttemptCount] (per-user data)

Number of failed or missed attempts, when the time slot arrives and activation is attempted but fails. When this number reaches the value set in ACTIVATION_SLOT_MISSTHRESHOLD, the computer attempts one immediate activation upon connecting to the network.

- To detect unmanaged users on the client computer, set the following registry value on the client computer:

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=DWORD value:1

  Detect unmanaged users on this computer=1

  Do not detect unmanaged users on this computer=0
- Access to external media encrypted with External Media Edition can be restricted to computers with access to the EE Server/VE Server that produced the encryption keys with which the media was encrypted.

  This feature is enabled by setting the following registry:

  [HKLM\SYSTEM\CurrentControlSet\Services\EMS]

  "EnterpriseUsage"=dword:0

  Off (default)=0

  File Access Restricted to Enterprise=1

  If this value is changed after files on external media are encrypted, the files will be re-encrypted based on the updated registry key value when the media is connected to the computer on which the registry setting was updated.
- To enable silent automatic reactivation in the rare case that a user becomes deactivated, the following registry value must be set on the client computer.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=dword:00000001

  0=Disabled (default)

  1=Enabled
- 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 will be used to encrypt these user directories.

  For more information about SDUser, see www.dell.com/support/article/us/en/19/SLN304916
- Setting the registry entry, EnableNGMetadata, if issues occur related with Microsoft updates on computers with Common key-encrypted data or with encrypting, decrypting, or unzipping large numbers of files within a folder.

  Set the EnableNGMetadata registry entry in the following location:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

"EnableNGMetadata" = dword:1

0=Disabled (default)

1=Enabled

- The non-domain activation feature can be enabled by contacting Dell ProSupport and requesting instructions.

# SED Client Registry Settings

- To set the retry interval when the EE Server/VE Server is unavailable to communicate with the SED client, add the following registry value.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=dword:300

  This value is the number of seconds the SED client waits to attempt to contact the EE Server/VE Server if it is unavailable to communicate with the SED client. The default is 300 seconds (5 minutes).
- If a self-signed certificate is used on the EE Server/VE Server for SED management, SSL/TLS trust validation must remain disabled on the client computer (SSL/TLS trust validation is *disabled* by default with SED management). Before *enabling* SSL/TLS trust validation on the client computer, the following requirements must be met.

  - A certificate signed by a root authority, such as EnTrust or Verisign, must be imported into EE Server/VE Server.
  - The full chain of trust of the certificate must be stored in the Microsoft keystore on the client computer.
  - To *enable* SSL/TLS trust validation for SED management, change the value of the following registry entry to 0 on the client computer.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Enabled

    1 = Disabled
- To use smart cards with Windows Authentication, the following registry value must be set on the client computer.

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1
- To use smart cards with Preboot Authentication, the following registry value must be set on the client computer. Also set the Authentication Method policy to Smart Card in the Remote Management Console, and commit the change.

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1
- 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.
- To set the interval at which the SED client will attempt to contact the EE Server/VE Server when it is unavailable to communicate with the SED client, set the following value on the client computer:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD Value:300

This value is the number of seconds the SED client waits to attempt to contact the EE Server/VE Server if it is unavailable to communicate with the SED client. The default is 300 seconds (5 minutes).

- The Security Server host may be changed from the original installation location if needed. The host information is read by the client computer every time a policy poll occurs. Change the following registry value on the client computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com
- The Security Server port may be changed from the original installation location if needed. This value is read by the client computer every time a policy poll occurs. Change the following registry value on the client computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888
- The Security Server URL may be changed from the original install location if needed. This value is read by the client computer every time a policy poll occurs. Change the following registry value on the client computer:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

# Advanced Authentication Client Registry Settings

- If you **do not** want the Advanced Authentication client (Security Tools) to change the services associated with smart cards and biometric devices to a startup type of "automatic", disable the service startup feature. Disabling this feature also suppresses warnings associated with the required services not running.

  When **disabled**, Security Tools will not attempt to start these services:

  - SCardSvr - Manages access to smart cards read by the computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.
  - SCPolicySvc - Allows the system to be configured to lock the user desktop upon smart card removal.
  - WbioSrvc - 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.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Enabled

    1 = Disabled
- To use smart cards with Windows Authentication, the following registry value must be set on the client computer.

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1
- To use smart cards with SED Preboot Authentication, the following registry value must be set on the client computer that is equipped with an SED.

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1

  Set the Authentication Method policy to Smart Card in the Remote Management Console, and commit the change.

# BitLocker Manager Client Registry Settings

- If a self-signed certificate is used on the EE Server/VE Server for BitLocker Manager, SSL/TLS trust validation must remain disabled on the client computer (SSL/TLS trust validation is *disabled* by default with BitLocker Manager). Before *enabling* SSL/TLS trust validation on the client computer, the following requirements must be met.
  - A certificate signed by a root authority, such as EnTrust or Verisign, must be imported into EE Server/VE Server.
  - The full chain of trust of the certificate must be stored in the Microsoft keystore on the client computer.
  - To *enable* SSL/TLS trust validation for BitLocker Manager, change the value of the following registry entry to 0 on the client computer.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Enabled

    1 = Disabled

# Install Using the Master Installer

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

  or

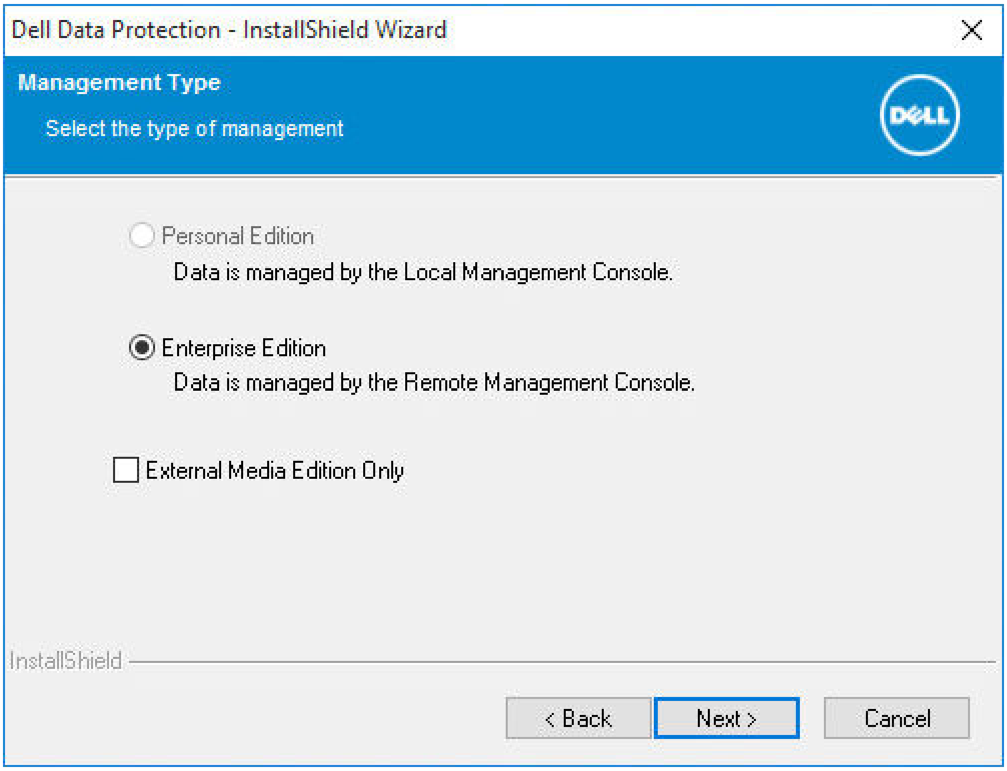
  - Install by Command Line Using the Master Installer

## Install Interactively Using the Master Installer

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

1. Locate **DDPSetup.exe** in the Dell installation media. Copy it to the local computer.
2. Double-click to launch the installer. This may take several minutes.
3. Click **Next** in the Welcome dialog.
4. Read the license agreement, accept the terms, and click **Next**.
5. Select **Enterprise Edition** and click **Next.**

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



Dell Data Protection - InstallShield Wizard

**Management Type**

Select the type of management

○ Personal Edition

Data is managed by the Local Management Console.

● Enterprise Edition

Data is managed by the Remote Management Console.

□ External Media Edition Only

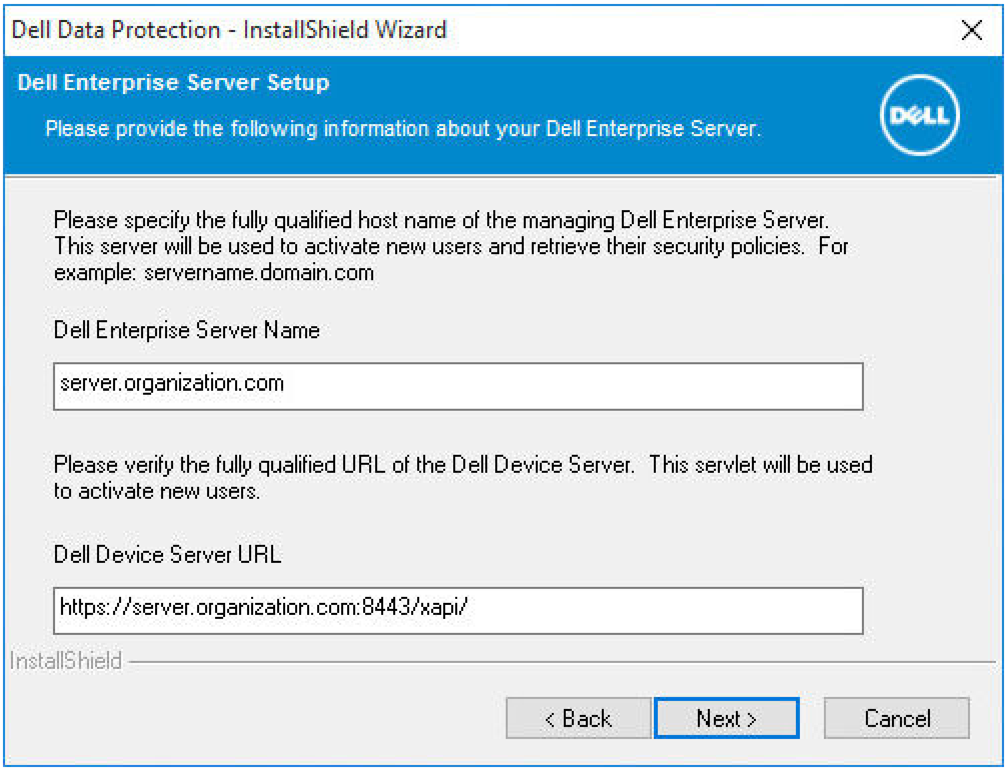
6 In the **Enterprise Server Name** field, enter the fully qualified host name of the EE Server/VE Server that will manage the target user, such as server.organization.com.

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

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

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

Click **Next.**


Dell Data Protection - InstallShield Wizard

Dell Enterprise Server Setup

Please provide the following information about your Dell Enterprise Server.

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

Dell Enterprise Server Name

server.organization.com

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

Dell Device Server URL

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

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

8 Select the components to be installed.

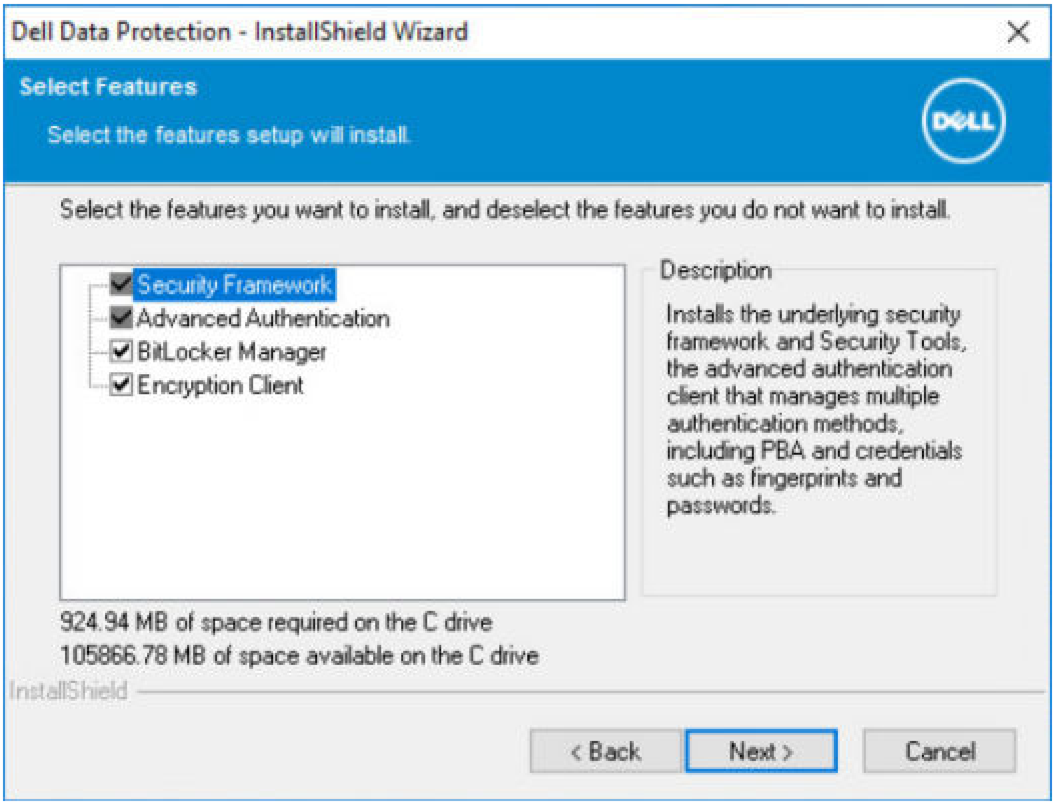
*Security Framework* installs the underlying security framework and Security Tools, the advanced authentication client that manages multiple authentication methods, including PBA and credentials such as fingerprints and passwords.

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

*Encryption* installs the Encryption client, the component that enforces security policy, whether a computer is connected to the network, disconnected from the network, lost, or stolen.

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

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


Dell Data Protection - InstallShield Wizard

**Select Features**

Select the features setup will install.

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

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

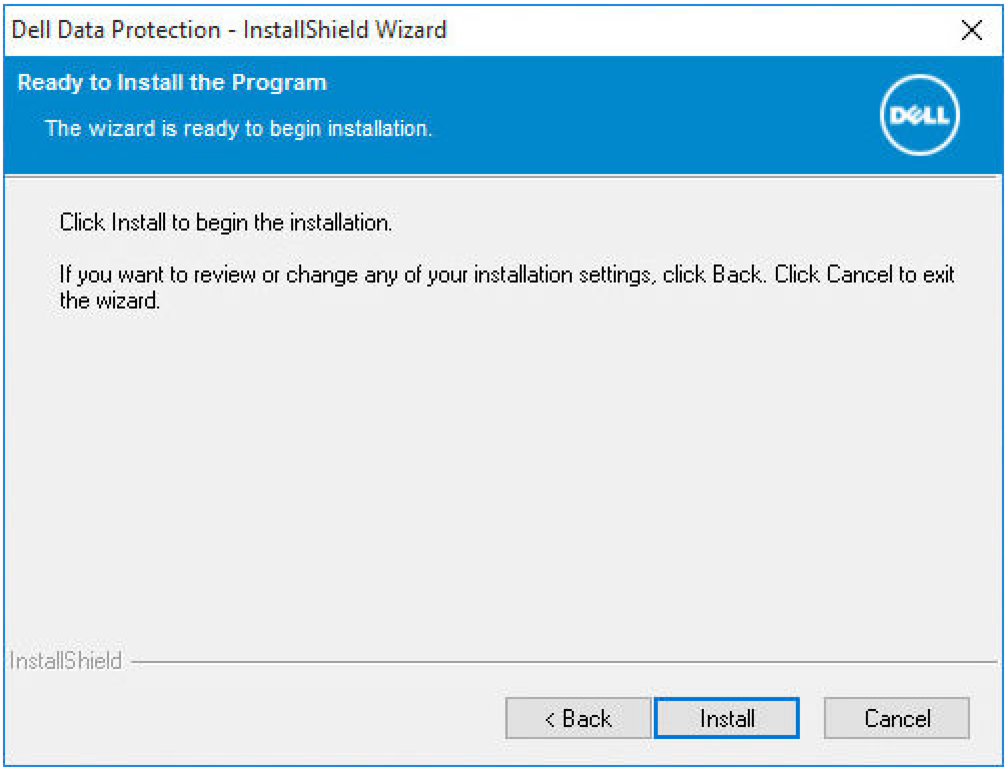
Description

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

924.94 MB of space required on the C drive

105866.78 MB of space available on the C drive

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


Dell Data Protection - InstallShield Wizard

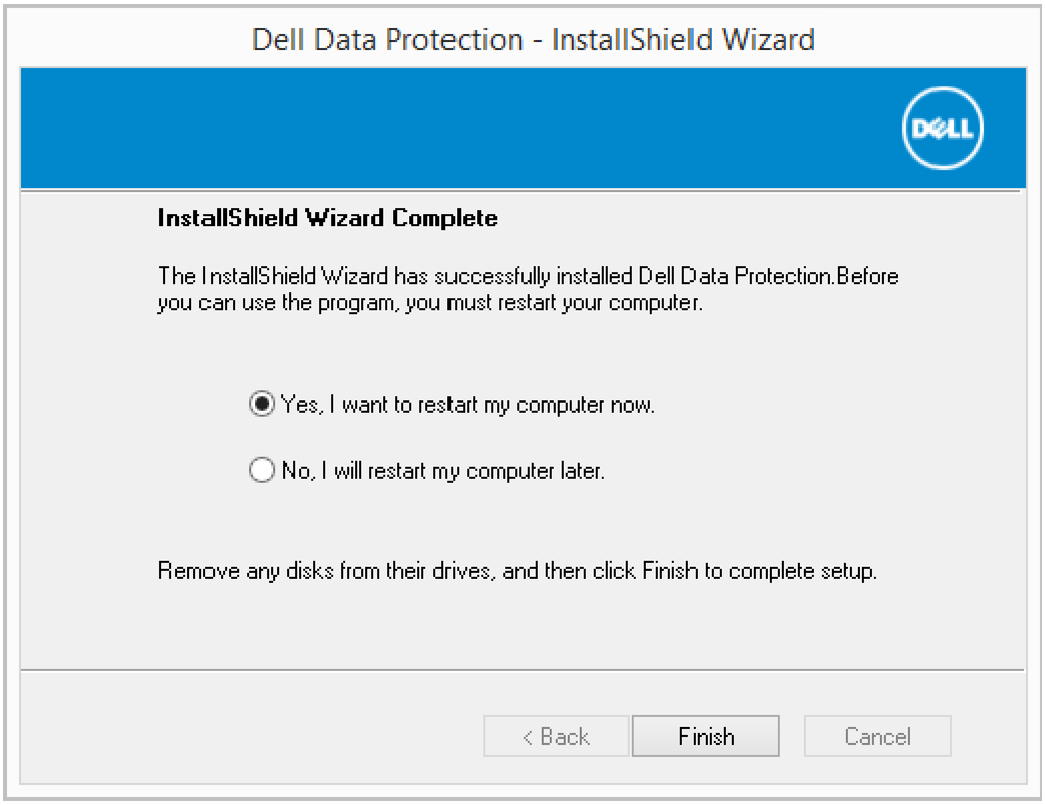
**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

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

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



Dell Data Protection - InstallShield Wizard

**InstallShield Wizard Complete**

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

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

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

Installation is complete.

# Install by Command Line Using the Master Installer

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

**Switches**

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

| Switch | Description |
|---|---|
| -y -gm2 | Pre-extraction of master installer. The -y and -gm2 switches must be used together.<br>Do not separate the switches. |
| /S | Silent installation |
| /z | Pass variables to the .msi inside the DDPSetup.exe |

**Parameters**

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

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

| Parameter | Description |
|---|---|
| FEATURES | Specifies the components that can be installed in SILENT mode.<br>DE = Drive Encryption (Encryption client)<br>EME = External Media Edition only<br>BLM = BitLocker Manager<br>SED = Self-encrypting Drive management (EMAgent/Manager, PBA/GPE Drivers) |
| BLM_ONLY=1 | Must be used when using FEATURES=BLM in the command line to exclude the SED Management plugin. |

### Example Command Line

- Command line parameters are case-sensitive.
- This example installs all components using the master installer on standard ports, silently, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs SED Management and External Media Edition with the master installer, on standard ports, silently, with a suppressed reboot, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs SED Management with the master installer, on standard ports, silently, with a suppressed reboot, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs SED Management with the master installer, on standard ports, silently, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs the Encryption client and BitLocker Manager (without the SED Management plugin), with the master installer, on standard ports, silently, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs BitLocker Manager (with the SED Management plugin) and External Media Edition, with the master installer, on standard ports, silently, with a suppressed reboot, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

- This example installs BitLocker Manager (without the SED Management plugin) and External Media Edition, with the master installer, on standard ports, silently, with a suppressed reboot, in the default location of **C:\Program Files\Dell\Dell Data Protection**, and configures it to use the specified EE Server/VE Server.

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

# Uninstall Using the Master Installer

- Each component must be uninstalled separately, followed by uninstallation of the master installer. The clients must be uninstalled in a **specific order to prevent uninstallation failures**.
- Follow the instructions in Extract the Child Installers from the Master Installer to obtain child installers.
- Ensure that the same version of master installer (and thereby clients) is used for uninstallation as installation.
- This chapter refers you to other chapters that contain *detailed* instructions of how to uninstall the child installers. This chapter explains the last step **only**, uninstalling the master installer.
- Uninstall the clients in the following order.

  a Uninstall Encryption Client.

  b Uninstall SED and Advanced Authentication Clients.

  c Uninstall BitLocker Manager Client.

  The Driver package does not need to be uninstalled.
- Proceed to Uninstall the Master Installer.

## Uninstall the Master Installer

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

### Command Line Uninstallation

- The following example silently uninstalls the master installer.

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

  Reboot the computer when finished.

# Install Using the Child Installers

- To install each client individually, the child executable files must first be extracted from the master installer, as shown in Extract the Child Installers from the Master Installer.
- Command examples included in this section assume the commands are run from C:\extracted.
- 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.
- Use these installers to install the clients using a scripted installation, batch files, or any other push technology available to your organization.
- The reboot has been suppressed in the command line examples. However, an eventual reboot is required. Encryption cannot begin until the computer has rebooted.
- 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 be create a log file by using /l*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  setup.exe. The content must always be enclosed in plain-text quotes. |
| /s | Silent mode |
| /x | Uninstall mode |
| /a | Administrative install (will copy all files inside the .msi) |

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

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

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

- Instruct users to see the following document and help files for application assistance:
  - See the *Dell Encrypt Help* to learn how to use the feature of the Encryption client. Access the help from <Install dir>:\Program Files \Dell\Dell Data Protection\Encryption\Help.
  - See the *EMS Help* to learn how the features of External Media Shield. Access the help from <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS.
  - See the *DDP Console Help* to learn how to use the features of Advanced Authentication. Access the help from <Install dir>: \Program Files\Dell\Dell Data Protection\Security Tools \Help.

# Install Drivers

- Drivers and firmware for 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 http://www.dell.com/support and selecting your computer model. Download the appropriate drivers and firmware based on your authentication hardware.
  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

  If installing on non-Dell hardware, download updated drivers and firmware from that vendor's website.

# 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.
- Users should update their policies by right-clicking the Dell Data Protection icon in the system tray and selecting **Check for Policy Updates** after installation completes.
- The Encryption client installer can be located at:
  - **From support.dell.com** - If needed, Obtain the Software from support.dell.com and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Encryption**.
  - **From Your Dell FTP Account** - Locate the installation bundle at DDP-Enterprise-Edition-8.x.x.xxx.zip and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Encryption**.

# Command Line Installation

- The following table details the parameters available for the installation.

| Parameters |
|---|
| SERVERHOSTNAME=<ServerName> (FQDN of the Dell Server for re-activation) |
| POLICYPROXYHOSTNAME=<RGKName> (FQDN of the default Policy Proxy) |
| MANAGEDDOMAIN=<MyDomain> (Domain to be used for the device) |

| Parameters |
|---|
| DEVICESERVERURL=<DeviceServerName/SecurityServerName> (URL used for activation; usually includes server name, port, and xapi) |
| GKPORT=<NewGKPort> (Gatekeeper port) |
| MACHINEID=<MachineName> (Computer name) |
| RECOVERYID=<RecoveryID> (Recovery ID) |
| REBOOT=ReallySuppress (Null allows for automatic reboots, ReallySuppress disables reboot) |
| HIDEOVERLAYICONS=1 (0 enables overlay icons, 1 disables overlay icons) |
| HIDESYSTRAYICON=1 (0 enables the systray icon, 1 disables the systray icon) |
| EME=1 (Install External Media Edition mode) |

For a list of basic .msi switches and display options that can be used in command lines, refer to Install Using the Child Installers.

- The following table details additional optional parameters related with activation.

| Parameters |
|---|
| SLOTTEDACTIVATON=1 (0 disables delayed/scheduled activations, 1 enables delayed/scheduled activations) |
| SLOTINTERVAL=30,300 (Schedules activations through x,x notation where the first value is the lower limit of the schedule and the second value is the upper limit - in seconds) |
| CALREPEAT=300 (MUST match or exceed the upper limit set in SLOTINTERVAL. Number of seconds the Encryption client waits before generating an activation attempt based on SLOTINTERVAL.) |

### Example Command Line

- The following example installs the client with default parameters (Encryption client, Encrypt for Sharing, no dialogue, no progress bar, automatic restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ /qn"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.
- The following example installs the Encryption client and Encrypt for Sharing, hides the DDP system tray icon, hides the overlay icons, no dialogue, no progress bar, suppresses restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ HIDESYSTRAYICON=1 HIDEOVERLAYICONS=1
REBOOT=ReallySuppress /qn"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

- Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.
- **Example Command Line to Install External Media Edition (EME) Only**
- Silent installation, no progress bar, automatic restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ EME=1 /qn"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.
- Silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection)

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
```

- Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.

> **NOTE:**
>
> Although the About box in the client displays software version number information, it does not display whether a full client is installed or EME only. To locate this information, go to C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log and find the following entry:
>
> [<date/timestamp>      DeviceInfo: <   >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

**Example Command Line to Convert External Media Edition to Full Shield Version**

- Decryption is not needed when converting External Media Edition to a full Shield version.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ REINSTALL=ALL EME=0 REINSTALLMODE=vemus /qn"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
REINSTALL="ALL" EME="0" REINSTALLMODE="vemus"
```

- Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.
- **Example Command Line to Install in Deferred Activation Mode**
- The following example installs the client with Deferred Activation in the default location of C:\Program Files\Dell\Dell Data Protection)

```
DDPE_XXbit_setup.exe /s /v"OPTIN=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION"
```

MSI Command:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" OPTIN="1"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
```

- The following example installs the client with Deferred Activation and with default parameters (Encryption client, Encrypt for Sharing, no dialogue, no progress bar, no restart, no Encryption overlay icons, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ OPTIN=1 HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

  MSI Command:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" OPTIN="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  HIDEOVERLAYICONS="1"
  ```

**NOTE:**

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

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

# Install Server Encryption Client

There are two methods available to install Server Encryption. Choose one of the following methods:

- Install Server Encryption Interactively

  **NOTE:**

  Server Encryption can be installed interactively only on computers running server operating systems. Installation on computers running non-server operating systems must be performed by command line, with the SERVERMODE=1 parameter specified.

- Install Server Encryption Using the Command Line

### Virtual User Account

- As part of the installation, a **virtual server user account** is created for the exclusive use of Server Encryption. Password and DPAPI authentication are disabled so that only the virtual server user can access encryption keys on the computer.

### Before You Begin

- The user account performing the installation must be a local or domain user with administrator-level permissions.
- To override the requirement that a domain administrator activate Server Encryption, or to run Server Encryption on non-domain or multi-domain servers, set the ssos.domainadmin.verify property to false in the application.properties file. The file is stored in the following file paths, based on the DDP Server you are using:

  Dell Enterprise Server - *<installation folder>*/Security Server/conf/application.properties

  Virtual Edition - /opt/dell/server/security-server/conf/application.properties
- The server must support port controls.

  Server Port Control System policies affect removable media on protected servers, for example, by controlling access and usage of the server's USB ports by USB devices.USB port policy applies to external USB ports. Internal USB port functionality is not affected by USB port policy. If USB port policy is disabled, the client USB keyboard and mouse will not work and the user will not be able to use the computer unless a Remote Desktop Connection is set up before the policy is applied.
- To successfully activate Server Encryption, the computer must have network connectivity.

- When the Trusted Platform Module (TPM) is available, it is used for sealing the GPK on Dell hardware. If a TPM is not available, Server Encryption uses Microsoft's Data Protection API (DPAPI) to protect the General Purpose Key.

> **NOTE:**
>
> When installing a new operating system on a Dell computer with TPM that is running Server Encryption, clear the TPM in the BIOS. See https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2 for instructions.

**Extract the Child Installer**

- Server Encryption requires only one of the installers in the master installer. To install Server Encryption, you must first extract the Encryption client's child installer, **DDPE_xxbit_setup.exe**, from the master installer. See Extract the Child Installers from the Master Installer.

# Install Server Encryption Interactively

- Use these instructions to install Server Encryption interactively. This installer includes the components you need for software encryption.

1 Locate **DDPE_XXbit_setup.exe** in the C:\extracted\Encryption folder. Copy it to the local computer.

2 If you are installing Server Encryption on a server, double-click the **DDPE_XXbit_setup.exe** file to launch the installer.

> **NOTE:**
>
> When Server Encryption is installed on a computer that is running a server operating system such as Windows Server 2012 R2, the installer installs encryption in Server mode by default.

3 In the Welcome dialog, click **Next.**

4 In the License Agreement screen, read the license agreement, agree to the terms, and click **Next**.

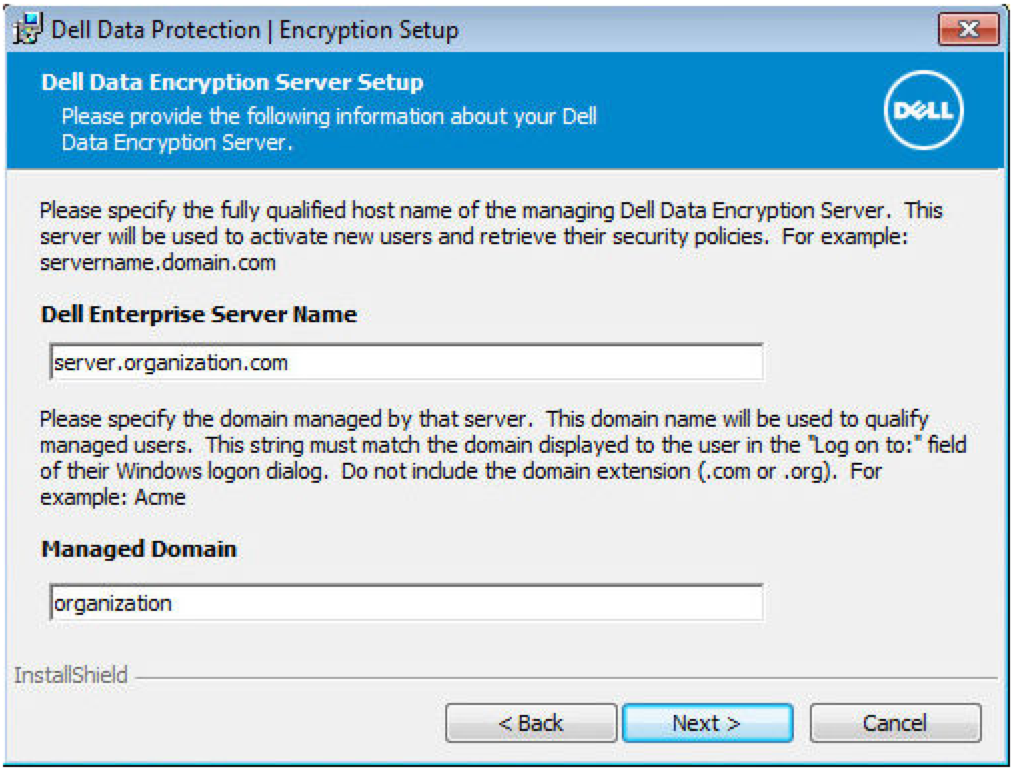
5 Click **Next** to install Server Encryption in the default location.

> **NOTE:**
>
> Dell recommends installing in the default location. Installing in a location other than the default location-whether in a different directory, on the D drive, or on a USB drive-is not recommended.

6 Click **Next** to skip the **Management Type** dialog.

7 In the Dell Enterprise Server Name field, enter the fully qualified host name of the Dell Enterprise Server or Virtual Edition that will manage the target user (example, *server.organization.com)*.

8 Enter the domain name in the **Managed Domain** field (example, organization), and click **Next**.



Dell Data Encryption Server Setup

Please provide the following information about your Dell Data Encryption Server.

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

Dell Enterprise Server Name

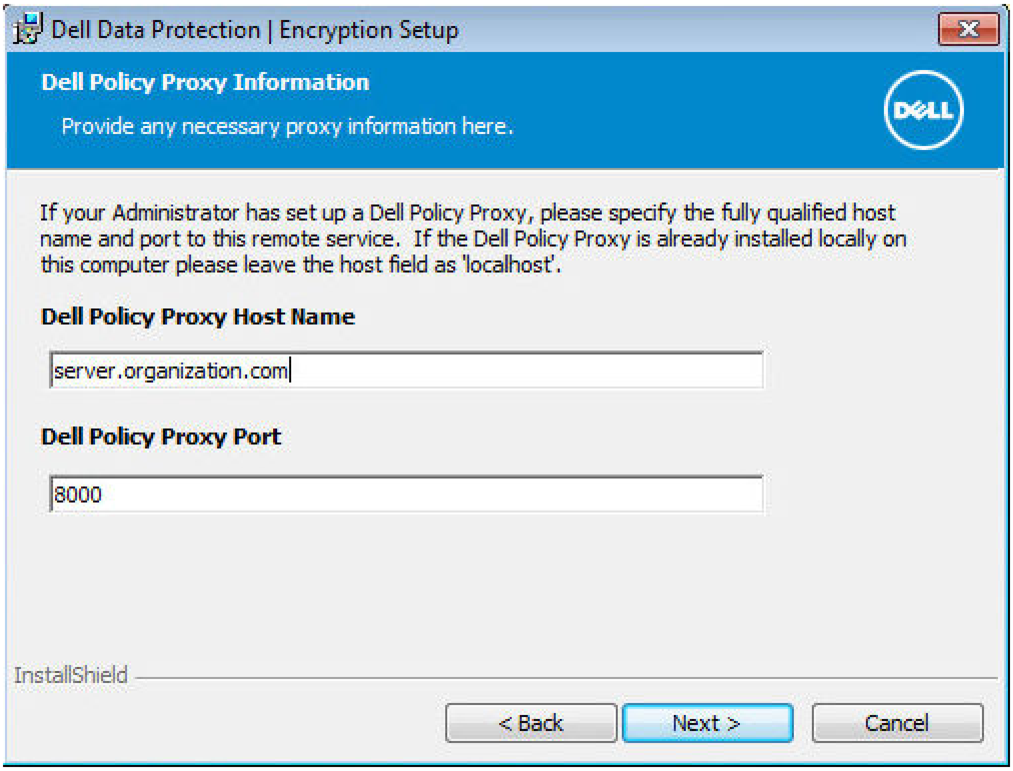
server.organization.com

Please specify the domain managed by that server. This domain name will be used to qualify managed users. This string must match the domain displayed to the user in the "Log on to:" field of their Windows logon dialog. Do not include the domain extension (.com or .org). For example: Acme

Managed Domain

organization

9 Click **Next** to skip the auto-populated **Dell Policy Proxy Information** dialog.



Dell Policy Proxy Information

Provide any necessary proxy information here.

If your Administrator has set up a Dell Policy Proxy, please specify the fully qualified host name and port to this remote service. If the Dell Policy Proxy is already installed locally on this computer please leave the host field as 'localhost'.

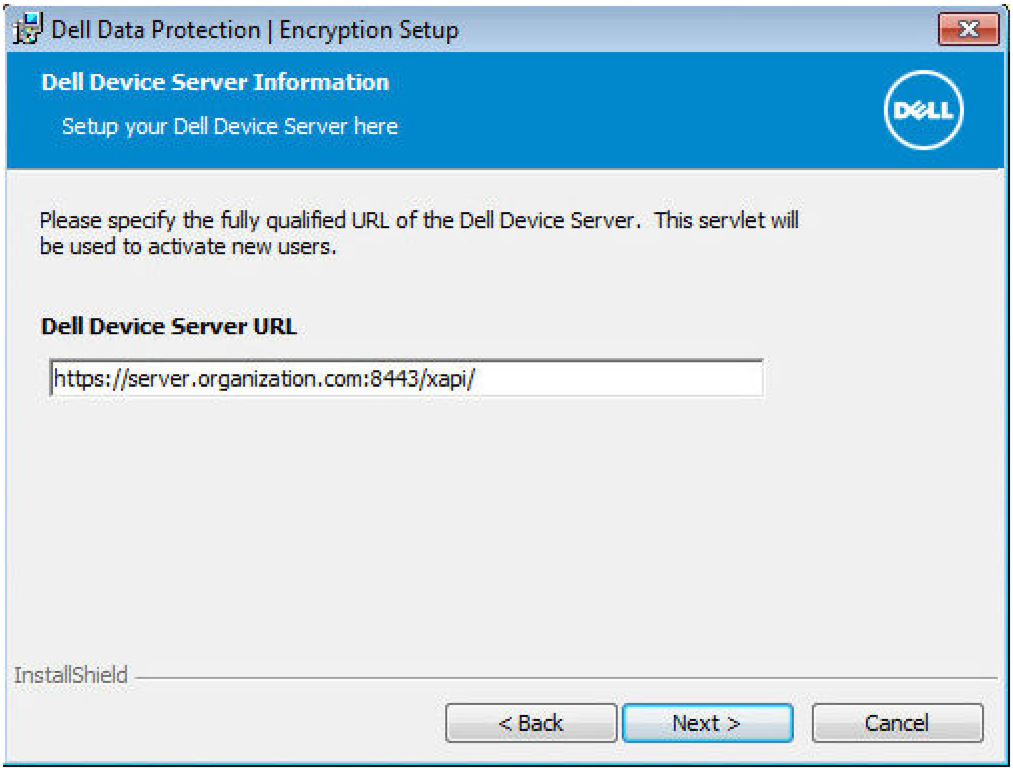
Dell Policy Proxy Host Name

server.organization.com

Dell Policy Proxy Port

8000

10 Click **Next** to skip the auto-populated **Dell Device Server Information** dialog.



Dell Data Protection | Encryption Setup

Dell Device Server Information

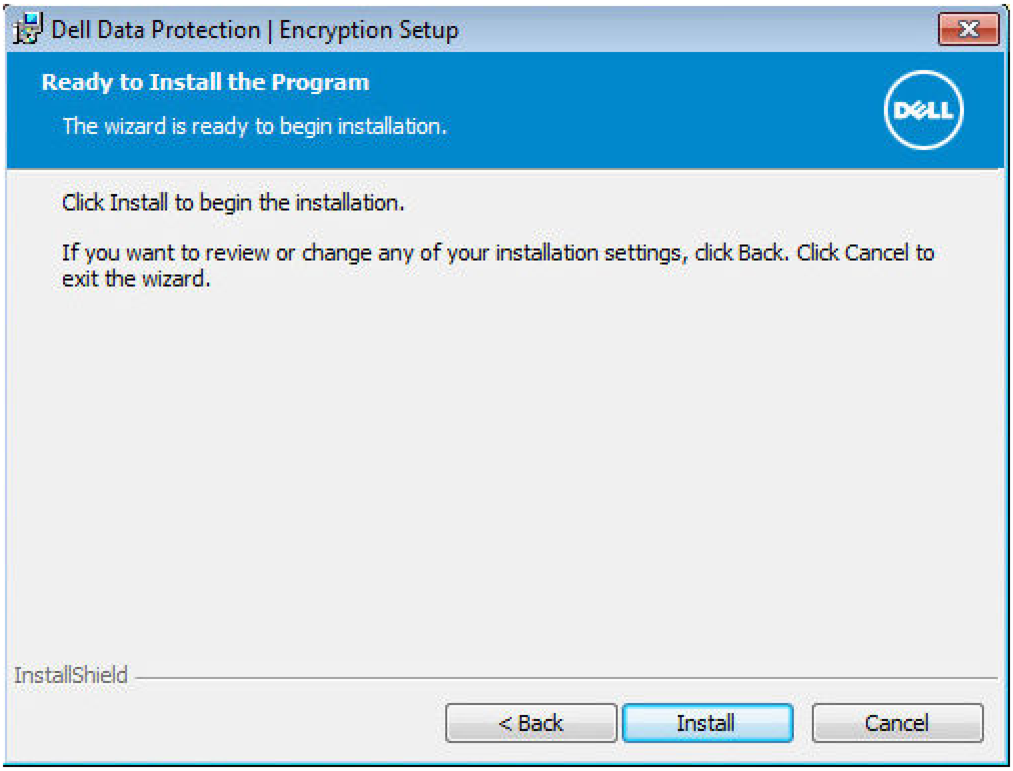
Setup your Dell Device Server here

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

Dell Device Server URL

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

11 Click **Install** to begin the installation.



Dell Data Protection | Encryption Setup

Ready to Install the Program

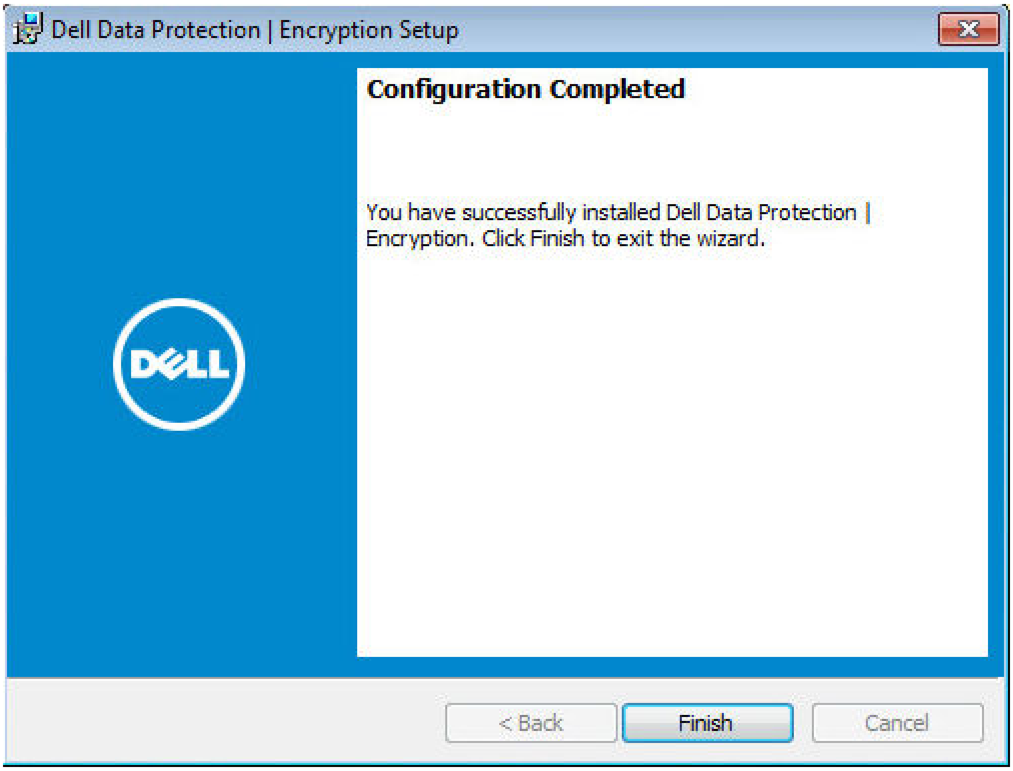
The wizard is ready to begin installation.

Click Install to begin the installation.

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

Installation may take several minutes.

12 In the **Configuration Completed** dialog, click Finish.



Configuration Completed

You have successfully installed Dell Data Protection | Encryption. Click Finish to exit the wizard.

Installation is complete.

ⓘ **NOTE:**

The log file for the installation is located in the account's %temp% directory, located at C:\Users\<user name>\AppData \Local\Temp. To locate the installer's log file, look for a file name that begins with MSI and ends with a .log extension. The file should have a date/time stamp matching the time when you ran the installer.

ⓘ **NOTE:**

As part of the installation, a **virtual server user account** is created for the exclusive use of Server Encryption. Password and DPAPI authentication are disabled so that only the virtual server user can access encryption keys on the computer.

13 Restart the computer.

ⓘ **IMPORTANT: Choose Snooze Reboot only if you need time to save your work and close any open applications.**

# Install Server Encryption Using the Command Line

**Server Encryption Client - locate the installer at C:\extracted\Encryption**

- Use **DDPE_xxbit_setup.exe** to install or upgrade using a scripted installation, using batch files, or any other push technology available to your organization.

**Switches**

The following table details the switches available for the installation.

| Switch | Meaning |
|---|---|
| /v | Pass variables to the .msi inside the DDPE_XXbit_setup.exe |
| /a | Administrative installation |
| /s | Silent mode |

### Parameters

The following table details the parameters available for the installation.

| Component | Log File | Command Line Parameters |
|---|---|---|
| All | /l*v [fullpath][filename].log * | SERVERHOSTNAME=<Management Server Name><br>SERVERMODE=1<br>POLICYPROXYHOSTNAME=<RGK Name><br>MANAGEDDOMAIN=<My Domain><br>DEVICESERVERURL=<Activation Server Name><br>GKPORT=<New GK Port><br>MACHINEID=<Machine Name><br>RECOVERYID=<Recovery ID><br>REBOOT=ReallySuppress<br>HIDEOVERLAYICONS=1<br>HIDESYSTRAYICON=1<br>EME=1 |

**NOTE:**
Although the reboot can be suppressed, an eventual reboot is required. Encryption cannot begin until the computer has rebooted.

### Options

The following table details the display options that can be specified at the end of the argument passed to the /v switch.

| 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 |

| Option | Meaning |
|---|---|
| /qn | No user interface |

ⓘ **NOTE:**

Do not use both **/q** and **/qn** in the same command line. Only use **!** and - after **/qb**.

- The command line parameter, SERVERMODE=1, is honored only during new installations. The parameter is ignored for uninstallations.
- Installing in a location other than the default location, whether in a different directory, on a drive other than C:, or on a USB drive is not recommended. Dell recommends installing in the default location.
- Enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.
- The Dell Activation Server URL (DEVICESERVERURL) is case sensitive.

**Example Command Line Installation**

- The following example installs the Server Encryption client with default parameters (Server Encryption client, silent installation, Encrypt for Sharing, no dialogue, no progress bar, automatic restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/qn"
  ```

  MSI Command:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- The following example installs the Server Encryption client with a log file and default parameters (Server Encryption client, silent installation, Encrypt for Sharing, no dialogue, no progress bar, no restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection\Encryption) and specifies a custom log file name ending with a number (DDP_ssos-090.log) that should be incremented if the command line is run more than once on the same server.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /norestart/qn"
  ```

  MSI Command:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/" /l*v
  DDP_ssos-090.log /norestart/qn"
  ```

  To specify a log location other than the default location where the executable is located, provide the complete path in the command. For example, /l*v C:\Logs\DDP_ssos-090.log will create install logs in a C:\Logs folder.

**Restart the computer**

After installation, restart the computer. The computer must be restarted as soon as possible.

ⓘ **IMPORTANT:**

Choose **Snooze Reboot** only if you need time to save your work and close any open applications.

# Activate Server Encryption

- The server must be connected to your organization's network.

- Ensure that the computer name of the server is the endpoint name you want to display in the Remote Management Console.
- A live, interactive user with domain administrator credentials must log on to the server at least once for the purpose of the initial activation. The logged on user can be of any type - domain or non-domain, remote-desktop-connected or interactive user at the server, but activation requires domain administrator credentials.
- Following the restart after installation, the Activation dialog displays. The administrator must enter domain administrator credentials with a user name in User Principal Name (UPN) format. The Server Encryption client does not activate automatically.
- During initial activation, a virtual server user account is created. After initial activation, the computer is restarted so that device activation can begin.
- During the Authentication and Device Activation phase, the computer is assigned a unique Machine ID, encryption keys are created and bundled, and a relationship is established between the encryption key bundle and the virtual server user. The encryption key bundle associates the encryption keys and policies with the new virtual server user to create an unbreakable relationship between the encrypted data, the specific computer, and the virtual server user. After device activation, the virtual server user appears in the Remote Management Console as SERVER-USER@<*fully qualified server name*>. For more information about activation, see Activation on a Server Operating System.

> **NOTE:**
>
> If you rename the server after activation, its display name will not change in the Remote Management Console. However, if the Server Encryption client activates again after the server name is changed, the new server name would appear in the Remote Management Console.

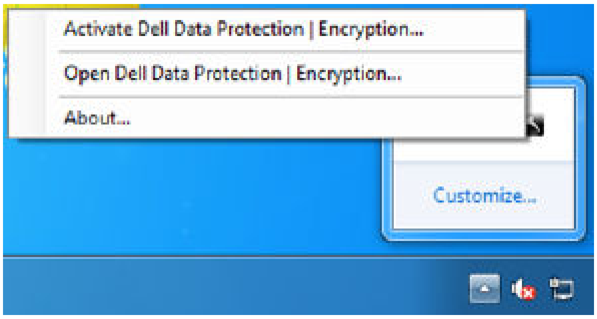
An Activation dialog displays once after each restart to prompt the user to activate Server Encryption. If activation is not completed, follow these steps:

1 Log on to the server either at the server or through Remote Desktop Connection.

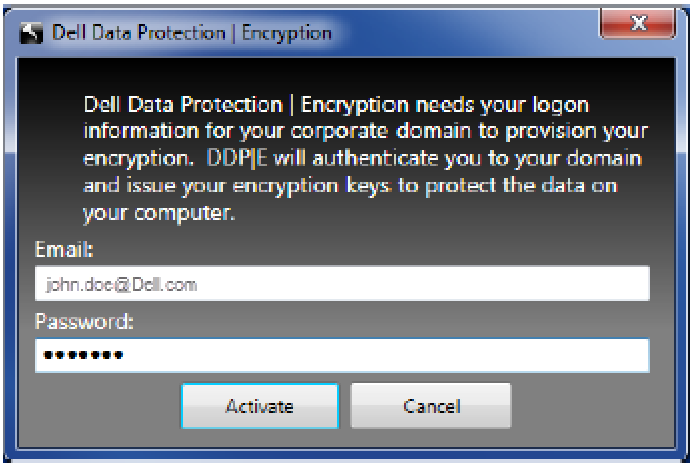
2 Right-click the Encryption icon in the system tray, and click **About**.

3 Verify that Encryption is running in Server mode.

4 Select **Activate Encryption** from the menu.


Activate Dell Data Protection | Encryption...
Open Dell Data Protection | Encryption...
About...
Customize...

5 Enter the username of a Domain Administrator in UPN format and password and click **Activate**. This is the same Activation dialog that appears each time an unactivated system is restarted.



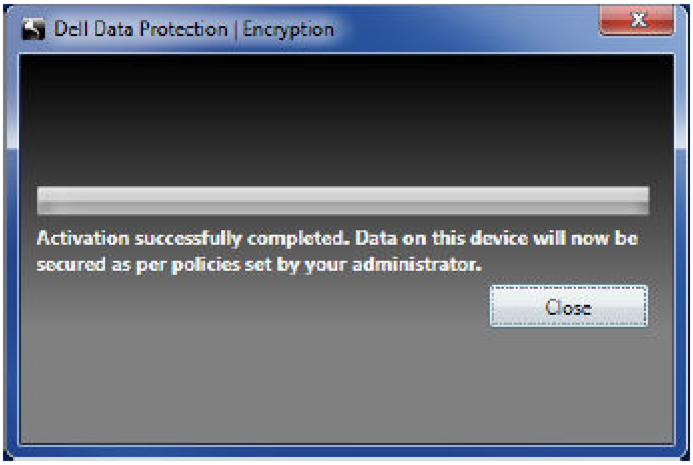
Dell Data Protection | Encryption needs your logon information for your corporate domain to provision your encryption. DDP|E will authenticate you to your domain and issue your encryption keys to protect the data on your computer.

Email:
john.doe@Dell.com

Password:
•••••••

The DDP Server issues an encryption key for the Machine ID, creates the **virtual server user account**, creates an encryption key for the user account, bundles the encryption keys, and creates the relationship between the encryption bundle and the virtual server user account.

6 Click **Close**.



Dell Data Protection | Encryption

Activation successfully completed. Data on this device will now be secured as per policies set by your administrator.

After activation, encryption begins.

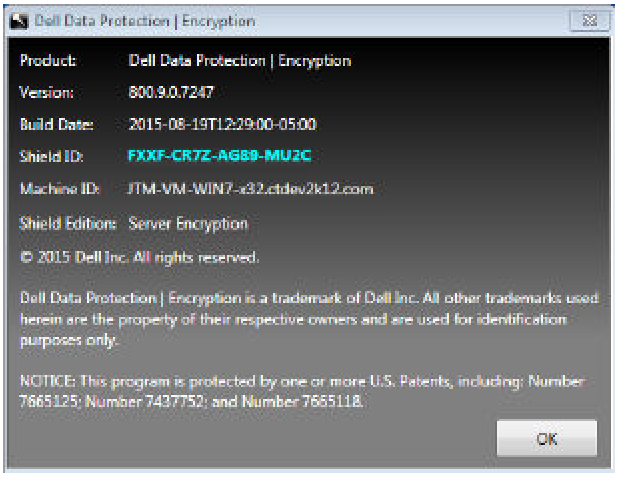
7 After the encryption sweep has finished, restart the computer to process any files that were previously in use. This is an important step for security purposes.

> **NOTE:**
> If the *Secure Windows Credentials* policy is set to True, Server Encryption encrypts the \Windows\system32\config files, which includes Windows credentials. The files in \Windows\system32\config are encrypted even if the *SDE Encryption Enabled* policy is **Not Selected**. By default, the *Secure Windows Credentials* policy is **Selected**.

> **NOTE:**
> After restarting the computer, authentication to the Common key material *always* requires the protected server's Machine key. The DDP Server returns an unlock key to access the encryption keys and policies in the vault. (The keys and policies are for the server, not for the user). Without the server's Machine key, the Common file encryption key cannot be unlocked, and the computer cannot receive policy updates.

### Confirm Activation

From the local console, open the **About** dialog to confirm that Server Encryption is installed, authenticated, and in Server mode. If the Shield ID is **red**, encryption has not yet been activated.



Dell Data Protection | Encryption

| | |
|---|---|
| Product: | Dell Data Protection \| Encryption |
| Version: | 800.9.0.7247 |
| Build Date: | 2015-08-19T12:29:00-05:00 |
| Shield ID: | FXXF-CR7Z-AG89-MU2C |
| Machine ID: | JTM-VM-WIN7-x32.ctdev2k12.com |
| Shield Edition: | Server Encryption |

© 2015 Dell Inc. All rights reserved.

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

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

## The Virtual Server User

- In the Remote Management Console, a protected server can be found under its machine name. In addition, each protected server has its own virtual server user account. Each account has a unique static username and unique machine name.
- The virtual server user account is only used by Server Encryption and is otherwise transparent to the operation of the protected server. The virtual server user is associated with the encryption key bundle and the policy proxy.
- After activation, the virtual server user account is the user account that is activated and associated with the server.
- After the virtual server user account is activated, all server logon/logoff notifications are ignored. Instead, during startup, the computer automatically authenticates with the virtual server user, and then downloads the Machine key from the Dell Data Protection Server.

# Install SED Management and Advanced Authentication Clients

- The SED client is required for Advanced Authentication in v8.x.
- Review SED 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 SSL/TLS trust validation.
- Users log in to the PBA using their Windows credentials.
- The SED and Advanced Authentication client installers can be located at:
  - **From support.dell.com** - If needed, Obtain the Software from support.dell.com and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Security Tools** and **C:\extracted\Security Tools\Authentication**.
  - **From Your Dell FTP Account** - Locate the installation bundle at DDP-Enterprise-Edition-8.x.x.xxx.zip and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Security Tools** and **C:\extracted\Security Tools\Authentication**.

## Command Line Installation

- The following table details the parameters available for the installation.

| Parameters |
|---|
| CM_EDITION=1 <remote management> |
| INSTALLDIR=<change the installation destination> |
| SERVERHOST=<securityserver.organization.com> |
| SERVERPORT=8888 |
| SECURITYSERVERHOST=<securityserver.organization.com> |
| SECURITYSERVERPORT=8443 |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

For a list of basic .msi switches and display options that can be used in command lines, refer to Install Using the Child Installers.

**Example Command Line**

**\Security Tools**

- The following example installs remotely managed SED (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

*Then*:

**\Security Tools\Authentication**

- The following example installs Advanced Authentication (silent installation, no reboot)

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

# Install BitLocker Manager Client

- Review BitLocker Manager 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 SSL/TLS trust validation.
- The BtLocker Manager client installers can be located at:
  - **From support.dell.com** - If needed, Obtain the Software from support.dell.com and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Security Tools**.
  - **From Your Dell FTP Account** - Locate the installation bundle at DDP-Enterprise-Edition-8.x.x.xxx.zip and then Extract the Child Installers from the Master Installer. After extraction, locate the file at **C:\extracted\Security Tools**.

# Command Line Installation

- The following table details the parameters available for the installation.

| Parameters |
|---|
| CM_EDITION=1 <remote management> |
| INSTALLDIR=<change the installation destination> |
| SERVERHOST=<securityserver.organization.com> |
| SERVERPORT=8888 |
| SECURITYSERVERHOST=<securityserver.organization.com> |
| SECURITYSERVERPORT=8443 |
| FEATURE=BLM <install BitLocker Manager only> |
| FEATURE=BLM,SED <install BitLocker Manager with SED> |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

For a list of basic .msi switches and display options that can be used in command lines, refer to Install Using the Child Installers.

**Example Command Line**

- The following example installs BitLocker Manager only (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

- The following example installs BitLocker Manager with SED (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM,SED /
norestart /qn"
```

# Uninstall Using the Child Installers

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

  If you decide to add separate a log file when you run the installer, ensure that the log file has a unique name, as child installer log files do not append. The standard .msi command can be used be create a log file by using /l C:\<any directory>\<any log file name>.log. Dell does not recommend using "/l*v" (verbose logging) in a command line uninstallation, as the username/password is recorded in the log file.
- All child installers use the same basic .msi switches and display options, except where noted, for command line uninstallations. The switches must be specified first. The /v switch is required and takes an argument. Other parameters go inside an argument that is passed to the /v switch.

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

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

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

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

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

# Uninstall Encryption and Server Encryption Client

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

## Process

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

## Command Line Uninstallation

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

| Parameter | Selection |
|---|---|
| CMG_DECRYPT | Property for selecting the type of Encryption Removal Agent installation:<br>3 - Use LSARecovery bundle<br>2 - Use previously downloaded forensics key material<br>1 - Download keys from the Dell Server |

| Parameter | Selection |
|---|---|
| | 0 - Do not install Encryption Removal Agent |
| CMGSILENTMODE | Property for silent uninstallation:<br>1 - Silent<br>0 - Not Silent |
| **Required Properties** | |
| DA_SERVER | FQHN for the EE Server hosting the negotiate session. |
| DA_PORT | Port on the EE Server for request (default is 8050). |
| SVCPN | Username in UPN format that the Key Server Service is logged on as on the EE Server. |
| DA_RUNAS | Username in SAM compatible format under whose context the key fetch request will be made. This user must be in the Key Server list in the EE Server. |
| DA_RUNASPWD | Password for the runas user. |
| FORENSIC_ADMIN | The Forensic Administrator account on the Dell Server, which can be used for forensic requests for uninstalls or keys. |
| FORENSIC_ADMIN_PWD | The password for the Forensic Administrator account. |
| **Optional Properties** | |
| SVCLOGONUN | Username in UPN format for Encryption Removal Agent Service log on as parameter. |
| SVCLOGONPWD | Password for log on as user. |

- The following example silently uninstalls the Encryption client and downloads the encryption keys from the EE Server.

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

  MSI Command:

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

  Reboot the computer when finished.

- The following example silently uninstalls the Encryption client and downloads the encryptions keys using a Forensic Administrator account.

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

  MSI Command:

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

  Reboot the computer when finished.

ⓘ **IMPORTANT:**

Dell recommends the following actions when using a Forensic Administrator password on the command line:

1 Create a Forensic Administrator account in the Remote Management Console for the purpose of performing the silent uninstallation.

2 Use a temporary password for that account that is unique to that account and time period.

3 After the silent uninstallation has been completed, remove the temporary account from the list of administrators or change its password.

ⓘ **NOTE:**

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

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

## Uninstall External Media Edition

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

**Command Line Uninstallation**

Run a command line similar to the following:

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

Reboot the computer when finished.

# Uninstall SED and Advanced Authentication Clients

- Network connection to the EE Server/VE Server is required for PBA deactivation.

## Process

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

## Deactivate the PBA

1 As a Dell administrator, log in to the Remote Management Console.

2 In the left pane, click **Protect & Manage** > **Endpoints**.

3 Select the appropriate Endpoint Type.

4 Select Show >*Visible*, *Hidden*, or *All*.

5 If you know the Hostname of the computer, enter it in the Hostname field (wildcards are supported). You may leave the field blank to display all computers. Click **Search**.

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

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

6 Select the **Details** icon of the desired computer.

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

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

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

10 Click **Save**.

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

12 Click **Apply Changes**.

Wait for the policy to propagate from the EE Server/VE Server to the computer targeted for deactivation.

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

# Uninstall SED Client and Advanced Authentication Clients

**Command Line Uninstallation**

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

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

Shut down and restart the computer when finished.

Then:

- The following example silently uninstalls the Advanced Authentication client.

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

Shut down and restart the computer when finished.

# Uninstall BitLocker Manager Client

## Command Line Uninstallation

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

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

Reboot the computer when finished.

# Commonly Used Scenarios

- To install each client individually, the child executable files must first be extracted from the master installer, as shown in Extract the Child Installers from the Master Installer.
- The SED client is required for Advanced Authentication in v8.x, which is why it is part of the command line in the following examples.
- 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.
- Use these installers to install the clients using a scripted installation, batch files, or any other push technology available to your organization.
- The reboot has been suppressed in the command line examples. However, an eventual reboot is required. Encryption cannot begin until the computer has rebooted.
- 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 be create a log file by using /l*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 |

- Instruct users to see the following document and help files for application assistance:
  - See the *Dell Encrypt Help* to learn how to use the feature of the Encryption client. Access the help from <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help.
  - See the *EMS Help* to learn how the features of External Media Shield. Access the help from <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS

- See the *Security Tools Help* to learn how to use the features of Advanced Authentication. Access the help from <Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help.

# Encryption Client and Advanced Authentication

- The following example installs remotely managed SED (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

  Then:

- The following example installs Advanced Authentication (silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection\Authentication).

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

- The following example installs the Encryption client with default parameters (Encryption client and Encrypt for Sharing, no dialogue, no progress bar, no restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.

# SED Client (including Advanced Authentication) and Encryption Client

- The following example installs drivers for Trusted Software Stack (TSS) for the TPM and Microsoft hotfixes at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

  These drivers must be installed when installing the Encryption client.

  ```
  setup.exe /S /z"\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
  ```

  Then:

- The following example installs remotely managed SED (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

  Then:

- The following example installs Advanced Authentication (silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection\Authentication).

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

  Then:

- The following example installs the client with default parameters (Encryption client and Encrypt for Sharing, no dialogue, no progress bar, no restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ /norestart /qn"
  ```

Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.

# SED Client (including Advanced Authentication) and External Media Shield

- The following example installs remotely managed SED (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

  Then:

- The following example installs Advanced Authentication (silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection\Authentication).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

  Then:

- The following example installs EMS only (silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

  Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.

# BitLocker Manager and External Media Shield

- The following example installs BitLocker Manager (silent installation, no reboot, no entry in the Control Panel Programs list, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

  Then:

- The following example installs EMS only (silent installation, no reboot, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

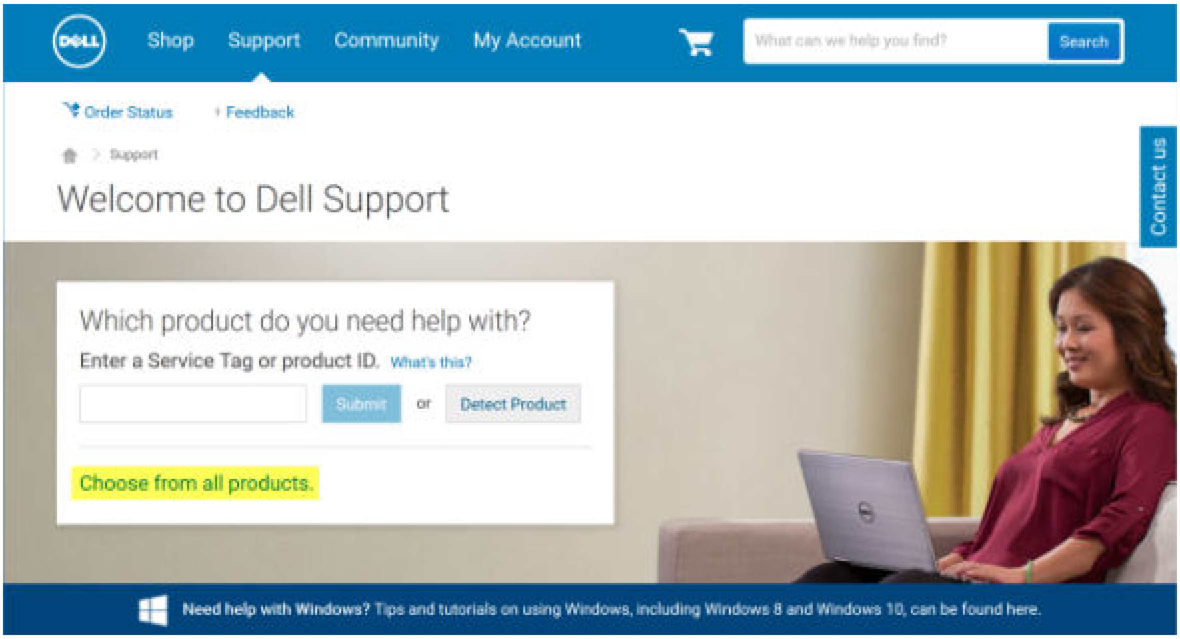
Replace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (without the trailing forward slash) if your EE Server is pre-v7.7.

# Download the Software

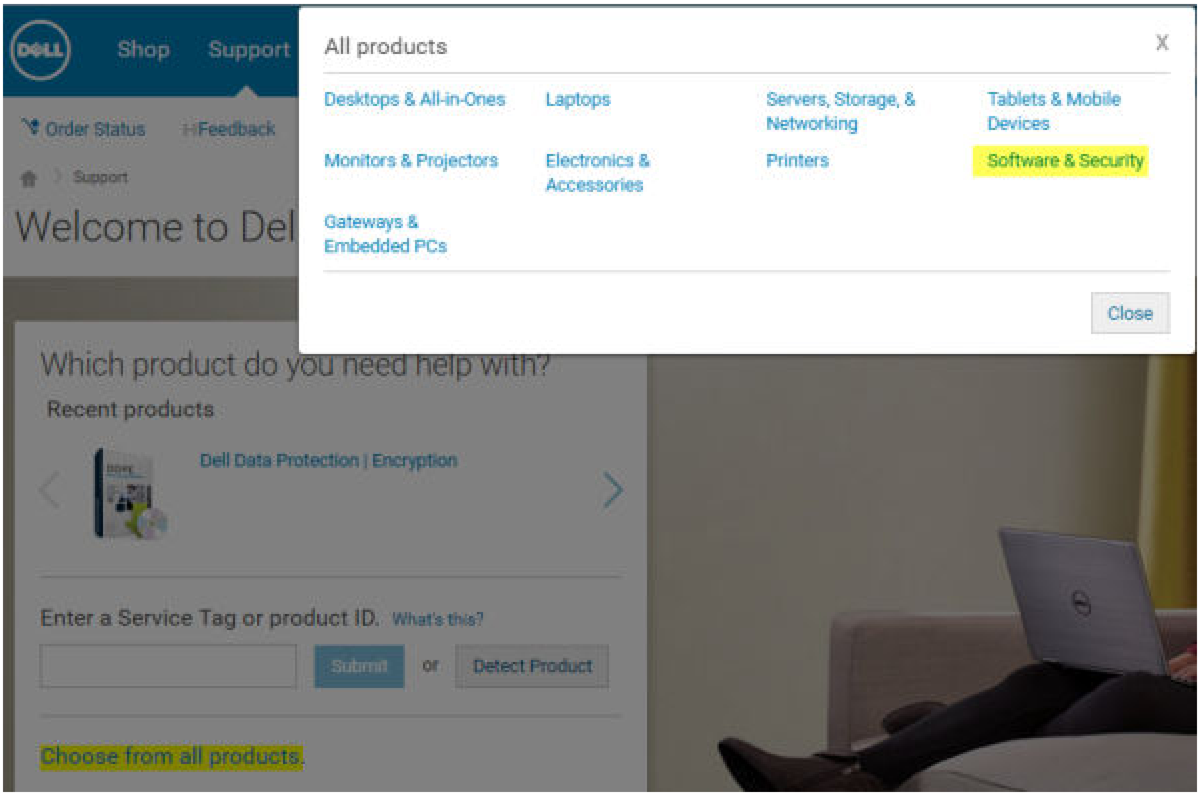
This section details obtaining the software from dell.com/support. If you already have the software, you can skip this section.

Go to dell.com/support to begin.

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

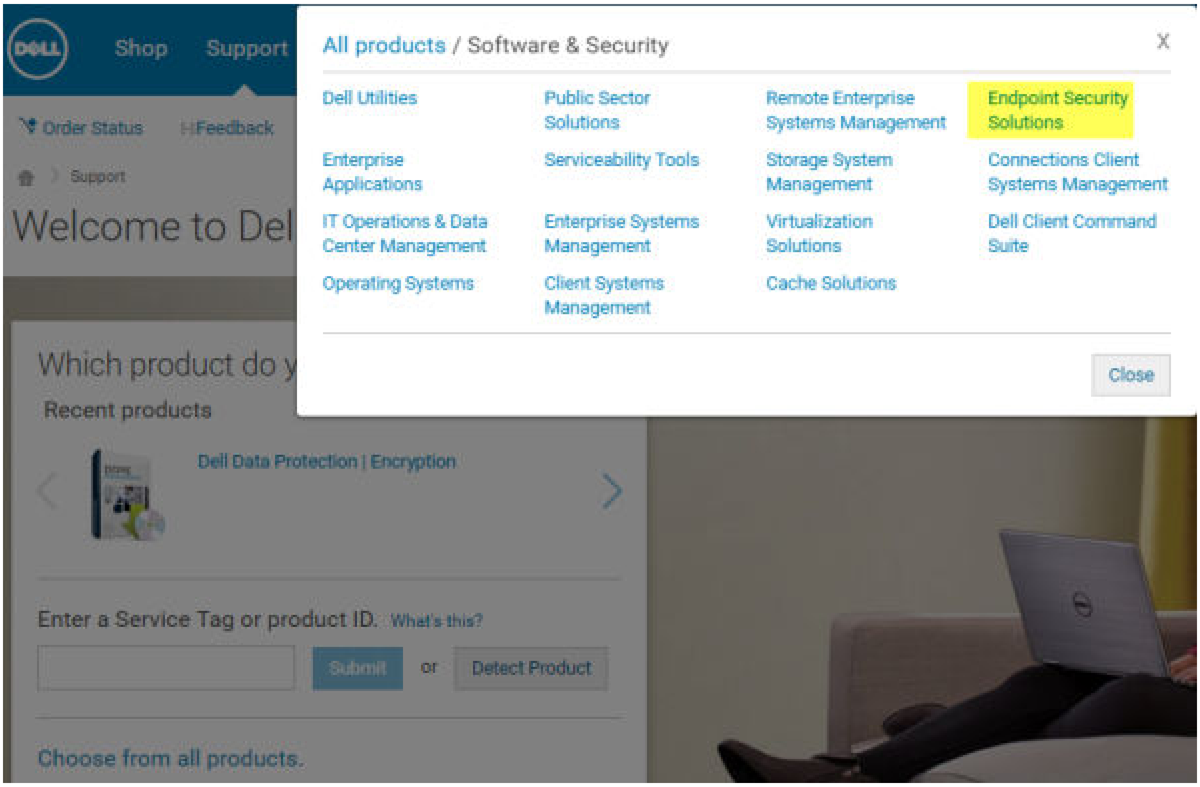

Shop
Support
Community
My Account
What can we help you find?
Search
Order Status
Feedback
Support
Welcome to Dell Support
Contact us
Which product do you need help with?
Enter a Service Tag or product ID. What's this?
Submit
or
Detect Product
Choose from all products.
Need help with Windows? Tips and tutorials on using Windows, including Windows 8 and Windows 10, can be found here.

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



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

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


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

4 Select the Dell Data Protection product.

Examples:

**Dell Encryption**

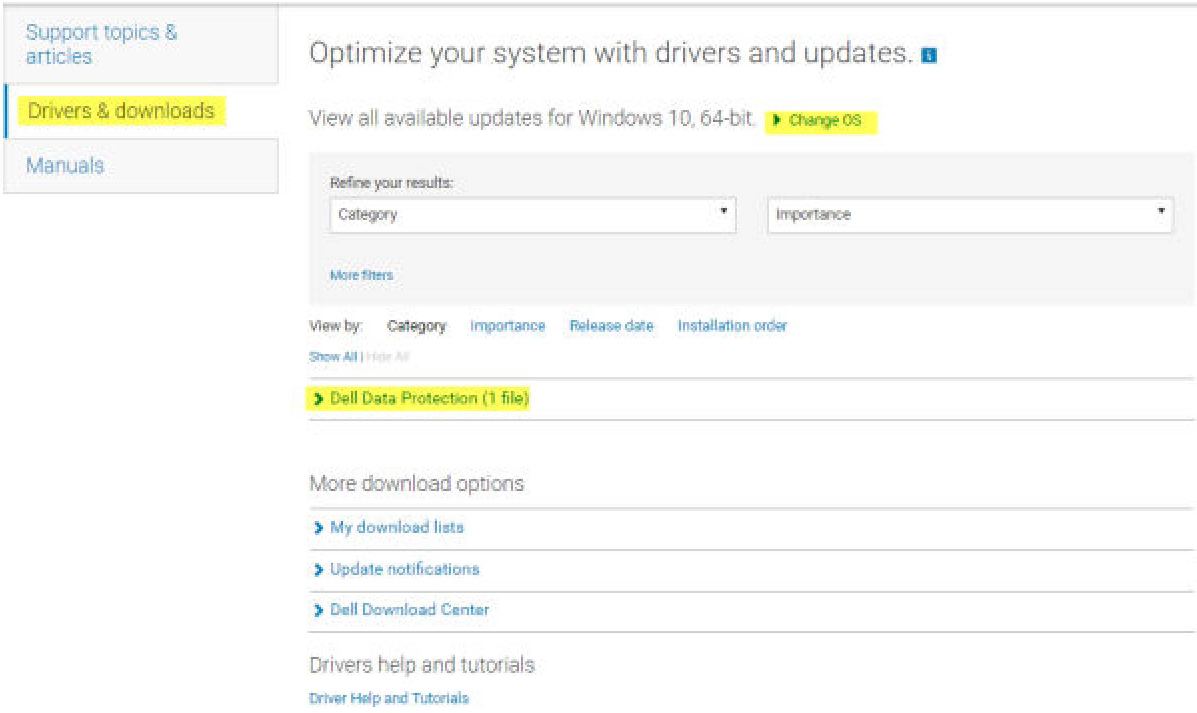
**Dell Endpoint Security Suite**

**Dell Endpoint Security Suite Enterprise**

5 Select **Drivers & downloads**.

6 Select the desired client operating system type.

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



Support topics & articles

Drivers & downloads

Manuals

Optimize your system with drivers and updates.

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

Refine your results:

Category ▾

Importance ▾

More filters

View by: Category Importance Release date Installation order

Show All | Hide All

› Dell Data Protection (1 file)

More download options

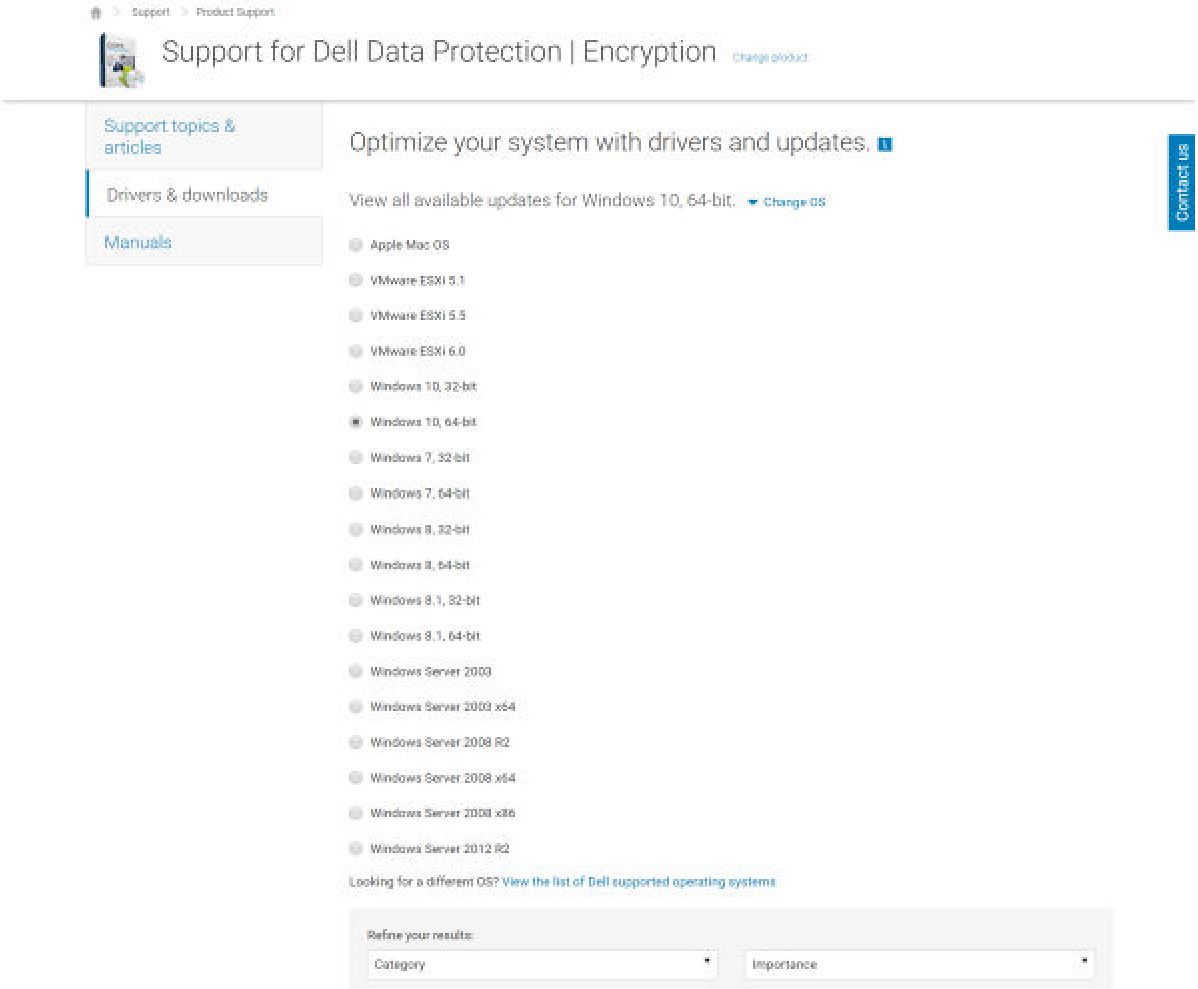
› My download lists

› Update notifications

› Dell Download Center

Drivers help and tutorials

Driver Help and Tutorials



Support > Product Support

Support for Dell Data Protection | Encryption Change product

Support topics & articles

Drivers & downloads

Manuals

Optimize your system with drivers and updates.

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

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

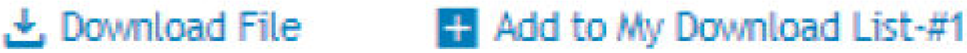
Looking for a different OS? View the list of Dell supported operating systems

Refine your results:

Category

Importance

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



10

# Pre-Installation Configuration for One-time Password, SED UEFI, and BitLocker

## Initialize the TPM

- You must be a member of the local Administrators group, or equivalent.
- The computer must be equipped with a compatible BIOS and a TPM.

This task is required if using One-time Password (OTP).

- Follow the instructions located at http://technet.microsoft.com/en-us/library/cc753140.aspx.

## Pre-Installation Configuration for UEFI Computers

### Enable Network Connectivity During UEFI Preboot Authentication

In order for preboot authentication to succeed on a computer with UEFI firmware, the PBA must have network connectivity. By default, computers with UEFI firmware do not have network connectivity until the operating system is loaded, which occurs after PBA mode.

The following procedure enables network connectivity during PBA for UEFI-enabled computers. Because the configuration steps vary from one UEFI computer model to the next, the following procedure is only an example.

1 Boot into the UEFI firmware configuration.

2 Press F2 continuously during boot until you see a message in the upper right screen similar to "preparing one-time boot menu."

3 Enter the BIOS administrator password, if prompted.

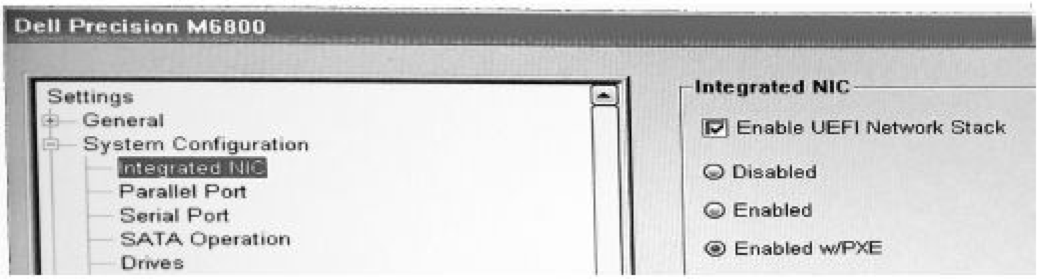
> **NOTE:**
> Typically, you will not see this prompt if this is a new computer since the BIOS password has not yet been configured.

4 Select **System Configuration**.

5 Select **Integrated NIC**.

6 Select the **Enable UEFI Network Stack** check box.

7 Select either **Enabled** or **Enabled w/PXE**.



Dell Precision M6800

Integrated NIC

☑ Enable UEFI Network Stack

○ Disabled

○ Enabled

● Enabled w/PXE

8 Select **Apply**

> **NOTE:**
> Computers *without* UEFI firmware do not require configuration.

# Disable Legacy Option ROMs

Ensure that the **Enable Legacy Option ROMs** setting is disabled in the BIOS.

1 Restart the computer.

2 As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.

3 Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.

4 Select **Settings** > **General** > **Advanced Boot Options**.

5 Clear the **Enable Legacy Option ROMs** check box and click **Apply**.

# Pre-Installation Configuration to Set Up a BitLocker PBA Partition

- You must create the PBA partition **before** installing BitLocker Manager.
- Turn on and activate the TPM **before** installing BitLocker Manager. BitLocker Manager will take ownership of the TPM (a reboot will not be required). However, if the TPM's ownership already exists, BitLocker Manager will begin the encryption setup process. The point is that the TPM must be "owned".
- You may need to partition the disk manually. See Microsoft's description of the BitLocker Drive Preparation Tool for further information.
- Use the BdeHdCfg.exe command to create the PBA partition. The default parameter indicates that the command line tool will follow the same process as the BitLocker Setup Wizard.

```
BdeHdCfg -target default
```

> **TIP:**
> For more options available for the BdeHdCfg command, see Microsoft's BdeHdCfg.exe Parameter Reference.

11

# Set GPO on Domain Controller to Enable Entitlements

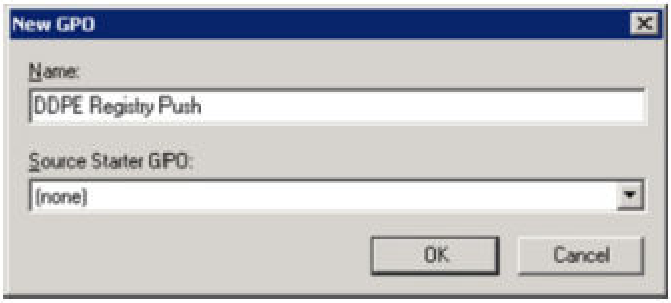
- If your clients will be entitled from Dell Digital Delivery (DDD), follow these instructions to set the GPO on the domain controller to enable entitlements (this may not be the same server running the EE Server/VE Server).
- The workstation must be a member of the OU where the GPO is applied.

> **NOTE:**
> Ensure that outbound port 443 is available to communicate with the EE Server/VE Server. If port 443 is blocked (for any reason), the entitlement functionality will not work.

1 On the Domain Controller to manage the clients, click **Start** > **Administrative Tools** > **Group Policy Management**.

2 Right-click the OU where the policy should be applied and select **Create a GPO in this domain**, and **Link it here...**.

3 Enter a name for the new GPO, select (none) for Source Starter GPO, and click **OK**.

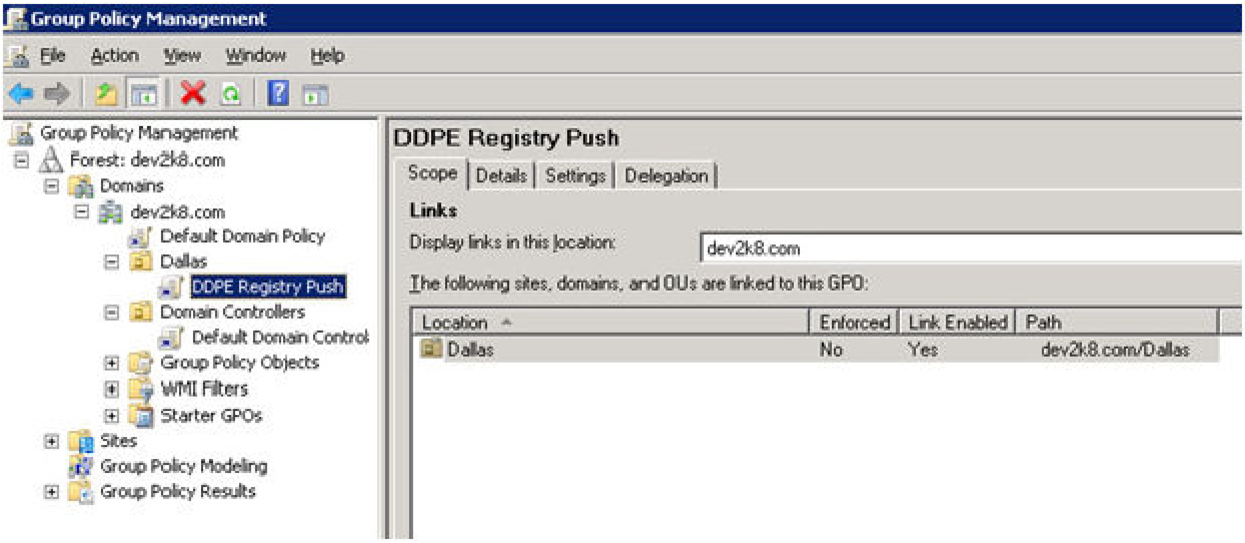


New GPO

Name: DDPE Registry Push

Source Starter GPO: (none)

4 Right-click the GPO that was created and select **Edit**.



DDPE Registry Push

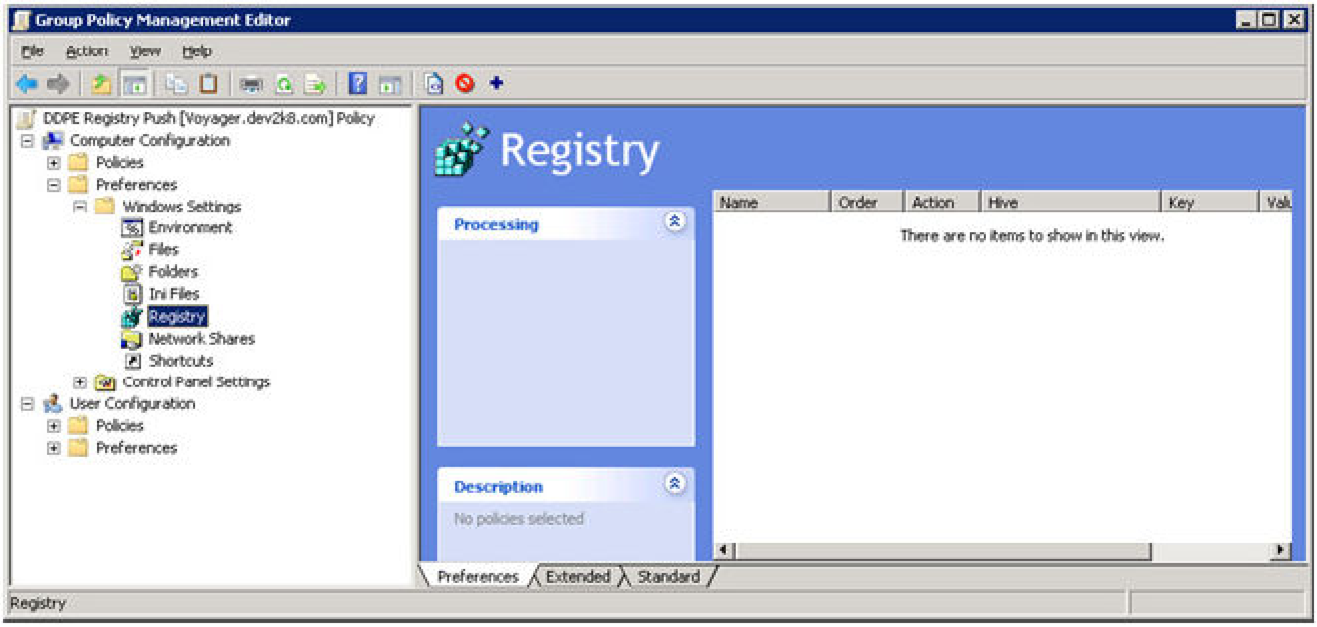
Links

Display links in this location: dev2k8.com

The following sites, domains, and OUs are linked to this GPO:

| Location | Enforced | Link Enabled | Path |
|---|---|---|---|
| Dallas | No | Yes | dev2k8.com/Dallas |

5 The Group Policy Management Editor loads. Access **Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**.



6 Right-click the Registry and select **New** > **Registry Item**. Complete the following.

Action: Create

Hive: HKEY_LOCAL_MACHINE

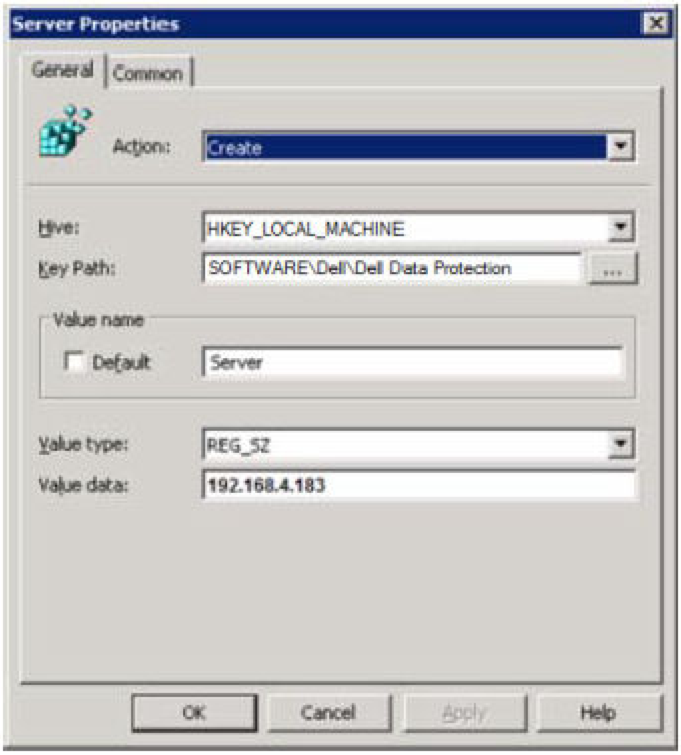
Key Path: SOFTWARE\Dell\Dell Data Protection

Value name: Server

Value type: REG_SZ

Value data: <IP address of the EE Server/VE Server>

7 Click **OK**.



Server Properties

Hive: HKEY_LOCAL_MACHINE

Key Path: SOFTWARE\Dell\Dell Data Protection

Value name

□ Default Server

Value type: REG_SZ

Value data: 192.168.4.183

8 Log out and then back into the workstation, or run **gpupdate /force** to apply the group policy.

# Extract the Child Installers from the Master Installer

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

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

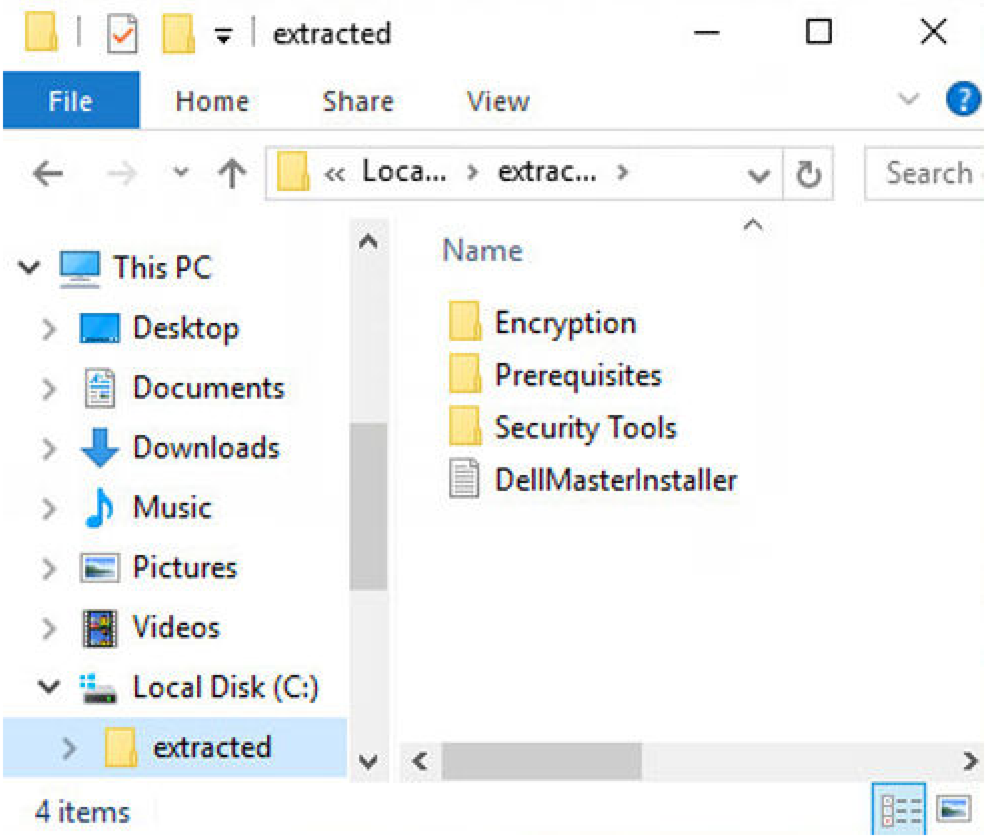
2 Open a command prompt in the same location as the **DDPSetup.exe** file and enter:

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

The extraction path cannot exceed 63 characters.

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\.



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

- This section explains how to configure components for use with Kerberos Authentication/Authorization when using an EE Server. The VE Server does not use the Key Server.

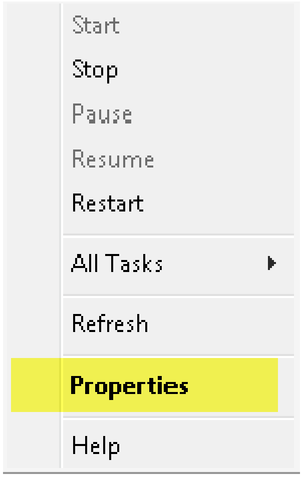
  The Key Server is a Service that listens for clients to connect on a socket. Once a client connects, a secure connection is negotiated, authenticated, and encrypted using Kerberos APIs (if a secure connection cannot be negotiated, the client is disconnected).

  The Key Server then checks with the Security Server (formerly the Device Server) to see if the user running the client is allowed to access keys. This access is granted on the Remote Management Console via individual domains.
- If Kerberos Authentication/Authorization is to be used, then the server that contains the Key Server component will need to be part of the affected domain.
- Because the VE Server does not use the Key Server, typical uninstallation is affected. When an Encryption client that is activated against a VE Server is uninstalled, standard forensic key retrieval through the Security Server is used, instead of the Key Server's Kerberos method. See Command Line Uninstallation for more information.

## Services Panel - Add Domain Account User

1 On the EE Server, navigate to the Services panel (Start > Run... > services.msc > OK).

2 Right-click Key Server and select **Properties**.

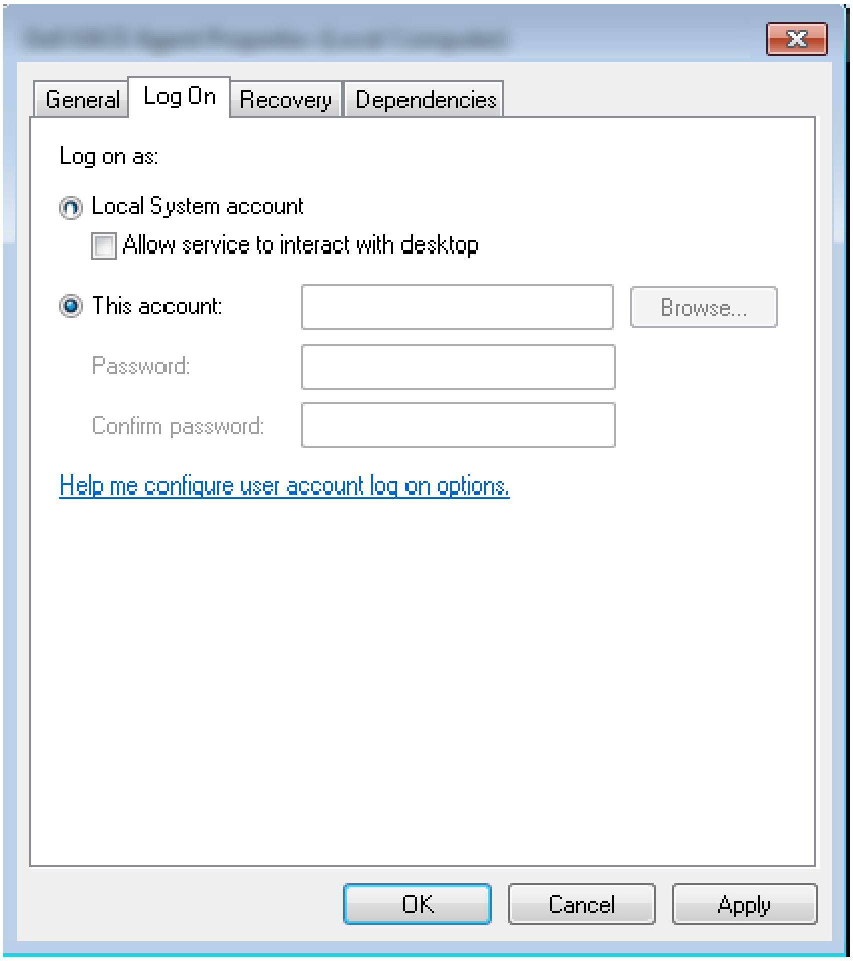


3 Select the Log On tab and select the **This account:** option.

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

Enter and confirm the password for the domain user.

Click **OK**



[redacted]

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account:

Password:

Confirm password:

Help me configure user account log on options.

4 Restart the Key Server Service (leave the Services panel open for further operation).

5 Navigate to <Key Server install dir> log.txt to verify that the Service started properly.

# Key Server Config File - Add User for EE Server Communication

1 Navigate to <Key Server install dir>.

2 Open *Credant.KeyServer.exe.config* with a text editor.

3 Go to <add key="user" value="superadmin" /> and change the "superadmin" value to the name of the appropriate user (you may also leave as "superadmin").

The "superadmin" format can be any method that can authenticate to the EE Server. The SAM account name, UPN, or domain \username is acceptable. Any method that can authenticate to the EE Server is acceptable because validation is required for that user account for authorization against Active Directory.

For example, in a multi-domain environment, only entering a SAM account name such as "jdoe" will likely fail because the EE Server will not be able to authenticate "jdoe" because it cannot find "jdoe". In a multi-domain environment, the UPN is recommended, although the domain\username format is acceptable. In a single domain environment, the SAM account name is acceptable.

4 Go to <add key="epw" value="<encrypted value of the password>" /> and change "epw" to "password". Then change "<encrypted value of the password>" to the password of the user from Step 3. This password is re-encrypted when the EE Server restarts.

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

# Sample Configuration File

```
<?xml version="1.0" encoding="utf-8" ?>

  <configuration>

    <appSettings>

       <add key="port" value="8050" /> [TCP port the Key Server will listen to. Default is 8050.]

       <add key="maxConnections" value="2000" /> [number of active socket connections the Key Server will allow]

       <add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Security Server (formerly Device Server) URL (the format is 8081/xapi for a pre-v7.7 EE Server)]

       <add key="verifyCertificate" value="false" /> [true verifies certs/set to false to not verify or if using self-signed certs]

<add key="user" value="superadmin" /> [User name used to communicate with the Security Server. This user must have the administrator role selected in the Remote Management Console. The "superadmin" format can be any method that can authenticate to the EE Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the EE Server is acceptable because validation is required for that user account for authorization against Active Directory. For example, in a multi-domain environment, only entering a SAM account name such as "jdoe" will likely fail because the EE Server will not be able to authenticate "jdoe" because it cannot find "jdoe". In a multi-domain environment, the UPN is recommended, although the domain\username format is acceptable. In a single domain environment, the SAM account name is acceptable.]

       <add key="cacheExpiration" value="30" /> [How often (in seconds) the Service should check to see who is allowed to ask for keys. The Service keeps a cache and keeps track of how old it is. Once the cache is older than the value, it gets a new list. When a user connects, the Key Server needs to download authorized users from the Security Server. If there is no cache of these users, or the list has not been downloaded in the last "x" seconds, it will be downloaded again. There is no polling, but this value configures how stale the list can become before it is refreshed when it is needed.]

       <add key="epw" value="encrypted value of the password" /> [Password used to communicate with the Security Server. If the superadmin password has been changed, it must be changed here.]

    </appSettings>

  </configuration>
```

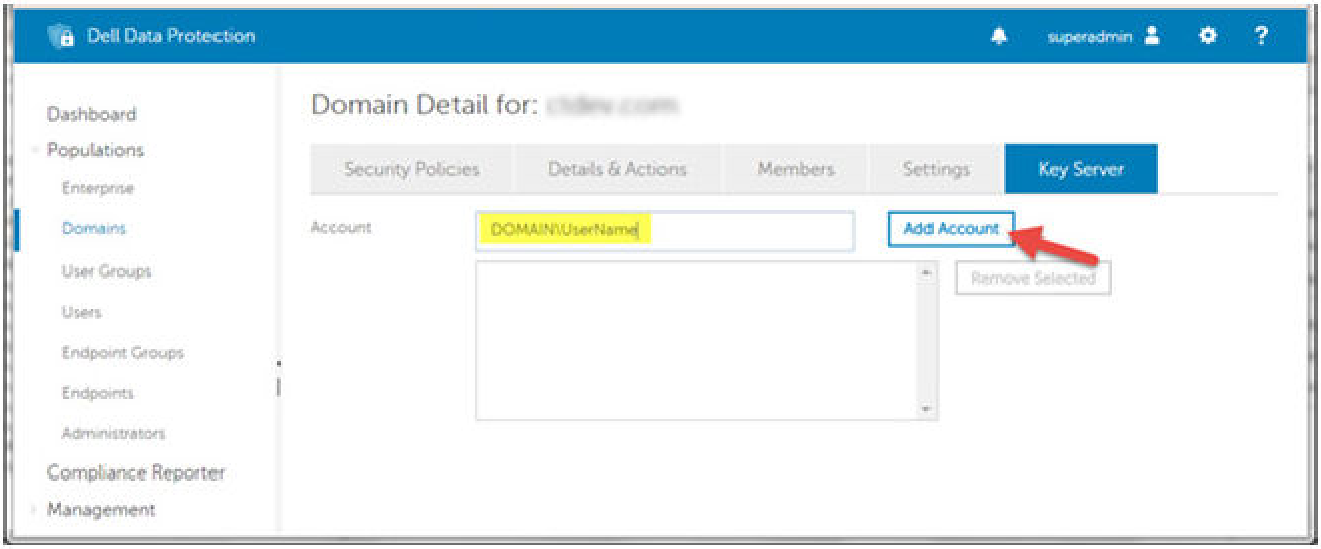
# Services Panel - Restart Key Server Service

1. Go back to the Services panel (Start > Run... > services.msc > OK).
2. Restart the Key Server Service.
3. Navigate to <Key Server install dir> log.txt to verify that the Service started properly.
4. Close the Services panel.

# Remote Management Console - Add Forensic Administrator

1. If needed, log on to the Remote Management Console.
2. Click **Populations** > **Domains**.
3. Select the appropriate Domain.
4. Click the **Key Server** tab.

5 In the Account field, add the user that will be performing the administrator activities. The format is DOMAIN\UserName. Click **Add Account**.



Domain Detail for:

Account: DOMAIN\UserName

6 Click **Users** in the left menu. In the search box, search for the username added in Step 5. Click **Search**.

7 Once the correct user is located, click the **Admin** tab.

8 Select **Forensic Administrator** and click **Update**.

The components are now configured for Kerberos Authentication/Authorization.

# Use the Administrative Download Utility (CMGAd)

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

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

## Use the Administrative Download Utility in Forensic Mode

1 Double-click **cmgad.exe** to launch the utility or open a command prompt where CMGAd is located and type **`cmgad.exe -f`** (or **`cmgad.exe`**).

2 Enter the following information (some fields may be pre-populated).

Device Server URL: Fully qualified Security Server (Device Server) URL. The format is https://securityserver.domain.com:8443/xapi/. If your EE Server is pre-v7.7, the format is https://deviceserver.domain.com:8081/xapi (different port number, without the trailing slash).

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

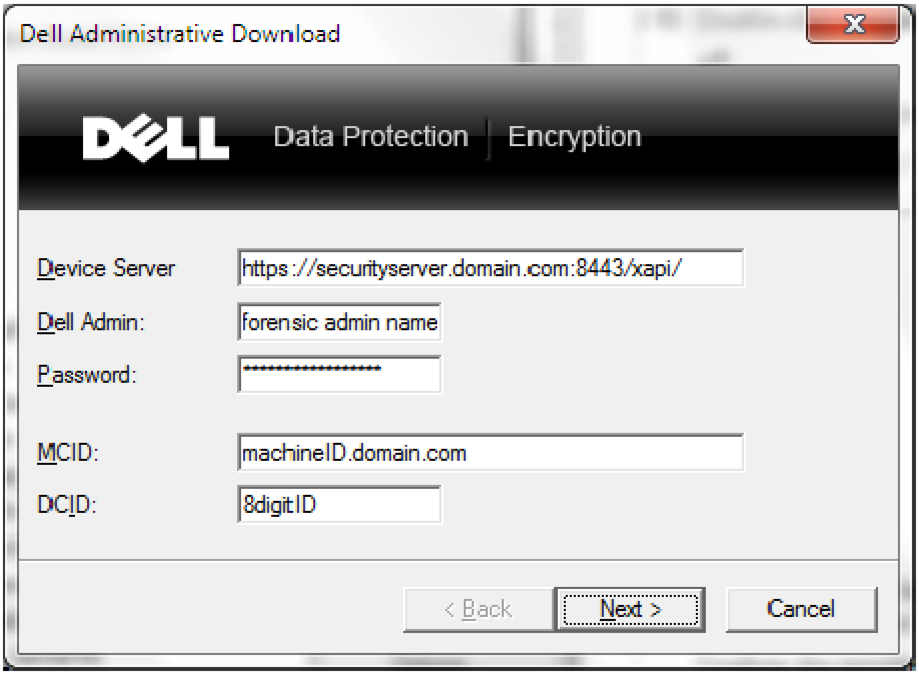
Password: Forensic administrator password

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

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

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

Click **Next**.


Dell Administrative Download
DELL Data Protection | Encryption

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

Dell Admin: forensic admin name

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

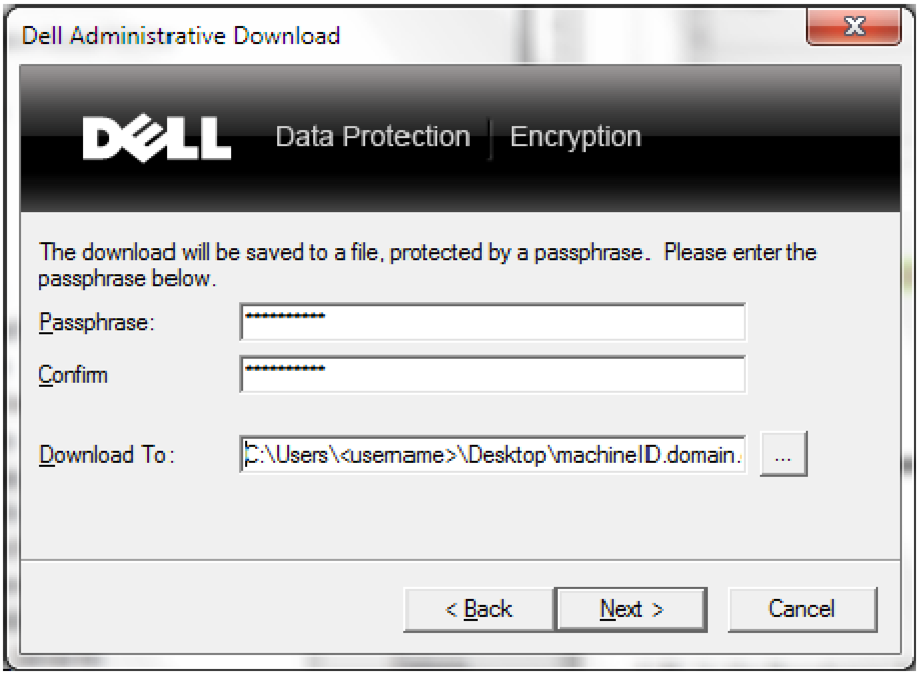
MCID: machineID.domain.com

DCID: 8digitID

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

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

Click **Next**.


Dell Administrative Download
DELL Data Protection | Encryption

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

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

Confirm: ***********

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

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

4 Click **Finish** when complete.

# Use the Administrative Download Utility in Admin Mode

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

1. Open a command prompt where CMGAd is located and type `cmgad.exe -a`.
2. Enter the following information (some fields may be pre-populated).

   Server: Fully qualified hostname of the Key Server, such as keyserver.domain.com

   Port Number: The default port is 8050

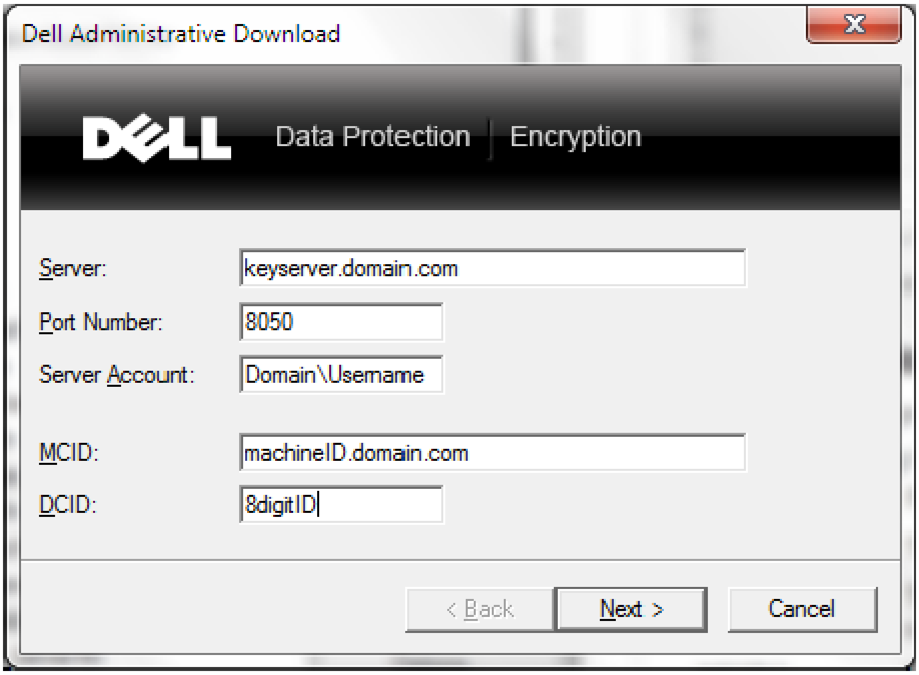
   Server Account: The domain user the Key Server is running as. The format is domain\username. The domain user running the utility must be authorized to perform the download from the Key Server

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

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

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

   Click **Next**.



Server: keyserver.domain.com

Port Number: 8050

Server Account: Domain\Username

MCID: machineID.domain.com

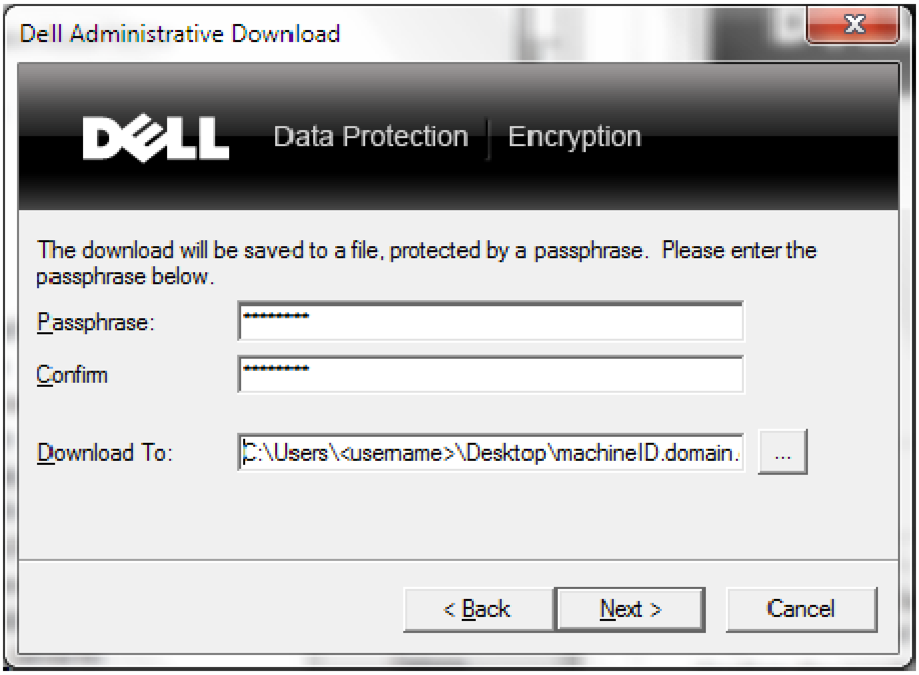
DCID: 8digitID

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

   Confirm the passphrase.

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

   Click **Next**.



Dell Administrative Download

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

Passphrase: *********

Confirm *********

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

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

4 Click **Finish** when complete.

# Configure Server Encryption

## Enable Server Encryption

NOTE:
Server Encryption converts User encryption to Common encryption.

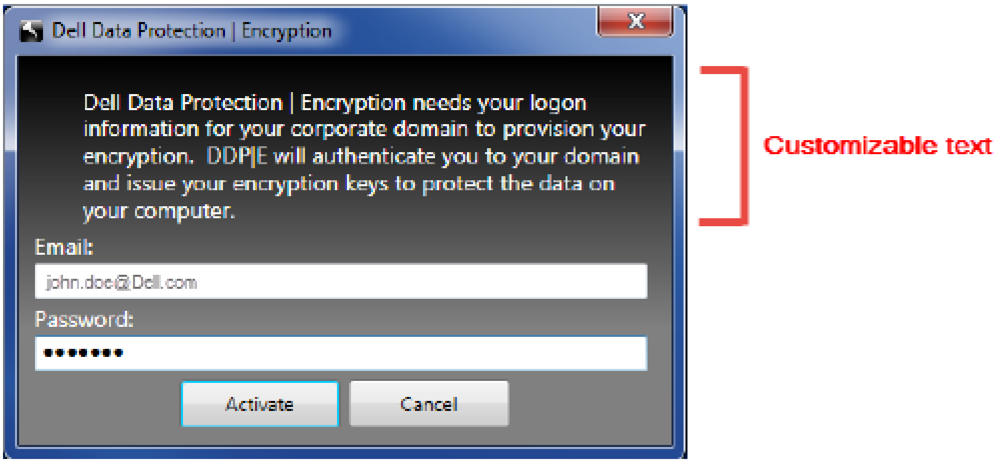
1 Log in as a Dell Administrator on the Dell Remote Management Console.
2 Select **Endpoint Group** (or **Endpoint**), search for the endpoint or endpoint group you want to enable, select **Security Policies**, and then select the **Server Encryption** policy category.
3 Set the following policies:
   - Server Encryption - **Select** to enable Server Encryption and related policies.
   - SDE Encryption Enabled - **Select** to turn on SDE encryption.
   - Encryption Enabled - **Select** to turn on Common encryption.
   - Secure Windows Credentials - This policy is **Selected** by default.

     When the *Secure Windows Credentials* policy is **Selected** (the default), all files in the \Windows\system32\config files folder are encrypted, including Windows credentials. To prevent Windows credentials from being encrypted, set the *Secure Windows Credentials* policy to **Not Selected**. Encryption of Windows credentials occurs independently of the *SDE Encryption Enabled* policy setting.
4 Save and commit the policies.

## Customize Activation Logon Dialog

The Activation Logon dialog displays:

- When an unmanaged user logs on.
- When the user selects Activate Dell Encryption from the Encryption icon's menu, located in the system tray.



Dell Data Protection | Encryption

Dell Data Protection | Encryption needs your logon information for your corporate domain to provision your encryption. DDP|E will authenticate you to your domain and issue your encryption keys to protect the data on your computer.

Email: john.doe@Dell.com

Password: •••••••

# Set Server Encryption EMS Policies

The ***originating encrypting computer*** is the computer that originally encrypts a removable device. When the originating computer is a ***protected server*** - a server with Server Encryption installed and activated - and the protected server first detects the presence of a removable device, the user is prompted to encrypt the removable device.

- EMS policies control removable media access to the server, authentication, encryption, and more.
- Port Control policies affect removable media on protected servers, for example, by controlling access and usage of the Server's USB ports by USB devices.

The policies for removable media encryption can be found in the Remote Management Console under the *Server Encryption* technology group.

**Server Encryption and External Media**

When the protected server's *EMS Encrypt External Media* policy is **Selected**, external media is encrypted. Server Encryption links the device to the protected server with the Machine key and to the user, with the User Roaming key of the removable device's owner/user. All files added to the removable device will then be encrypted with those same keys, regardless of the computer it is connected to.

> **NOTE:**
>
> Server Encryption converts User encryption to Common encryption, except on removable devices. On removable devices, encryption is performed with the User roaming key associated with the computer.

When the user does not agree to encrypt the removable device, the user's access to the device can be set to *blocked* when used on the protected server, *Read only* while used on the protected server, or *Full access*. The protected server's policies determine the level of access on an unprotected removable device.

Policy updates occur when the removable device is re-inserted into the originating protected server.

**Authentication and External Media**

The protected server's policies determine authentication functionality.

After a removable device has been encrypted, only its owner/user can access the removable device on the protected server. Other users will not be able to access the encrypted files on the removable media.

Local automatic authentication allows the protected removable media to be automatically authenticated when inserted in the protected server when the owner of that media is logged in. When automatic authentication is disabled, the owner/user must authenticate to access the protected removable device.

When a removable device's originating encrypting computer is a protected server, the owner/user must always log in to the removable device when using it on non-originating computers, regardless of the EMS policy settings defined on the other computers.

Refer to AdminHelp for information on Server Encryption Port Control and EMS policies.

# Suspend an Encrypted Server Instance

Suspending an encrypted server prevents access to its encrypted data after a restart. The virtual server user cannot be suspended. Instead, the Server Encryption Machine key is suspended.

> **NOTE:**
>
> Suspending the server endpoint does not immediately suspend the server. The suspension takes place the next time the key is requested, typically the next time the server is restarted.

> **IMPORTANT:**
> Use with care. Suspending an encrypted server instance could result in instability, depending on policy settings and whether the protected server is suspended while disconnected from the network.

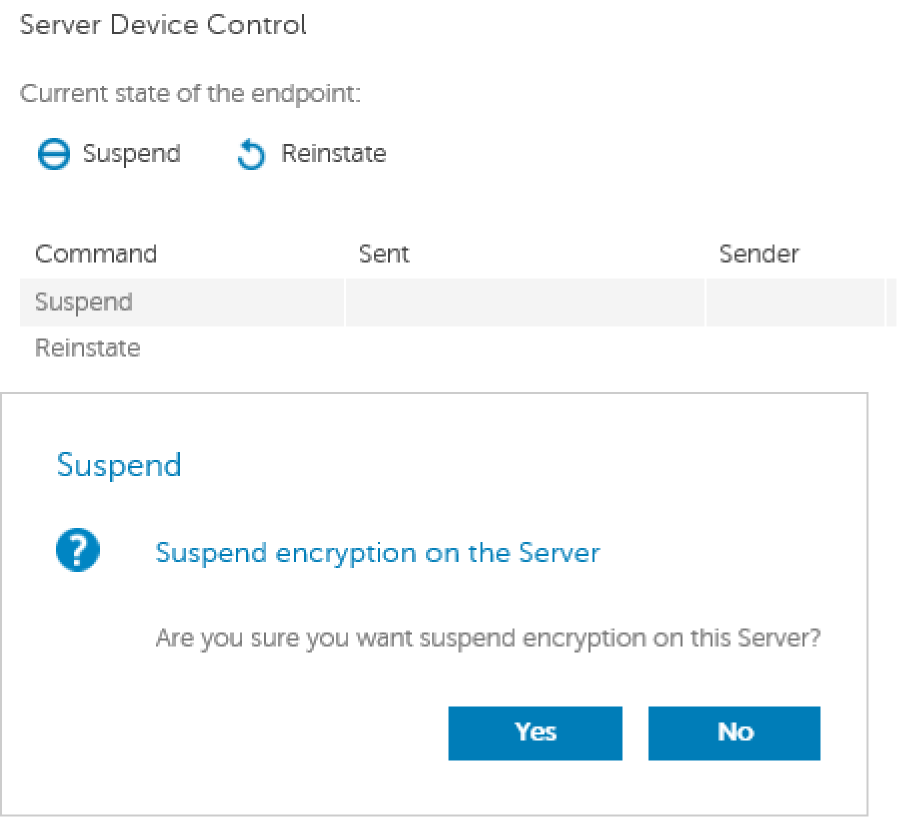
**Prerequisites**

- Help Desk Administrator rights, assigned in the Remote Management Console, are required to suspend an endpoint.
- The administrator must be logged in to the Remote Management Console.

In the left pane of the Remote Management Console, click **Populations** > **Endpoints**.

Search or select a Hostname, then click the **Details & Actions** tab.

Under Server Device Control, click **Suspend** then **Yes**.



Server Device Control

Current state of the endpoint:

| Command | Sent | Sender |
|---|---|---|
| Suspend | | |
| Reinstate | | |

Suspend

Suspend encryption on the Server

Are you sure you want suspend encryption on this Server?

> **NOTE:**
> Click the **Reinstate** button to allow Server Encryption to access encrypted data on the server after it restarts.

# Configure Deferred Activation

Enterprise Edition with Deferred Activation differs from Enterprise Edition activation in two ways:

**Device-based Encryption policies**

Enterprise Edition encryption policies are user-based; Enterprise Edition with Deferred Activation's encryption policies are device-based. User encryption is converted to Common encryption. This difference allows the user to bring a personal device to use within the organization's domain, while the organization maintains its security by centrally managing encryption policies.

**Activation**

With Enterprise Edition, activation is automatic. When Enterprise Edition with Deferred Activation is installed, automatic activation is disabled. Instead, the user chooses whether to activate encryption, and when to activate it.

> ⓘ **IMPORTANT:**
> Before a user permanently leaves the organization and while his email address is still active, the user must run the Encryption Removal Agent and uninstall the Encryption client from his personal computer.

## Deferred Activation Customization

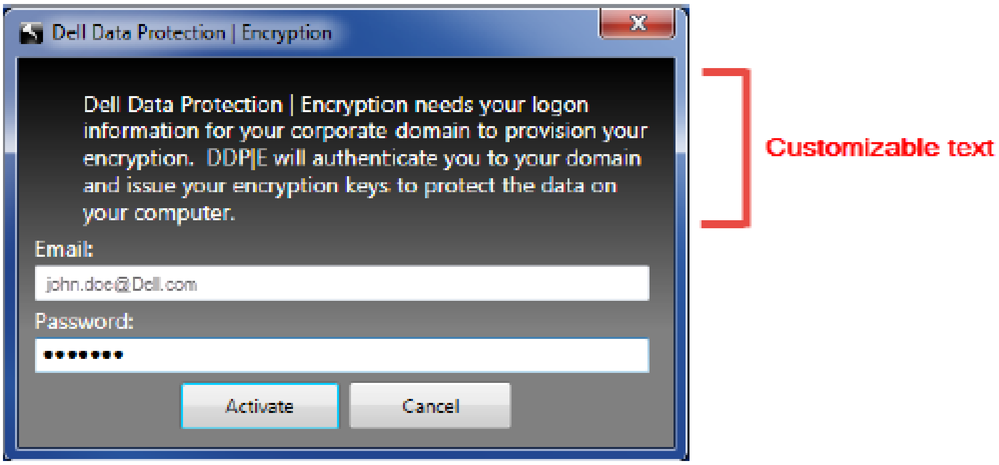
These client-side tasks allow Deferred Activation customization.

- Add a disclaimer to the Activation Logon dialog box
- Disable automatic re-activation (optional)

Add a disclaimer to the Activation Logon dialog box

The Activation Logon dialog displays at these times:

- When an unmanaged user logs on.
- When the user decides to activate encryption and selects Activate Encryption from the system tray Encryption icon menu.



Dell Data Protection | Encryption

Dell Data Protection | Encryption needs your logon information for your corporate domain to provision your encryption. DDP|E will authenticate you to your domain and issue your encryption keys to protect the data on your computer.

Email: john.doe@Dell.com

Password: ●●●●●●●

# Prepare the Computer for Installation

If the data is encrypted with a non-Dell encryption product, before installing the Encryption client, decrypt data using the existing encryption software, and then uninstall the existing encryption software. If the computer does not restart automatically, restart the computer.

### Create a Windows Password

Dell highly recommends that a Windows password be created (if one does not already exist) to protect access to the encrypted data. Creating a password for the computer prevents others from logging on to your user account without your password.

### Uninstall Previous Versions of the Encryption Client

Before uninstalling a previous version of the Encryption client, stop or pause an encryption sweep, if necessary.

If the computer is running a version of Dell Encryption earlier than v8.6, uninstall the Encryption client from the command line. For instructions, see *Uninstall Encryption and Server Encryption Client*.

> ⓘ NOTE:
>
> If you plan to install the latest version of the Encryption client immediately after uninstallation, it is not necessary to run the Encryption Removal Agent to decrypt the files.
>
> To upgrade a previous version of the Encryption client installed with Deferred Activation, use the Control Panel/Uninstall a Program utility. This uninstallation method is possible even if OPTIN is disabled.

> ⓘ NOTE:
>
> If no users were previously activated, the Encryption client clears the OPTIN setting from the SDE vault since the setting is left-over from a previous installation. The Encryption client blocks Deferred Activations if users previously activated but the OPTIN flag is not set in the SDE vault.

# Install the Encryption Client with Deferred Activation

To install the Encryption client with Deferred Activation, install the Encryption client with the OPTIN=1 parameter. For more information about client installation with the OPTIN=1 parameter, see Install Encryption Client.

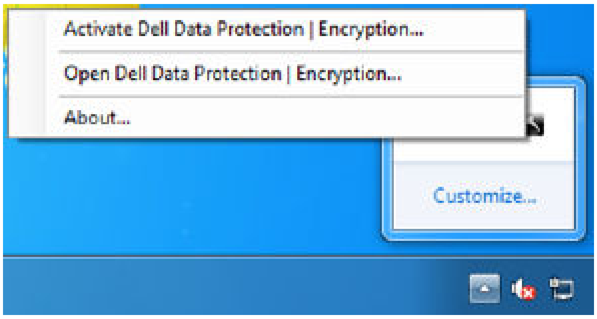
# Activate the Encryption Client with Deferred Activation

- Activation associates a domain user with a local user account and a specific computer.
- Multiple users can activate on the same computer, provided they use unique local accounts and have unique domain email addresses.
- A user can activate the Encryption client only once per domain account.

Before you activate the Encryption client:

- Log in to the local account that you use the most often. The data associated with this account is the data that will be encrypted.
- Connect to your organization's network.

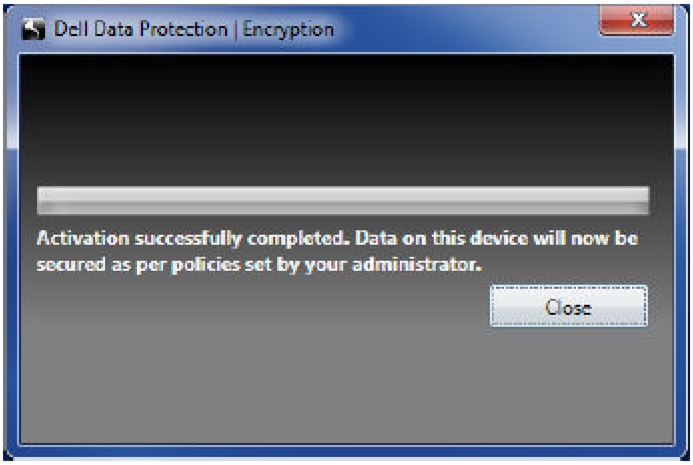
1 Right-click the Encryption icon in the system tray, and click **About**.
2 Select **Activate Encryption** from the menu.


Activate Dell Data Protection | Encryption...
Open Dell Data Protection | Encryption...
About...
Customize...

3 Enter the domain email address and password and click **Activate**.

> **NOTE:**
> Non-domain or personal email addresses cannot be used for activation.

4 Click **Close**.



Activation successfully completed. Data on this device will now be secured as per policies set by your administrator.

The Dell Server combines the encryption key bundle with the user's credentials and with the computer's unique ID (machine ID), creating an unbreakable relationship between the key bundle, the specific computer, and the user.

5 Restart the computer to begin the encryption sweep.

> **NOTE:**
> The Local Management Console, accessible from the system tray icon, shows the policies sent by the Server, not the effective policy.

# Troubleshoot Deferred Activation

## Troubleshoot Activation

**Problem: Cannot access certain files and folders**

Inability to access certain files and folders is a symptom of being logged in with a different account than the one under which the user activated.

The Activation Logon dialog automatically displays even though the user has previously activated.

**Possible Solution**

Log out and log back in with the credentials of the activated account and try to access the files again.

In the rare event that the Encryption client cannot authenticate the user, the Activation Logon dialog prompts the user for credentials to authenticate and access encryption keys. To use the automatic re-activation feature, the *AutoReactivation* and *AutoPromptForActivation* registry keys must BOTH be enabled. Although the feature is enabled by default, it can be manually disabled. For more information, see Disable Automatic Re-activation.

**Error Message: Server Authentication Failed**

The Server was not able to authenticate the email address and password.

**Possible Solutions**

- Use the email address associated with the organization. Personal email addresses cannot be used for activation.
- Re-enter the email address and password and ensure there are no typographical errors.
- Ask the administrator to verify that the email account is active and is not locked.
- Ask the administrator to reset the user's domain password.

**Error Message: Network connection error**

The Encryption client could not communicate with the Dell Server.

**Possible Solutions**

- Connect directly to the organization's network and try to activate again.
- If VPN access is required to connect to the network, check the VPN connection and try again.
- Check the Dell Server URL to ensure it matches the URL provided by the administrator.

  The URL and other data that the user entered into the installer are stored in the registry. Check the accuracy of the data under [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] and [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]
- Disconnect and reconnect:

  Disconnect the computer from the network.

  Reconnect to the network.

  Restart the computer.

  Try to connect to the network again.

**Error Message: Legacy Server Not Supported**

Encryption cannot be activated against a legacy server; the Dell Server must be v9.1 or higher.

**Possible Solution**

- Check the Dell Server URL to ensure it matches the URL provided by the administrator.

  The URL and other data that the user entered into the installer are stored in the registry.
- Check the accuracy of the data under [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] and [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

**Error Message: Domain User Already Activated**

A second user has logged on to the local computer and tried to activate against a domain account that has already been activated.

A user can activate the Encryption client only once per domain account.

**Possible Solution**

Decrypt and uninstall the Encryption client while logged in as the second activated user.

#### Error Message: Server Error General

An error has occurred on the Server.

#### Possible Solution

The administrator should check the Server logs to ensure services are running.

The user should try to activate later.

### Tools

CMGad

Use the CMGAd utility prior to launching the Encryption Removal Agent to obtain the encryption key bundle. The CMGAd utility and its instructions are located in the Dell installation media (Dell-Offline-Admin-XXbit-8.x.x.xxx.zip)

### Log Files

In C:\ProgramData\Dell\Dell Data Protection\Encryption, look for the log file called **CmgSysTray**.

Search for the phrase "Manual activation result".

The error code is on the same line, followed by " status = "; the status indicates what went wrong.

# Troubleshooting

## All Clients - Troubleshooting

- **Master installer log files** are located at C:\ProgramData\Dell\Dell Data Protection\Installer.
- Windows creates unique **child installer installation log files** for the logged in user at %temp%, located at C:\Users\<UserName>\AppData\Local\Temp.
- Windows creates log files for client prerequisites, such as Visual C++, for the logged in user at %temp%, located at C:\Users\<UserName>\AppData\Local\Temp. For example, C:\Users\<UserName>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log
- Follow the instructions at http://msdn.microsoft.com to verify the version of Microsoft .Net that is installed on the computer targeted for installation.

  Go to https://www.microsoft.com/en-us/download/details.aspx?id=30653to download the full version of Microsoft .Net Framework 4.5.
- See *Dell Data Protection | Security Tools Compatibility* if the computer targeted for installation has (or has had in the past) Dell Access installed. DDP|A is not compatible with this suite of products.

## Encryption and Server Encryption Client Troubleshooting

### Upgrade to the Windows 10 Anniversary Update

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

### Activation on a Server Operating System

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

**Troubleshooting Initial Activation**

Initial activation fails when:

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

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

The user name or password does not match.

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

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

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

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

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

or

```
The operation timed out.
```

Server Encryption could not communicate with port 8449 over https to the DDP Security Server.

**Possible Solutions**

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

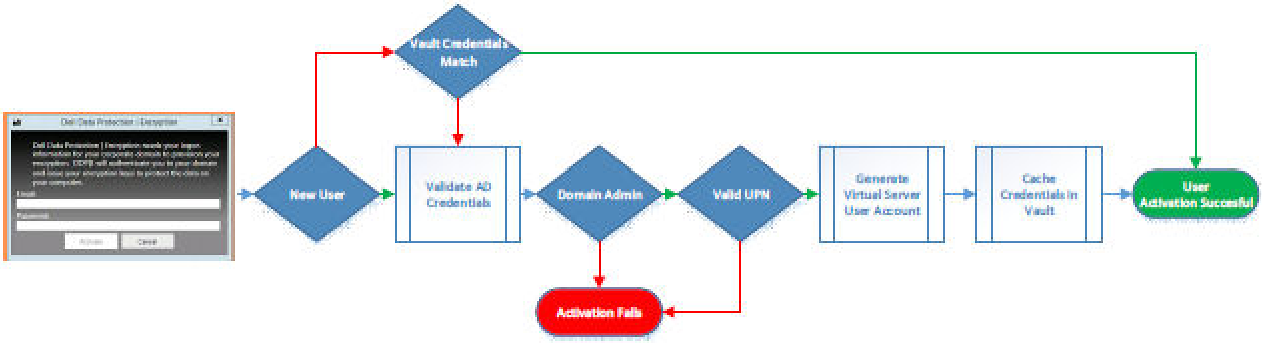
**Error Message: Activation failed because the Server is unable to support this request.**

**Possible Solutions**

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

**Initial Activation Process**

The following diagram illustrates a successful initial activation.



Dell Data Protection | Encryption needs your logon information for your corporate domain to provision your encryption. DDPE will authenticate you to your domain and issue your encryption keys to protect the data on your computer.

Email

Password

Dell Data Protection | Encryption
Activate
Cancel
Vault Credentials Match
New User
Validate AD Credentials
Domain Admin
Valid UPN
Generate Virtual Server User Account
Cache Credentials in Vault
User Activation Succesful
Activation Fails

The initial activation process of Server Encryption requires a live user to access the server. The user can be of any type: domain or non-domain, remote-desktop-connected or interactive user, but the user must have access to Domain Administrator credentials.

The Activation dialog box displays when one of the two following things happens:

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

  The initial activation process is as follows:

1 The user logs in.

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

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

4 The user right-clicks the Encryption client icon in the system tray and selects **Activate Dell Encryption**.

5 The user enters Domain Administrator credentials in the Activate dialog.

> **NOTE:**
>
> The requirement for Domain Administrator credentials is a safety measure that prevents Server Encryption from being rolled out to other server environments that do not support it. To disable the requirement for Domain Administrator credentials, see Before You Begin.

6 DDP Server checks for the credentials in the enterprise vault (Active Directory or equivalent) to verify that the credentials are Domain Administrator credentials.

7 A UPN is constructed using the credentials.

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

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

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

9 When activation is successful, the user restarts the computer, which kicks off the second part of activation, Authentication and Device Activation.

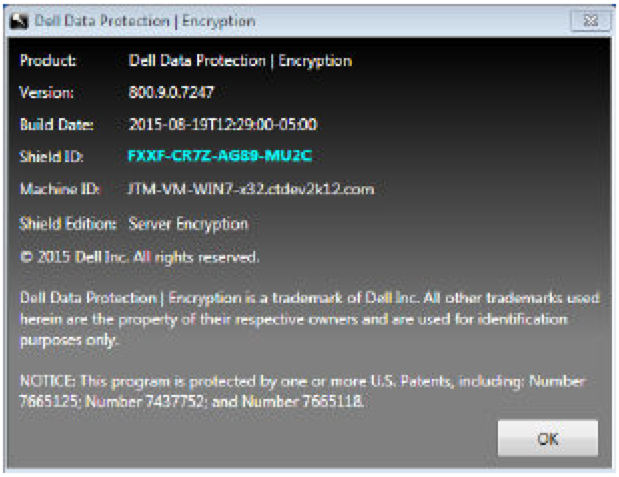
**Troubleshooting Authentication and Device Activation**

Device activation fails when:

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

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

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



Dell Data Protection | Encryption

Product: Dell Data Protection | Encryption

Version: 800.9.0.7247

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

Shield ID: FXXF-CR7Z-AG89-MU2C

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

Shield Edition: Server Encryption

© 2015 Dell Inc. All rights reserved.

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

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

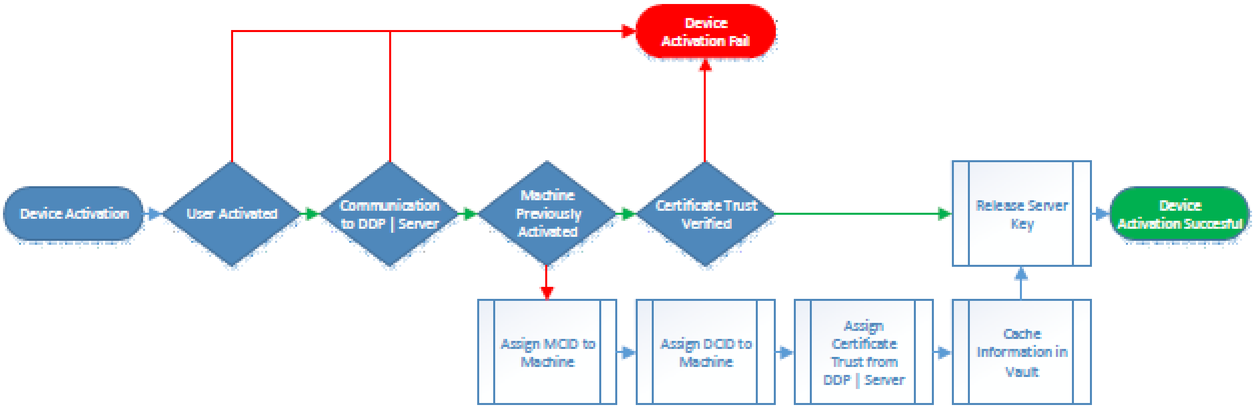
- If the Shield ID is red, encryption has not yet been activated.
- In the Remote Management Console, the version of a server with Server Encryption installed is listed as *Shield for Server*.
- If the Machine key retrieval fails due to a network failure, Server Encryption registers for network notifications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

- If the Machine key retrieval fails:
  - The virtual server user logon is still successful.
  - Set up the *Retry Interval Upon network Failure* policy to make key retrieval attempts on a timed interval.

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

**Authentication and Device Activation Process**

The following diagram illustrates successful authentication and device activation.


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

1 When restarted after a successful initial activation, a computer with Server Encryption automatically authenticates using the virtual server user account and runs the Encryption client in Server mode.

2 The computer checks its device activation status with the DDP Server:

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

3 After the DDP Server assigns the trust certificate to the server, the server can access its encryption keys.

4 Device activation is successful.

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

# (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.

# EMS and PCS Interactions

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

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

### To Encrypt Data Written to CD/DVD

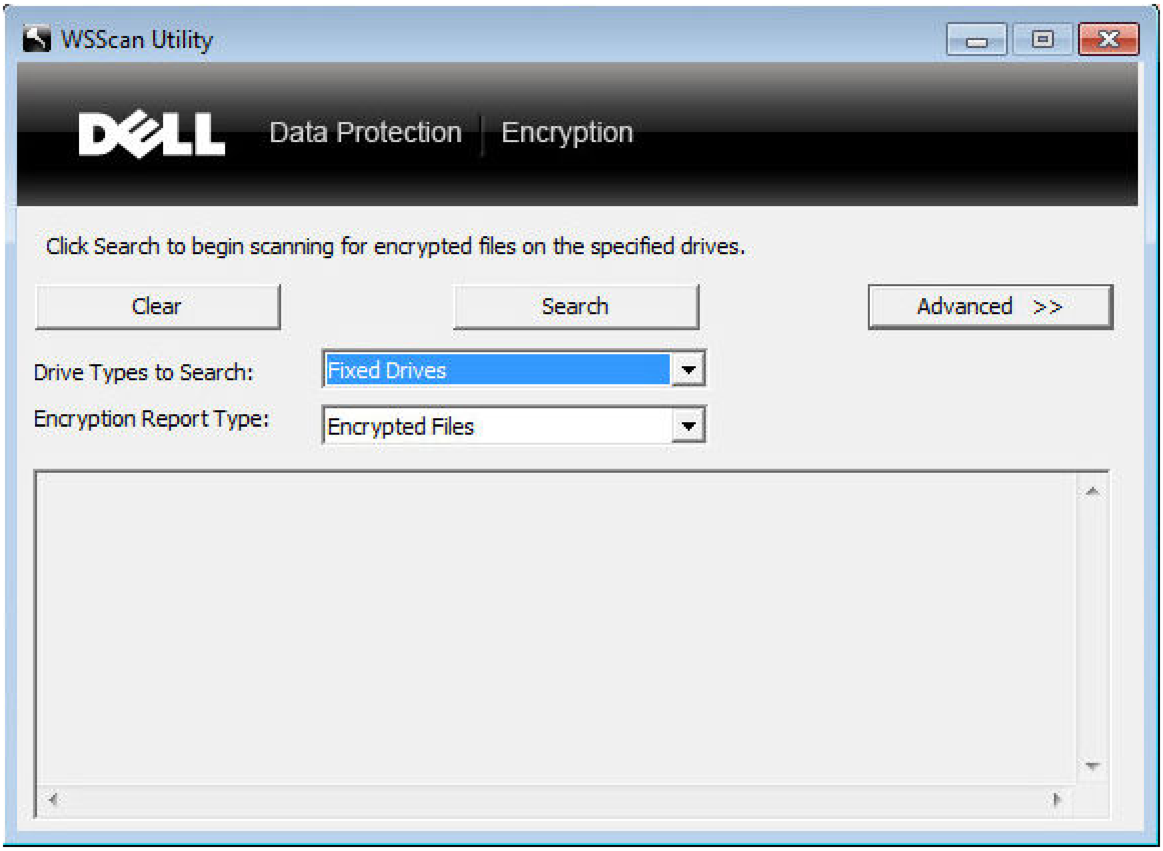
- Set EMS Encrypt External Media = True.
- Set EMS Exclude CD/DVD Encryption = False.
- Set Subclass Storage: Optical Drive Control = UDF Only.

# Use WSScan

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

### Run WSScan

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



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

Drive Types to Search: Fixed Drives

Encryption Report Type: Encrypted Files

OR

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

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

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

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

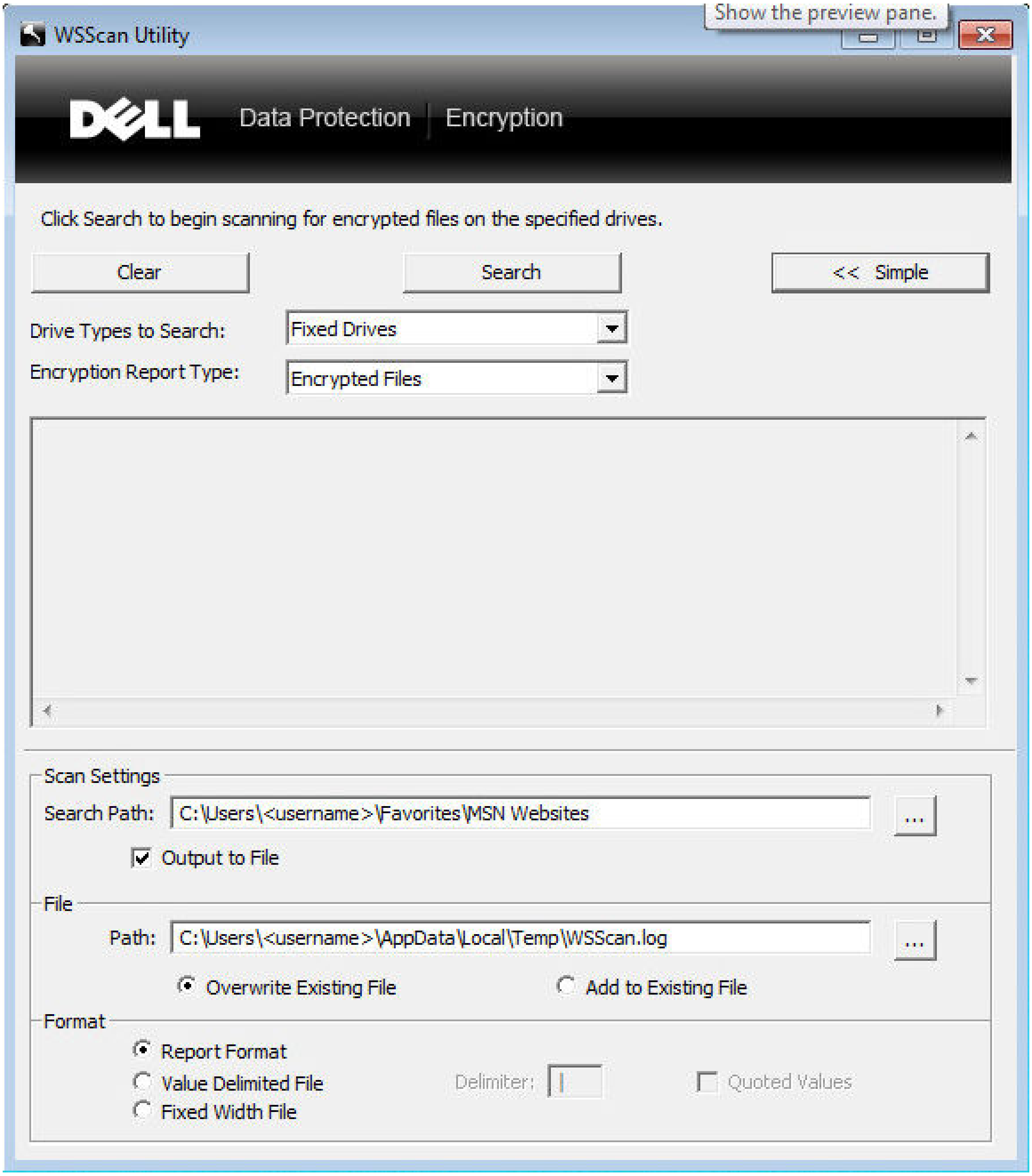
5 Select **Add to Existing File** if you do not want to overwrite any existing WSScan output files.

6 Choose the output format:

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

7 Click **Search**.

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



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

Drive Types to Search: Fixed Drives

Encryption Report Type: Encrypted Files

Scan Settings

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

☑ Output to File

File

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

● Overwrite Existing File ○ Add to Existing File

Format

● Report Format

○ Value Delimited File Delimiter: | □ Quoted Values

○ Fixed Width File

### WSScan Command Line Usage

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r] [-
u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

| Switch | Meaning |
|---|---|
| Drive | Drive to scan. If not specified, the default is all local fixed hard drives. Can be a mapped network drive. |
| -ta | Scan all drives |
| -tf | Scan fixed drives (default) |
| -tr | Scan removable drives |

| Switch | Meaning |
|---|---|
| -tc | Scan CDROMs/DVDROMs |
| -s | Silent operation |
| -o | Output file path |
| -a | Append to output file. The default behavior truncates the output file. |
| -f | Report format specifier (Report, Fixed, Delimited) |
| -r | Run WSScan without administrator privileges. **Some files may not be visible if this mode is used.** |
| -u | Include unencrypted files in output file.<br>This switch is sensitive to order: "u" must be first, "a" must be second (or omitted), "-" or "v" must be last. |
| -u- | Only include unencrypted files in output file |
| -ua | Report unencrypted files also, but use all user policies to display the "should" field. |
| -ua- | Report unencrypted files only, but use all user policies to display the "should" field. |
| -uv | Report unencrypted files that violate policy only (Is=No / Should=Y) |
| -uav | Report unencrypted files that violate policy only (Is=No / Should=Y), using all user policies. |
| -d | Specifies what to use as a value separator for delimited output |
| -q | Specifies the values that should be in enclosed in quotes for delimited output |
| -e | Include extended encryption fields in delimited output |
| -x | Exclude directory from scan. Multiple exclusions are allowed. |
| -y | Sleep time (in milliseconds) between directories. This switch results in slower scans, but potentially a more responsive CPU. |

### 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.<br>**SysData:** SDE Encryption Key.<br>**User:** User Encryption Key.<br>**Common:** Common Encryption Key. |

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

# Use WSProbe

The Probing Utility is for use with all versions of the Encryption client, with the exception of EMS policies. Use the Probing Utility to:

- Scan or schedule scanning of an encrypted computer. The Probing Utility observes your Workstation Scan Priority policy.
- Temporarily disable or re-enable the current user Application Data Encryption List.
- Add or remove process names on the privileged list.
- Troubleshoot as instructed by Dell ProSupport.

### Approaches to Data Encryption

If you specify policies to encrypt data on Windows devices, you can use any of the following approaches:

- The first approach is to accept the default behavior of the client. If you specify folders in Common Encrypted Folders or User Encrypted Folders, or set Encrypt "My Documents", Encrypt Outlook Personal Folders, Encrypt Temporary Files, Encrypt Temporary Internet Files, or Encrypt Windows Paging File to selected, affected files are encrypted either when they are created, or (after being created by an unmanaged user) when a managed user logs on. The client also scans folders specified in or related to these policies for possible encryption/decryption when a folder is renamed, or when the client receives changes to these policies.
- You can also set Scan Workstation on Logon to True. If Scan Workstation on Logon is True, when a user logs on, the client compares how files in currently- and previously-encrypted folders are encrypted to the user policies, and makes any necessary changes.
- To encrypt files that meet your encryption criteria but were created prior to your encryption policies going into effect, but do not want the performance impact of frequent scanning, you can use this utility to scan or schedule scanning of the computer.

### Prerequisites

- The Windows device you want to work with must be encrypted.

- The user you want to work with must be logged on.

### Use the Probing Utility

WSProbe.exe is located in the installation media.

#### Syntax

```
wsprobe [path]
```

```
wsprobe [-h]
```

```
wsprobe [-f path]
```

```
wsprobe [-u n] [-x process_names] [-i process_names]
```

#### Parameters

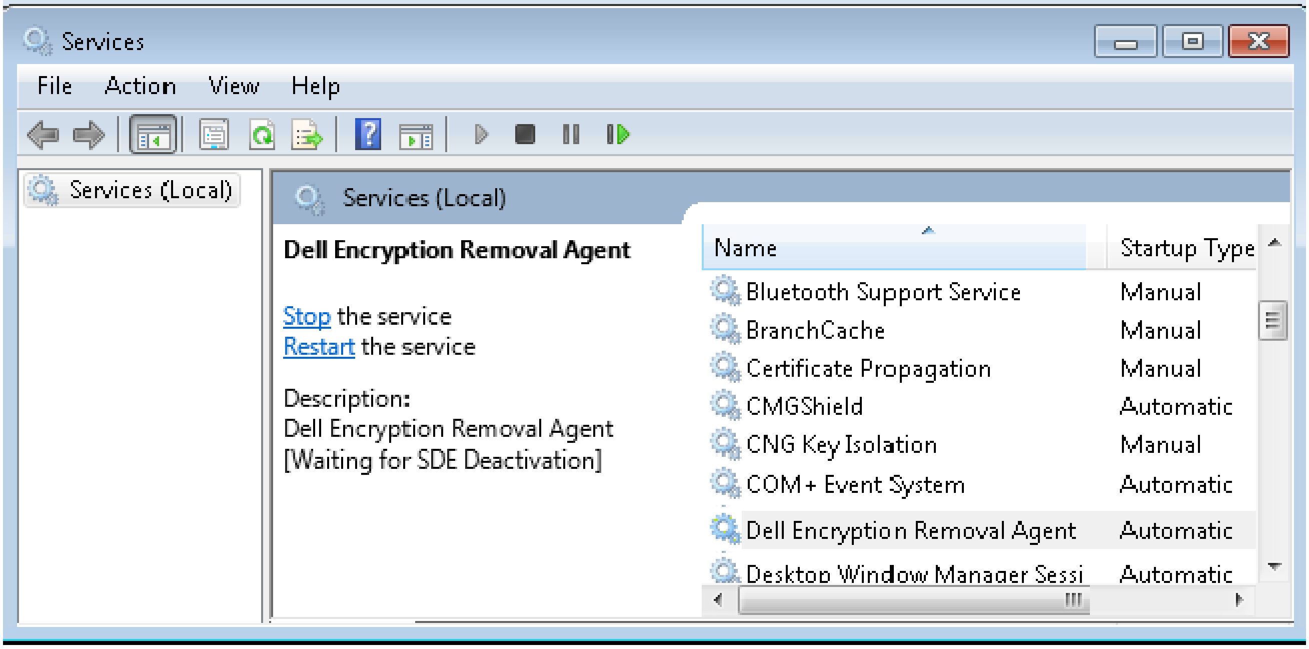
| Parameter | To |
|---|---|
| path | Optionally specify a particular path on the device that you want to scan for possible encryption/ decryption. If you do not specify a path, this utility scans all folders related to your encryption policies. |
| -h | View command line Help. |
| -f | Troubleshoot as instructed by Dell ProSupport |
| -u | Temporarily disable or re-enable the user Application Data Encryption List. This list is only effective if Encryption Enabled is selected for the current user. Specify 0 to disable or 1 to re-enable. The current policy in force for the user is reinstated at the next logon. |
| -x | Add process names to the privileged list. The computer and installer process names on this list, plus those you add using this parameter or HKLM\Software\CREDANT\CMGShield \EUWPrivilegedList, are ignored if specified in the Application Data Encryption List. Separate process names with commas. If your list includes one or more spaces, enclose the list in double quotes. |
| -i | Remove process names previously added to the privileged list (you cannot remove hard-coded process names). Separate process names with commas. If your list includes one or more spaces, enclose the list in double quotes. |

# 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. See (Optional) Create an Encryption Removal Agent Log File for instructions.
- **Complete** - The decryption sweep is complete. The Service, the executable, the driver, and the driver executable are all scheduled for deletion on the next restart.



**Dell Encryption Removal Agent**

Stop the service
Restart the service

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

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

# SED Client Troubleshooting

## Use the Initial Access Code Policy

- This policy is used to log on to a computer when network access is unavailable. Meaning, access to the EE Server/VE Server and AD are both unavailable. Only use the *Initial Access Code* policy if absolutely necessary. Dell does not recommend this method to log in. Using the *Initial Access Code* policy does not provide the same level of security as the usual method of logging in using username, domain, and password.

  In addition to being a less secure method of logging in, if an end user is activated using the *Initial Access Code*, then there is no record on the EE Server/VE Server of that user activating on this computer. In turn, there is no way to generate a Response Code from the EE Server/VE Server for the end user if they fail password and self help questions.
- The *Initial Access Code* can only be used **one** time, immediately after activation. After an end user has logged in, the *Initial Access Code* will not be available again. The first domain login that occurs after the *Initial Access Code* is entered will be cached, and the *Initial Access Code* entry field will not be displayed again.
- The *Initial Access Code* will **only** display under the following circumstances:
  - A user has never activated inside the PBA.

- The client has no connectivity to the network or EE Server/VE Server.

### Use Initial Access Code

1. Set a value for the **Initial Access Code** policy in the Remote Management Console.
2. Save and commit the policy.
3. Start the local computer.
4. Enter the **Initial Access Code** when the Access Code screen displays.
5. Click the **blue arrow**.
6. Click **OK** when the Legal Notice screen displays.
7. Log in to Windows with the user credentials for this computer. These credentials must be part of the domain.
8. After logging in, open the Security Console and verify that the PBA user was successfully created.

   Click **Log** in the top menu and look for the message *Created PBA user for <domain\username>*, which indicates the process was successful.
9. Shut down and restart the computer.
10. At the login screen, enter the username, domain, and password that was previously used to log in to Windows.

    You must match the username format that was used when creating the PBA user. Thus, if you used the format domain/username, you must enter domain/username for the Username.
11. (Credant Manager only) Respond to the Question and Answer prompts.

    Click the **blue arrow**.
12. Click **Login** when the Legal Notice screen displays.

    Windows now launches and the computer can be used as usual.

# Create a PBA Log File for Troubleshooting

- There may be cases when a PBA log file is needed for troubleshooting PBA issues, such as:
  - You are unable to see the network connection icon, yet you know there is network connectivity. The log file contains DHCP information to resolve the issue.
  - You are unable to see the EE Server/VE Server connection icon. The log file contains information to help diagnose EE Server/VE Server connectivity issues.
  - Authentication fails even when entering correct credentials. The log file used with the EE Server/VE Server logs can help diagnose the issue.

### Capture Logs When Booting Into the PBA (Legacy PBA)

1. Create a folder on a USB drive and name it **\CredantSED**, at the root level of the USB drive.
2. Create a file named actions.txt and place it in the **\CredantSED** folder.
3. In actions.txt, add the line:

   ```
   get environment
   ```
4. Save and close the file.

   *Do not insert the USB drive when the computer is powered down*. If the USB drive is already inserted during the shutdown state, remove the USB drive.
5. Power on the computer and log in to the PBA. Insert the USB drive into the computer that the logs are to be collected from during this step.
6. After inserting the USB drive, wait for 5-10 seconds, then remove the drive.

   A credpbaenv.tgz file is created in the **\CredantSED** folder that contains the needed log files.

### Capture Logs When Booting Into the PBA (UEFI PBA)

1 Create a file called **PBAErr.log** at the root level of the USB drive.
2 Insert the USB drive **before** powering on the computer.
3 Remove the USB drive **after** reproducing the issue requiring the logs.

The PBAErr.log file will be updated and written to real-time.

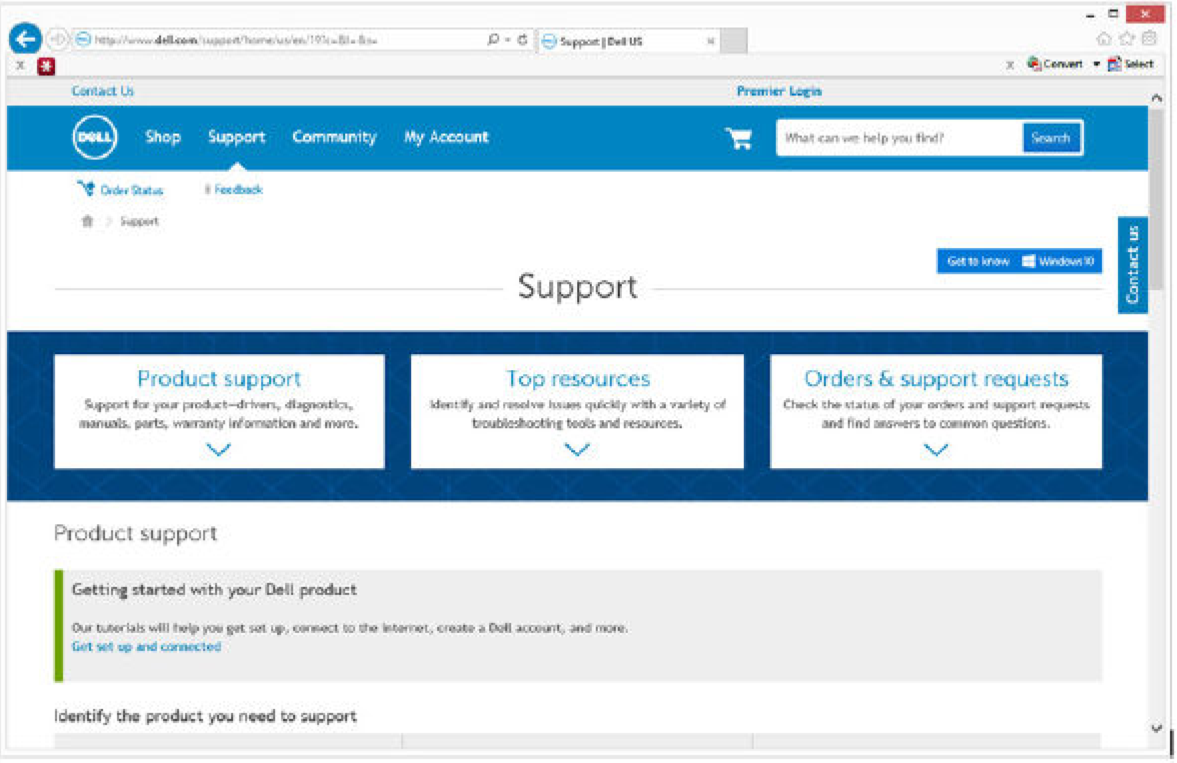
# Dell ControlVault Drivers

## Update Dell ControlVault Drivers and Firmware

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

### Download Latest Drivers

1 Go to support.dell.com.



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

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

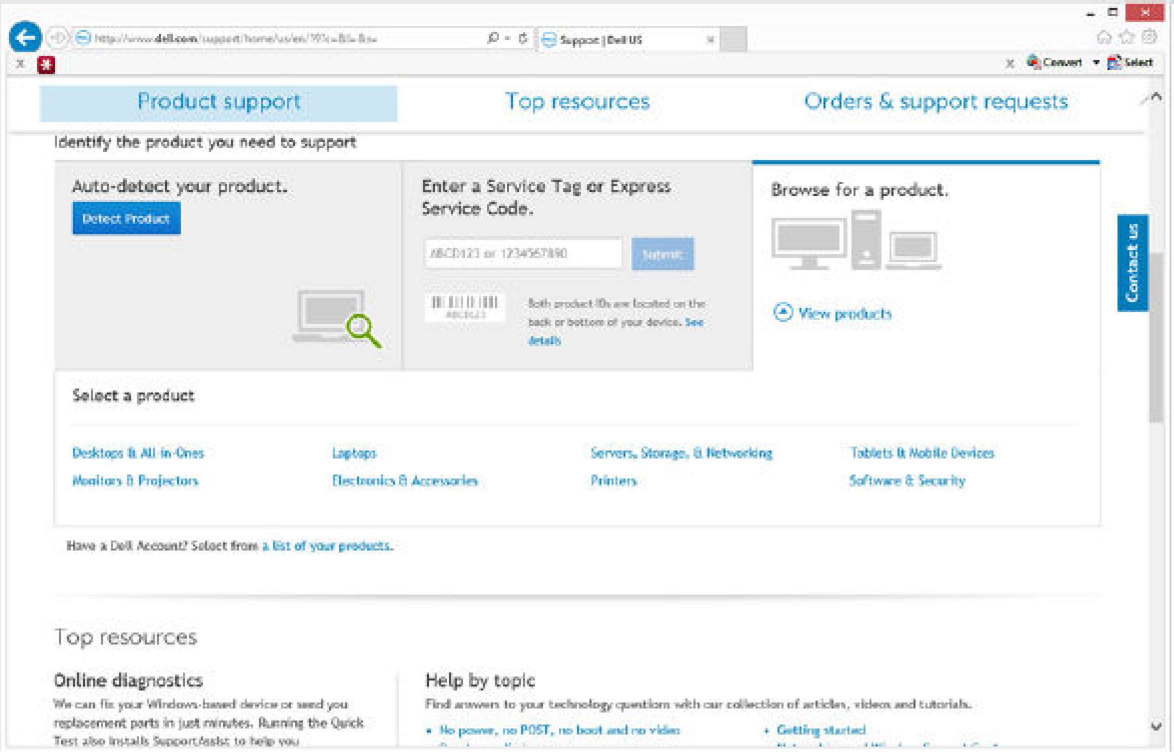
Check the status of your orders and support requests and find answers to common questions.

Getting started with your Dell product

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

Identify the product you need to support

2 Select your computer model.



Identify the product you need to support

Auto-detect your product.

Enter a Service Tag or Express Service Code.

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

Browse for a product.

Select a product

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

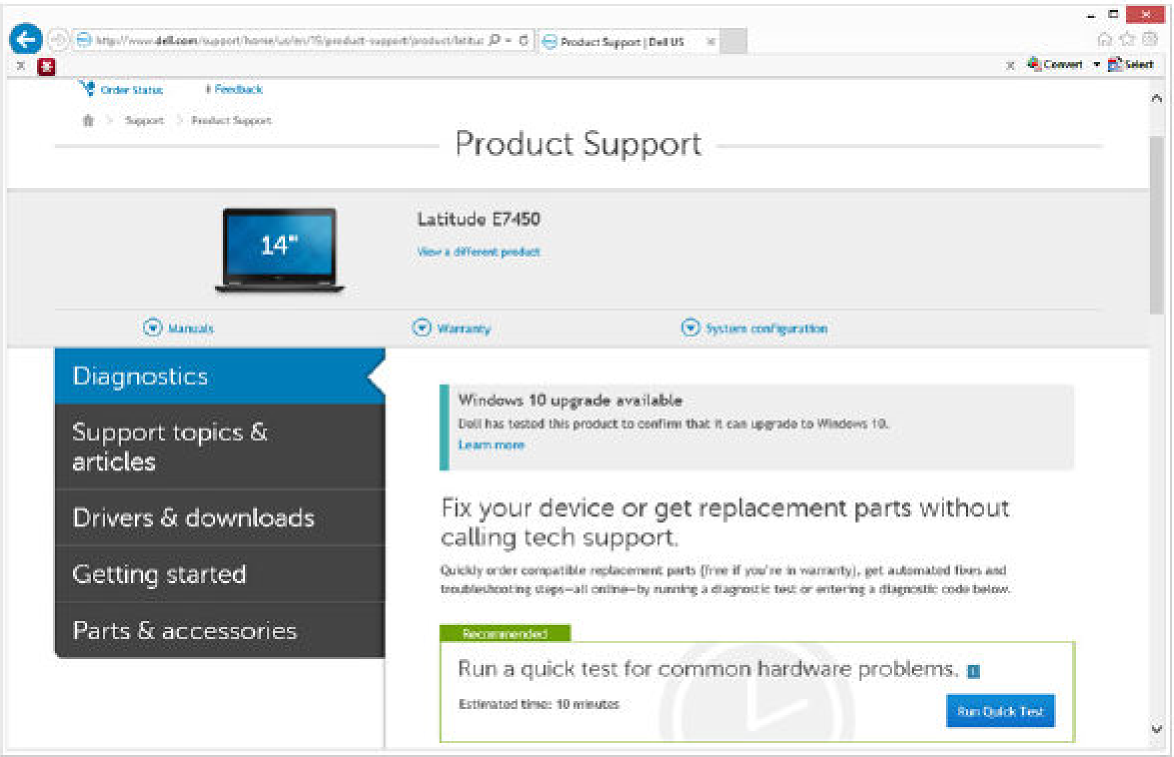
Top resources

Online diagnostics

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

Help by topic

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



Product Support

Latitude E7450

Windows 10 upgrade available

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

Learn more

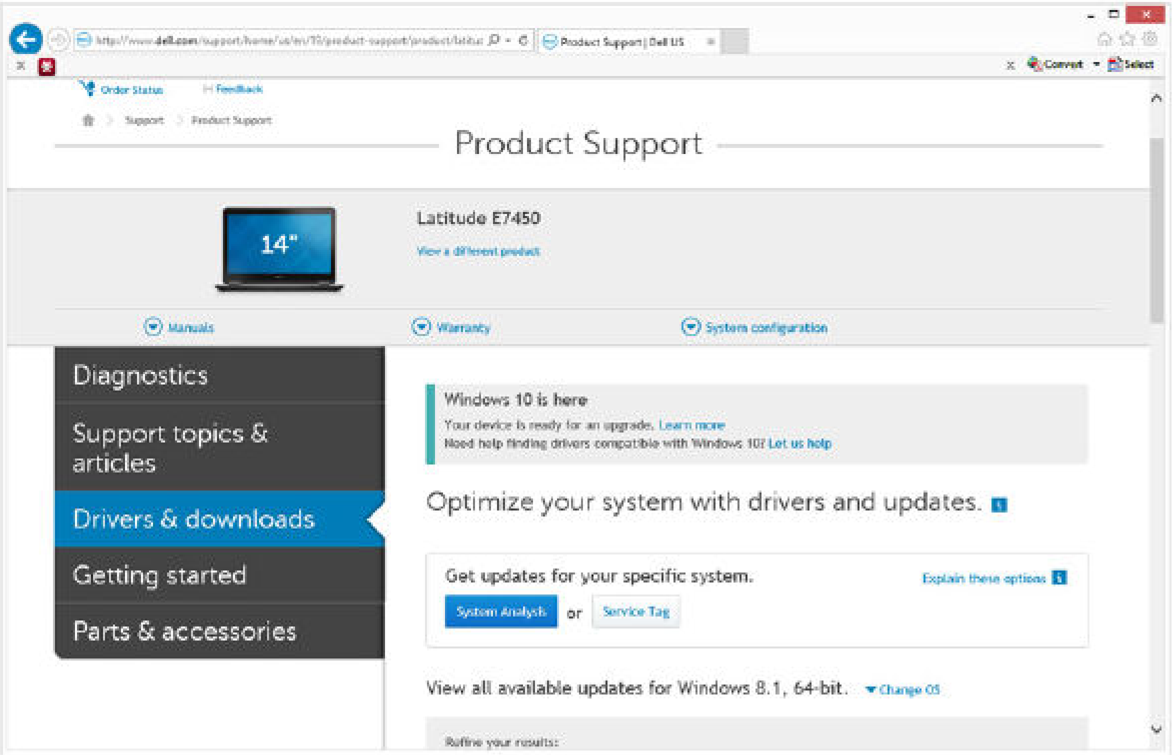
Fix your device or get replacement parts without calling tech support.

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

Run a quick test for common hardware problems.

Estimated time: 10 minutes

3 Select **Drivers & Downloads**.



Windows 10 is here

Your device is ready for an upgrade. Learn more

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

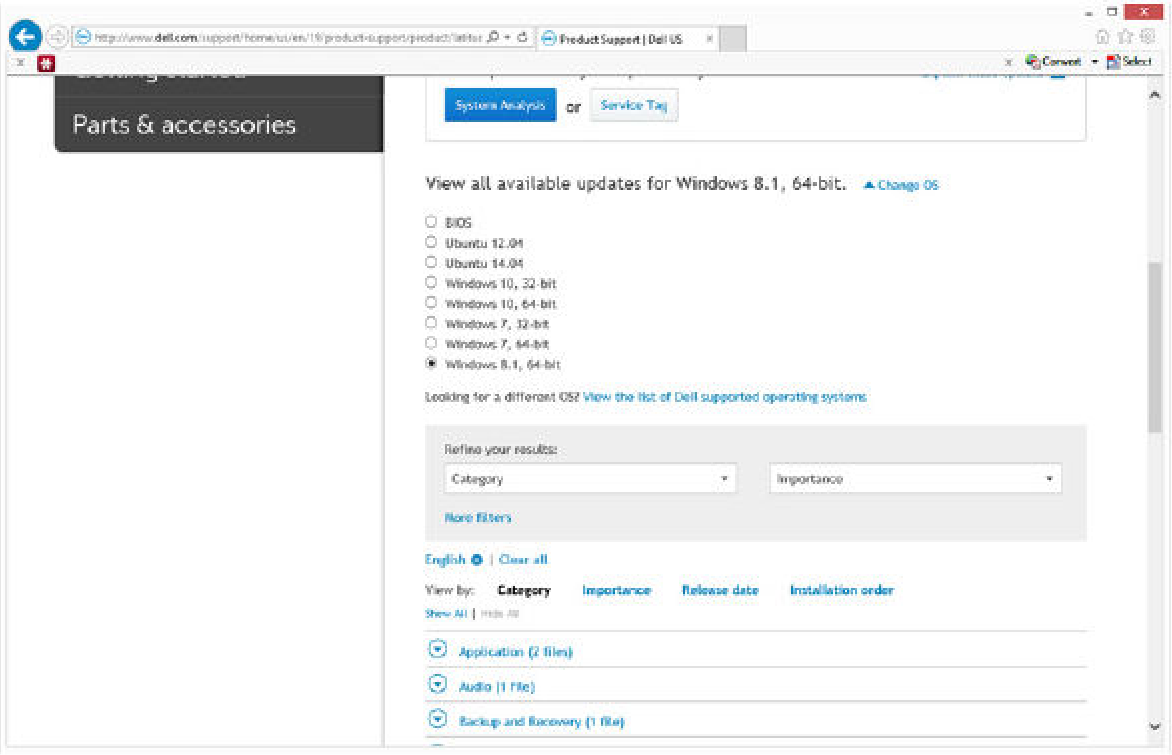
Optimize your system with drivers and updates.

Get updates for your specific system.

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

Refine your results:

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


http://www.dell.com/support/home/us/en/19/product-support/product/latitu
Product Support | Dell US
Convert
Select
Parts & accessories
System Analysis
or
Service Tag

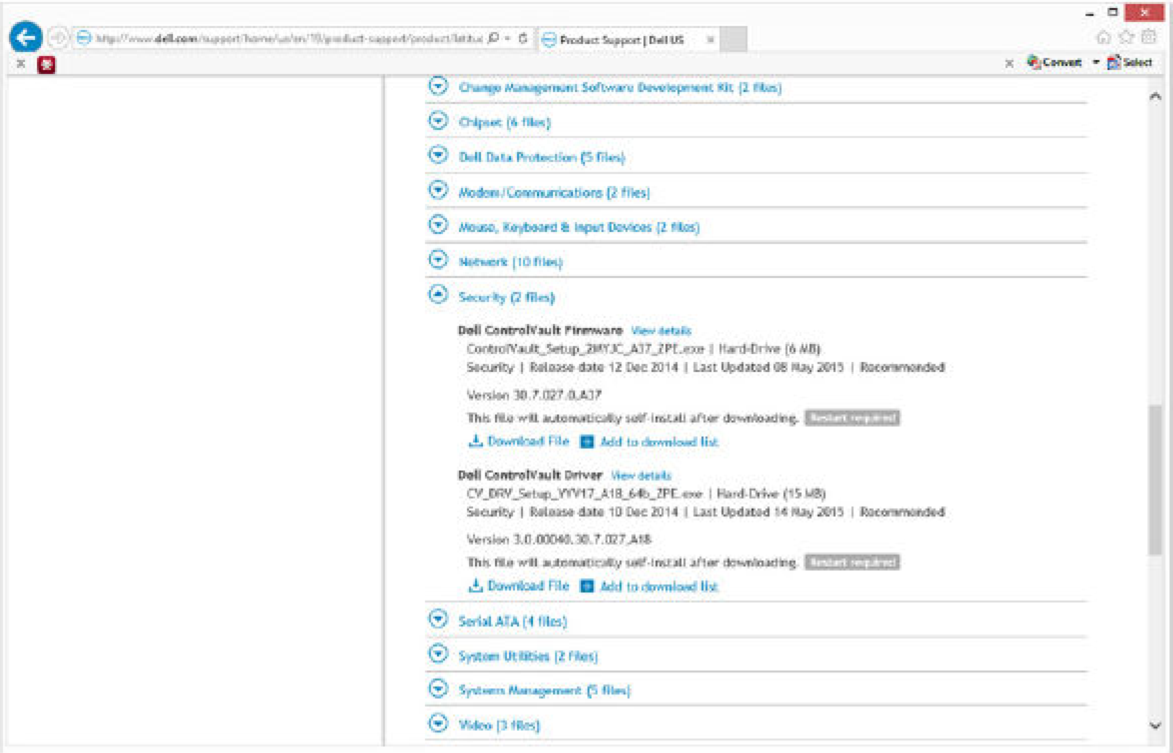
View all available updates for Windows 8.1, 64-bit.

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

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

Refine your results:

5 Expand the **Security** category.



Change Management Software Development Kit (2 files)

Chipset (6 files)

Dell Data Protection (5 files)

Modem/Communications (2 files)

Mouse, Keyboard & Input Devices (2 files)

Network (10 files)

Security (2 files)

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

Version 30.7.027.0,A37

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

Download File  Add to download list

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

Version 3.0.00040.30.7.027,A18

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

Download File  Add to download list

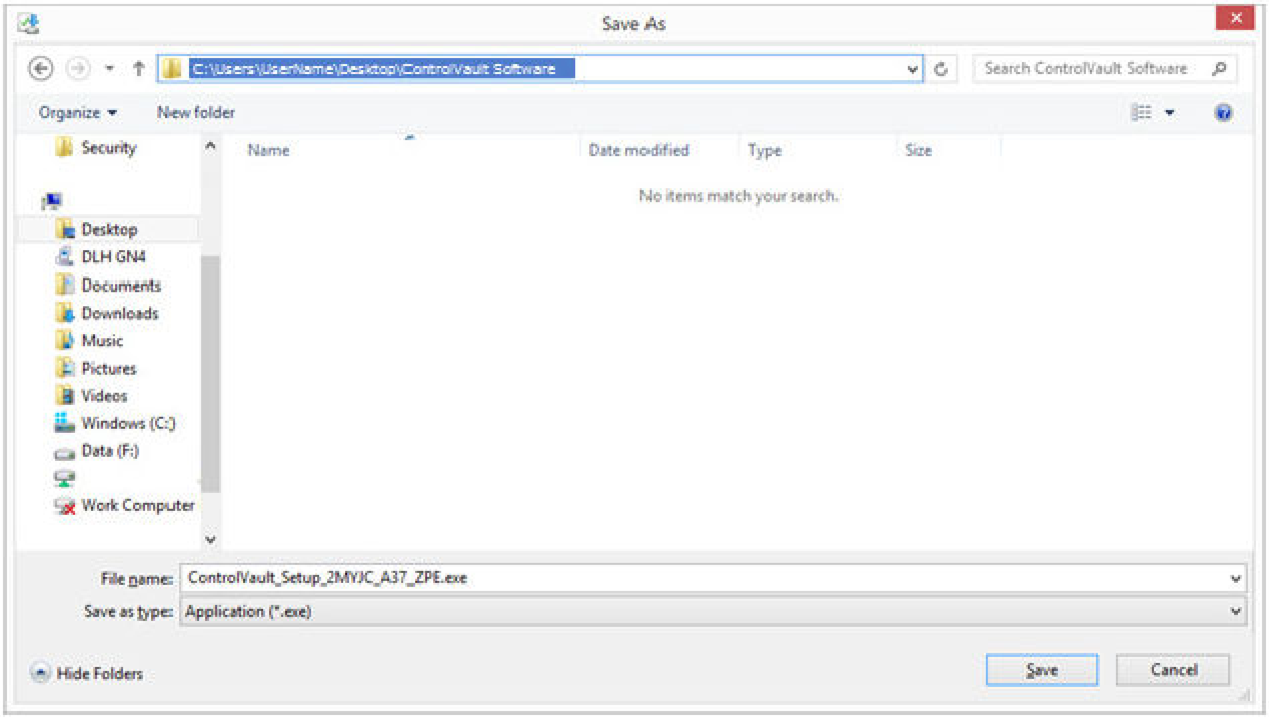
Serial ATA (4 files)

System Utilities (2 files)

Systems Management (5 files)

Video (3 files)

6 Download and save the Dell ControlVault Drivers.



C:\Users\UserName\Desktop\ControlVault Software

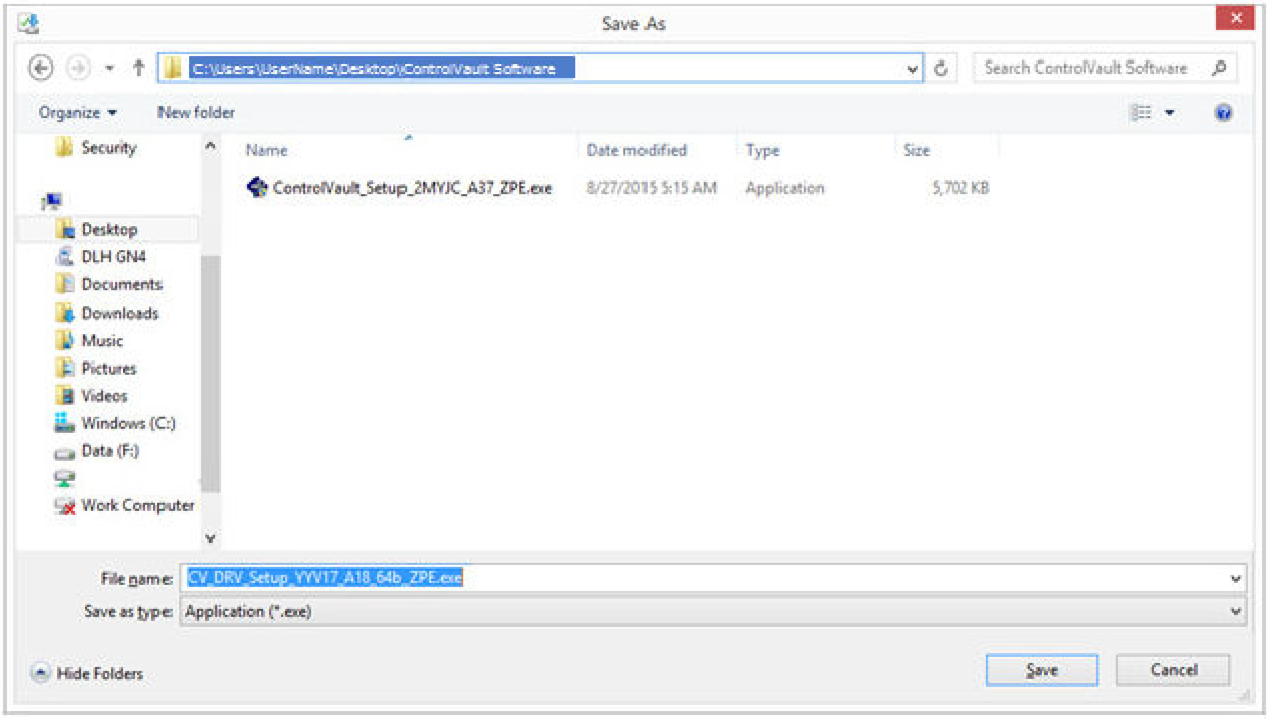
Search ControlVault Software

No items match your search.

File name: ControlVault_Setup_2MYJC_A37_ZPE.exe

Save as type: Application (*.exe)

7 Download and save the Dell ControlVault Firmware.



C:\Users\UserName\Desktop\ControlVault Software

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

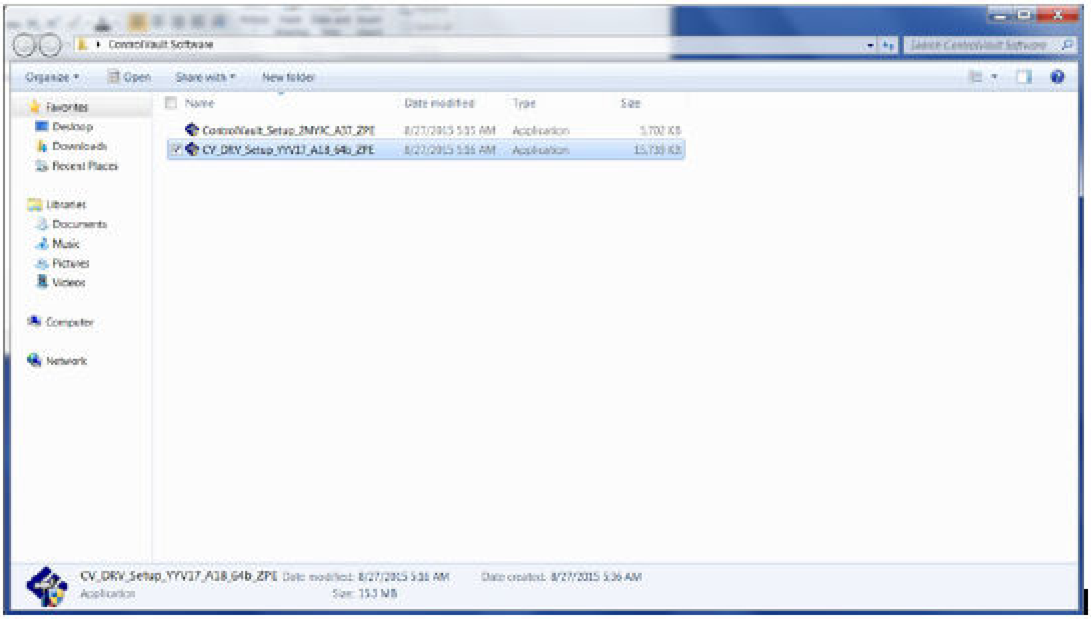
File name: CV_DRV_Setup_YYV17_A18_64b_ZPE.exe

Save as type: Application (*.exe)

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

### Install Dell ControlVault Driver

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



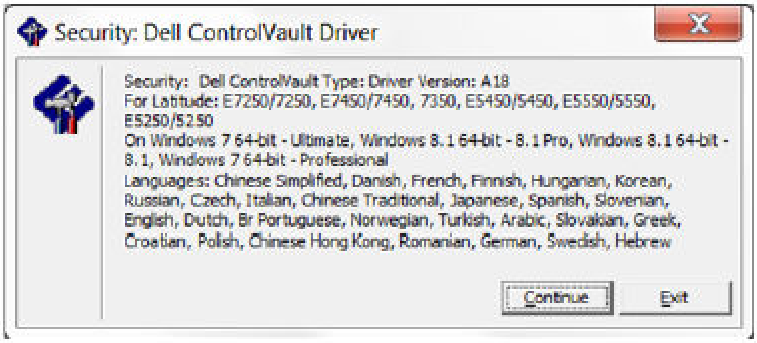
| Name | Date modified | Type | Size |
|---|---|---|---|
| ControlVault_Setup_2MYJC_A37_ZPE | 8/27/2015 5:35 AM | Application | 5,702 KB |
| CV_DRV_Setup_YYV17_A18_64b_ZPE | 8/27/2015 5:36 AM | Application | 15,730 KB |

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

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

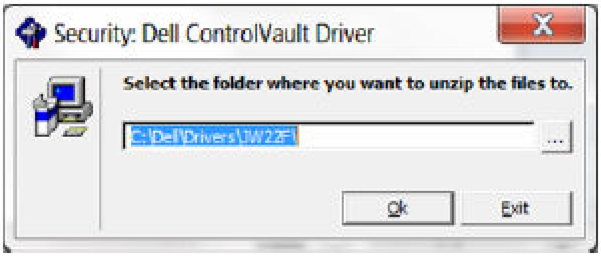
> **TIP:**
>
> Be sure to install the driver first. The filename of the driver *at the time of this document creation* is ControlVault_Setup_2MYJC_A37_ZPE.exe.

3 Click **Continue** to begin.



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

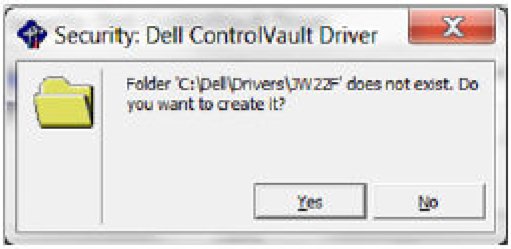
4 Click **Ok** to unzip the driver files in the default location of C:\Dell\Drivers\<New Folder>.



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

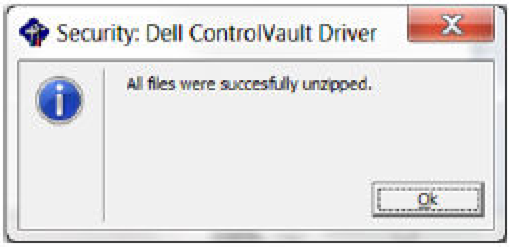
C:\Dell\Drivers\JW22F\

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



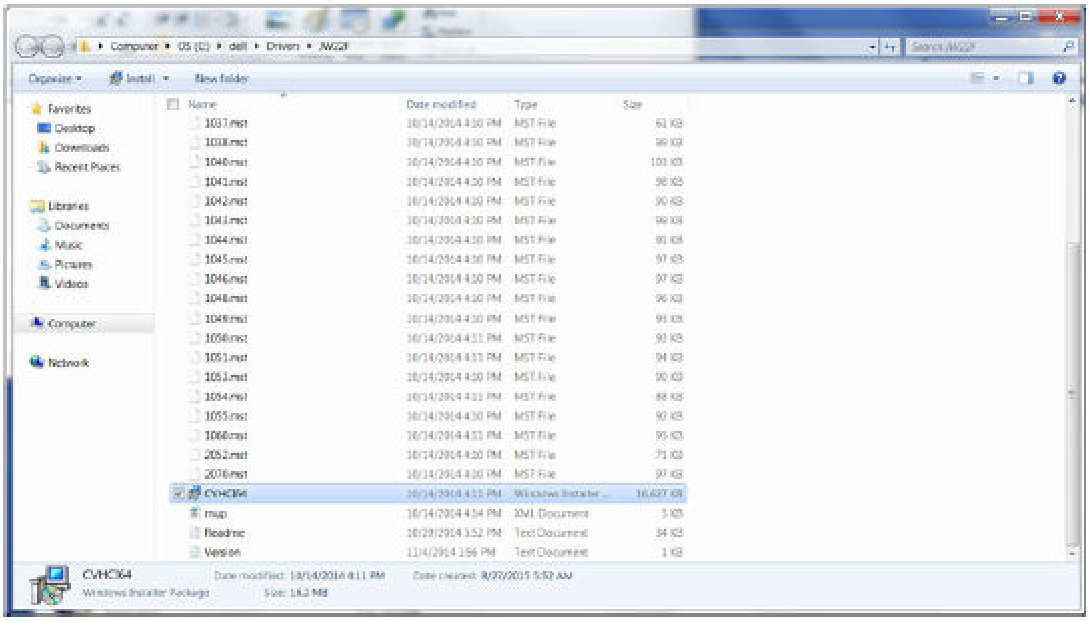
Folder 'C:\Dell\Drivers\JW22F' does not exist. Do you want to create it?

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



All files were succesfully unzipped.

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

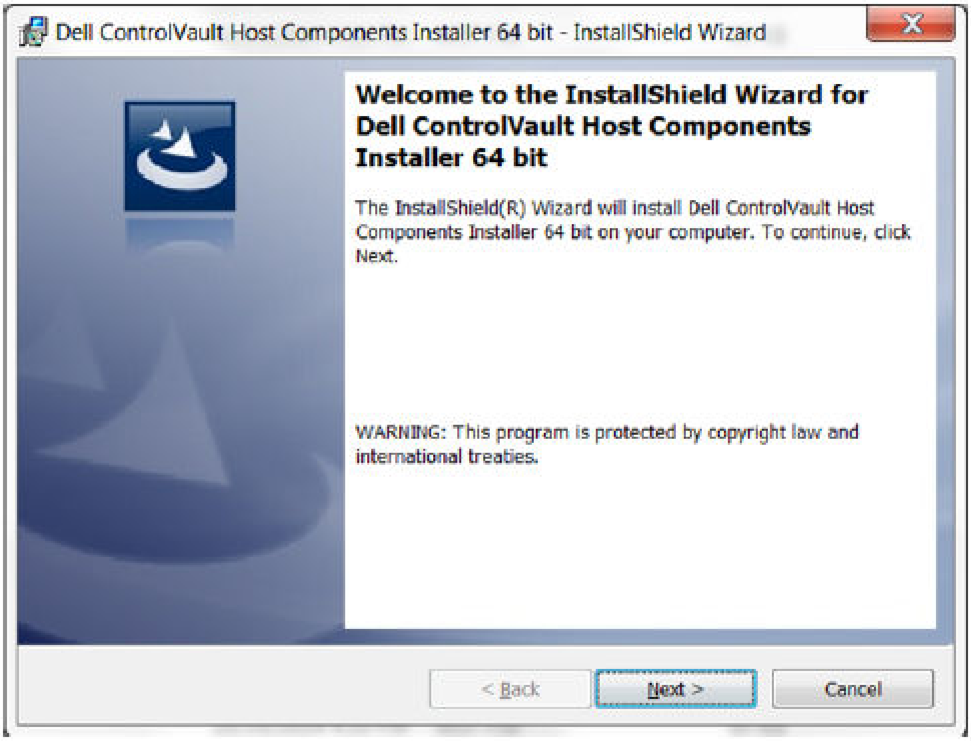


| Name | Date modified | Type | Size |
|---|---|---|---|
| 1037.mst | 10/14/2014 4:10 PM | MST File | 61 KB |
| 1038.mst | 10/14/2014 4:10 PM | MST File | 99 KB |
| 1040.mst | 10/14/2014 4:10 PM | MST File | 103 KB |
| 1041.mst | 10/14/2014 4:10 PM | MST File | 98 KB |
| 1042.mst | 10/14/2014 4:10 PM | MST File | 90 KB |
| 1043.mst | 10/14/2014 4:10 PM | MST File | 99 KB |
| 1044.mst | 10/14/2014 4:10 PM | MST File | 91 KB |
| 1045.mst | 10/14/2014 4:10 PM | MST File | 97 KB |
| 1046.mst | 10/14/2014 4:10 PM | MST File | 97 KB |
| 1048.mst | 10/14/2014 4:10 PM | MST File | 96 KB |
| 1049.mst | 10/14/2014 4:10 PM | MST File | 93 KB |
| 1050.mst | 10/14/2014 4:11 PM | MST File | 93 KB |
| 1051.mst | 10/14/2014 4:11 PM | MST File | 94 KB |
| 1053.mst | 10/14/2014 4:10 PM | MST File | 90 KB |
| 1054.mst | 10/14/2014 4:11 PM | MST File | 88 KB |
| 1055.mst | 10/14/2014 4:10 PM | MST File | 92 KB |
| 1060.mst | 10/14/2014 4:11 PM | MST File | 95 KB |
| 2052.mst | 10/14/2014 4:10 PM | MST File | 71 KB |
| 2076.mst | 10/14/2014 4:10 PM | MST File | 97 KB |
| CVHCI64 | 10/14/2014 4:11 PM | Windows Installer ... | 16,627 KB |
| map | 10/14/2014 4:14 PM | XML Document | 5 KB |
| Readme | 10/29/2014 5:52 PM | Text Document | 34 KB |
| Version | 11/4/2014 1:56 PM | Text Document | 1 KB |

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

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

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

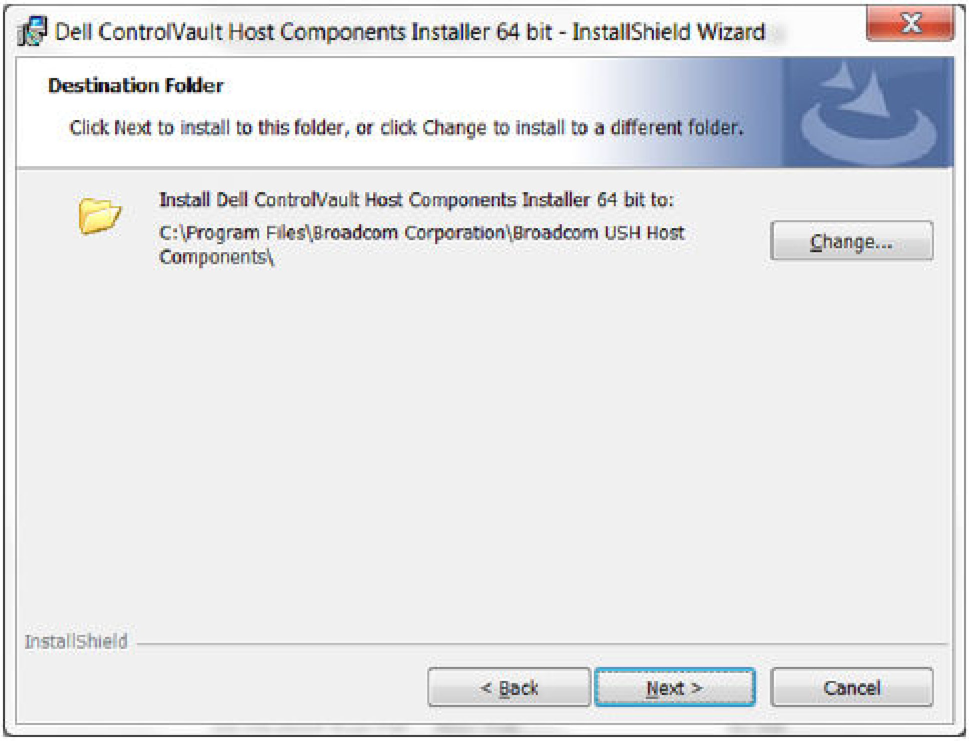

Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard
< Back
Next >
Cancel

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

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

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

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



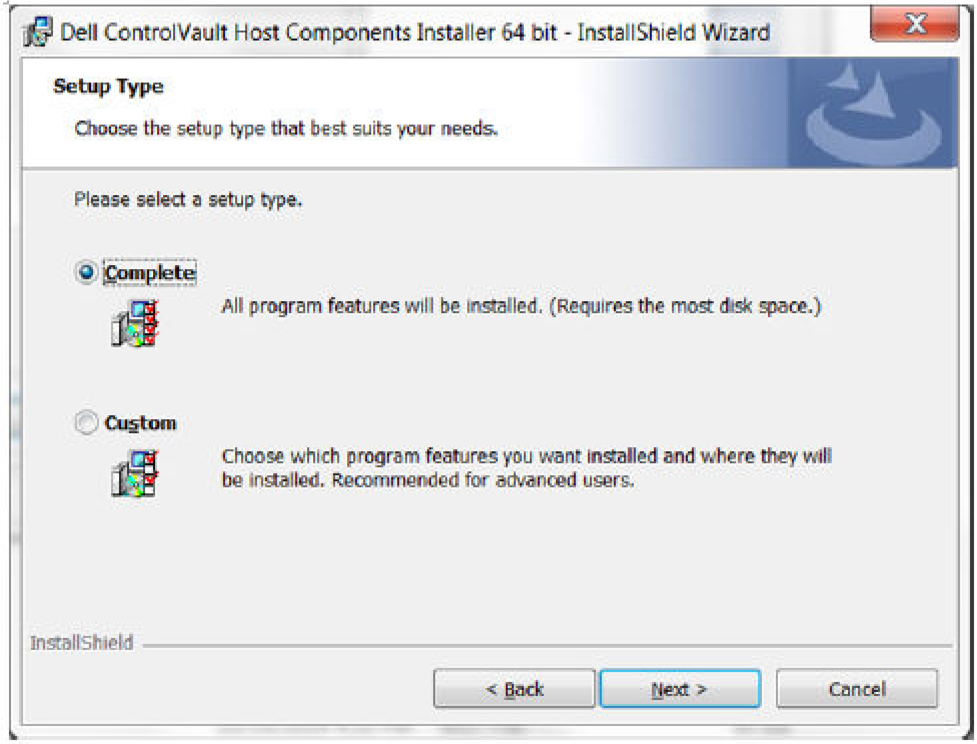
Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

**Destination Folder**

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

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

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

**Setup Type**

Choose the setup type that best suits your needs.

Please select a setup type.

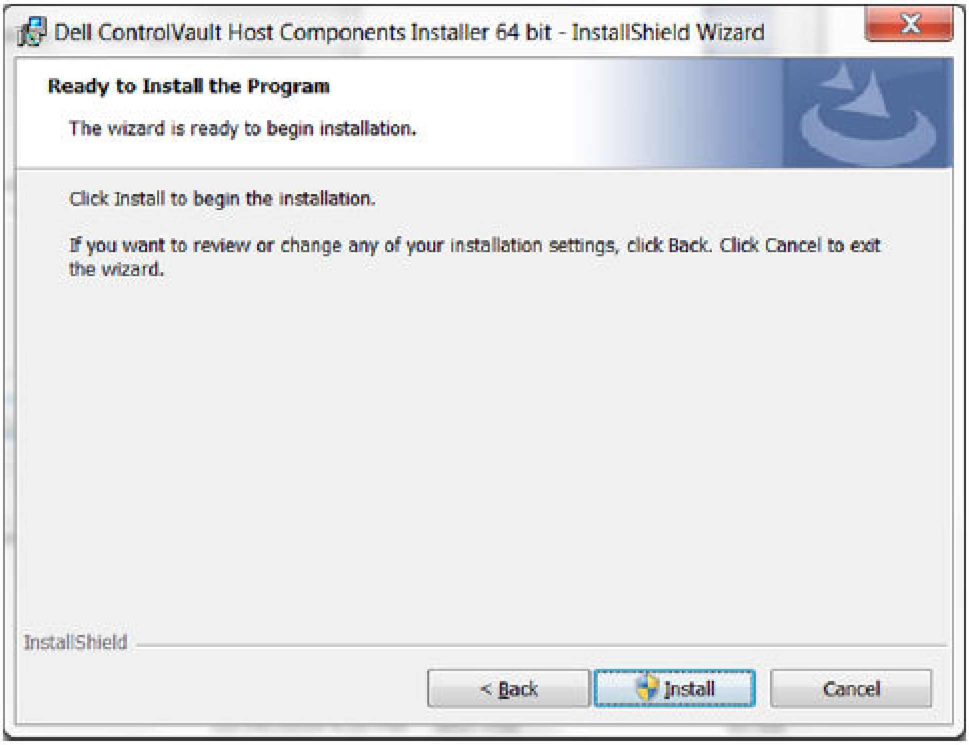
● Complete

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

○ Custom

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

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

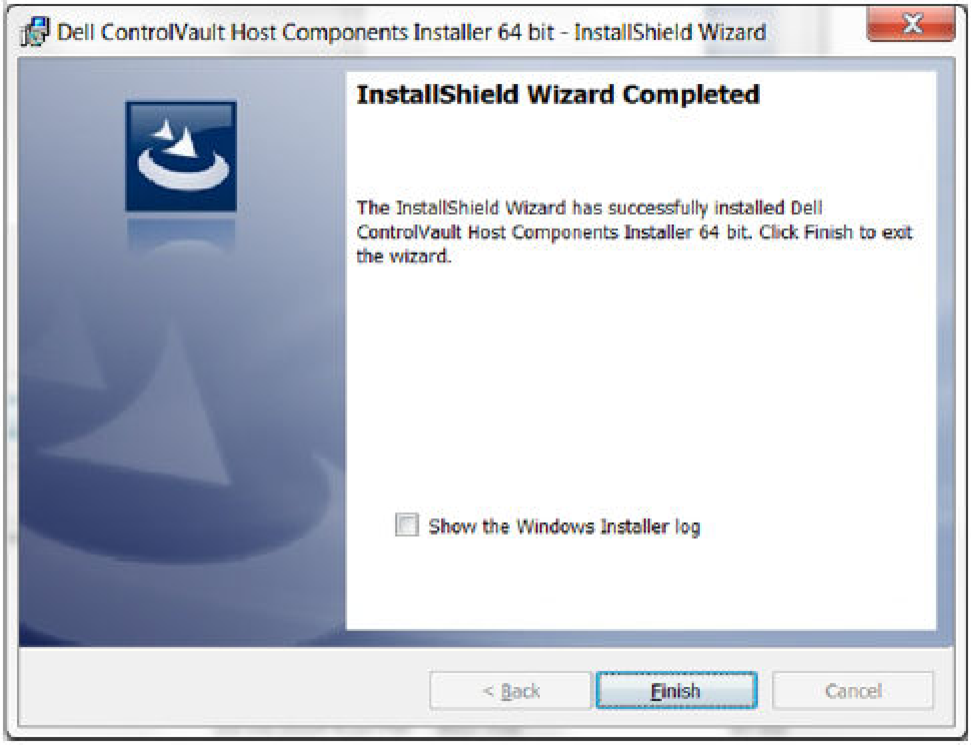
**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

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

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



Dell ControlVault Host Components Installer 64 bit - InstallShield Wizard

**InstallShield Wizard Completed**

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

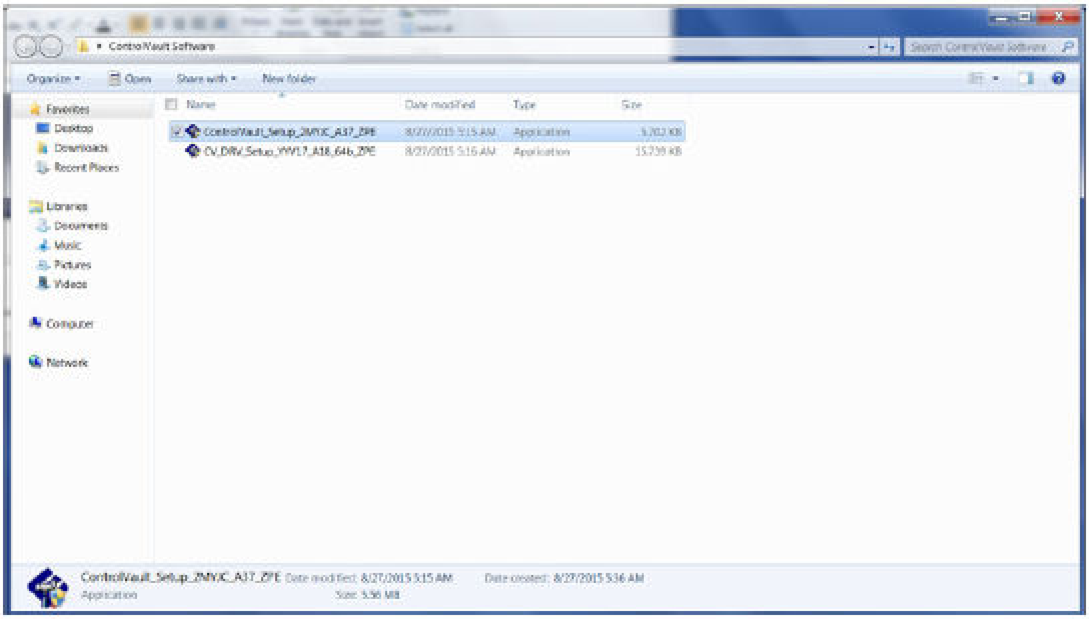
□ Show the Windows Installer log

### Verify Driver Installation

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

### Install Dell ControlVault Firmware

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



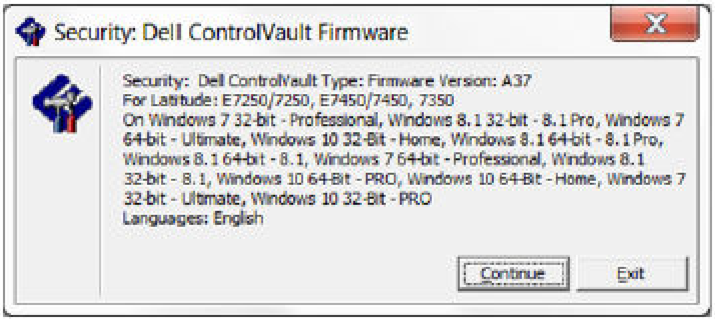
ControlVault Software

| Name | Date modified | Type | Size |
|---|---|---|---|
| ControlVault_Setup_2MYJC_A37_ZPE | 8/27/2015 5:15 AM | Application | 5,702 KB |
| CV_DRV_Setup_YWY17_A18_64b_ZPE | 8/27/2015 5:16 AM | Application | 15,739 KB |

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

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

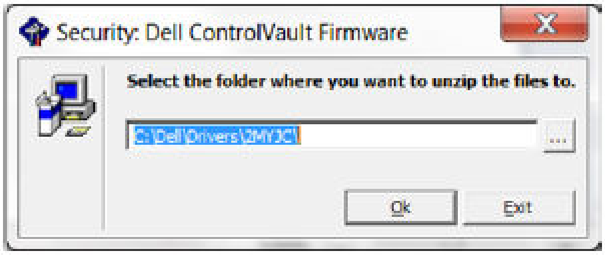
3 Click **Continue** to begin.



Security: Dell ControlVault Firmware

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

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

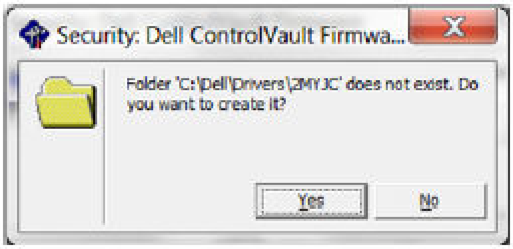


Security: Dell ControlVault Firmware

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

C:\Dell\Drivers\2MYJC\

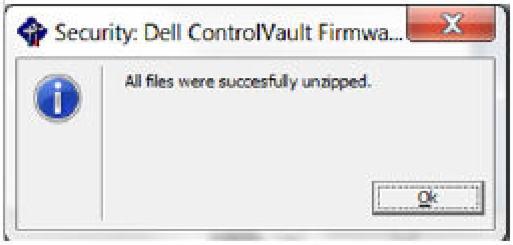
5 Click **Yes** to allow the creation of a new folder.



Security: Dell ControlVault Firmwa...

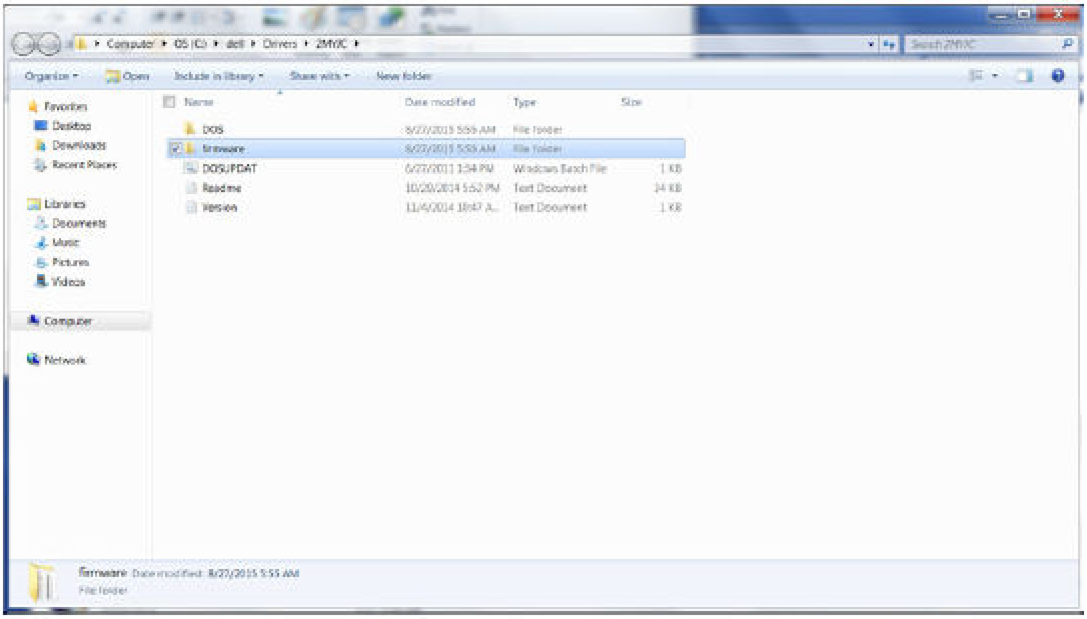
Folder 'C:\Dell\Drivers\2MYJC' does not exist. Do you want to create it?

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



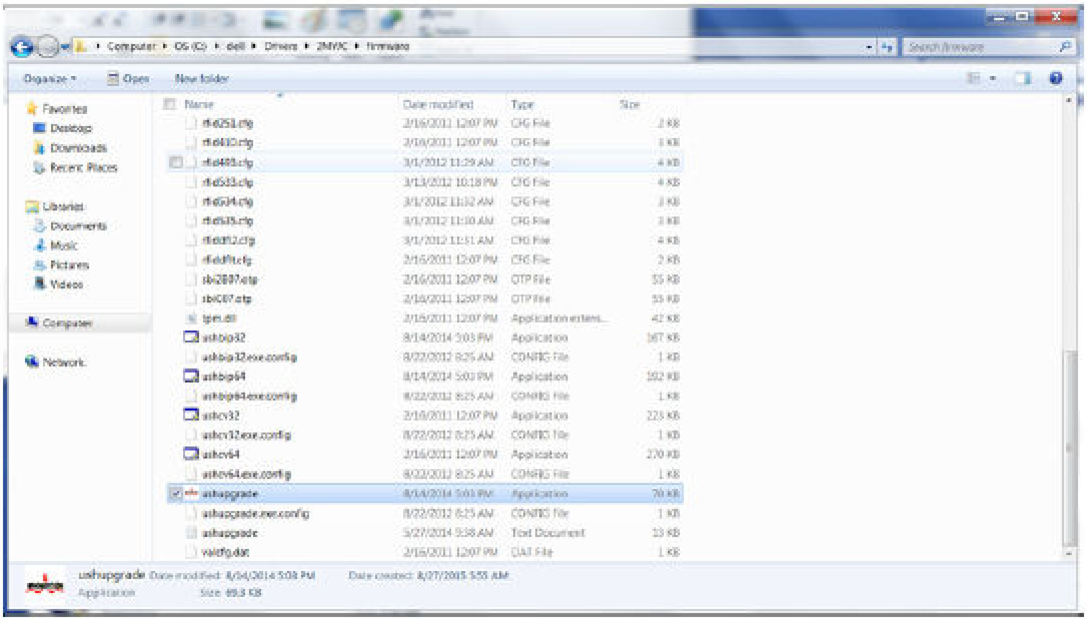
All files were succesfully unzipped.

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



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

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

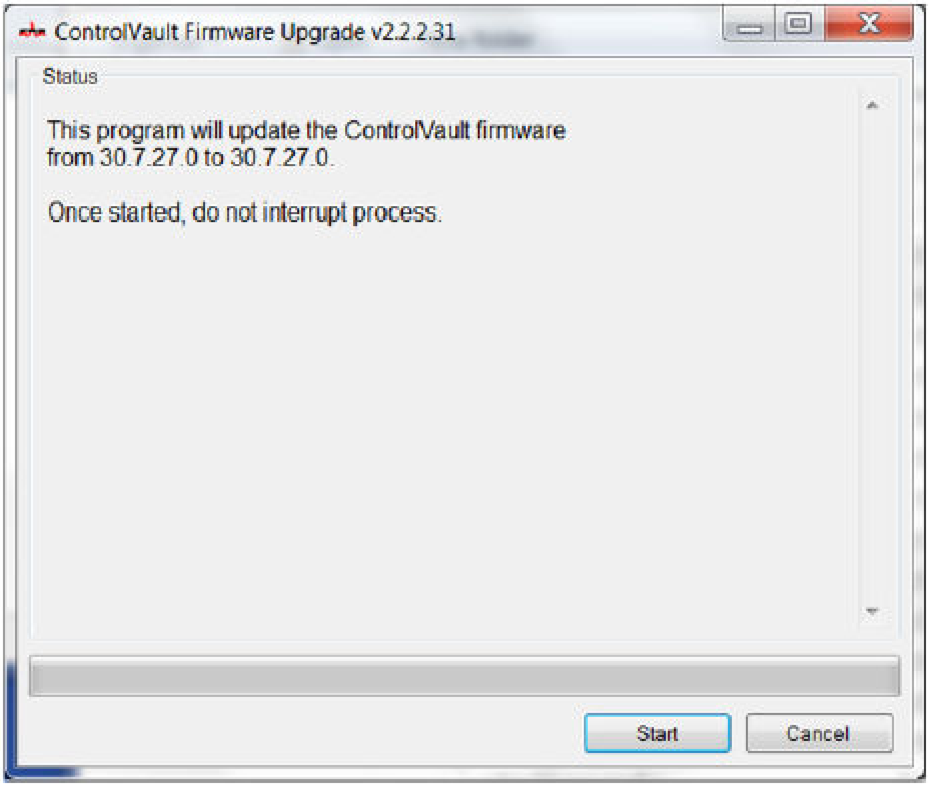


| Name | Date modified | Type | Size |
|---|---|---|---|
| rfid251.cfg | 2/16/2011 12:07 PM | CFG File | 2 KB |
| rfid410.cfg | 2/16/2011 12:07 PM | CFG File | 3 KB |
| rfid488.cfg | 3/1/2012 11:29 AM | CFG File | 4 KB |
| rfid533.cfg | 3/13/2012 10:18 PM | CFG File | 4 KB |
| rfid534.cfg | 3/1/2012 11:32 AM | CFG File | 3 KB |
| rfid535.cfg | 3/1/2012 11:30 AM | CFG File | 3 KB |
| rfiddf12.cfg | 3/1/2012 11:31 AM | CFG File | 4 KB |
| rfiddflt.cfg | 2/16/2011 12:07 PM | CFG File | 2 KB |
| sbi2887.otp | 2/16/2011 12:07 PM | OTP File | 55 KB |
| sbiC07.otp | 2/16/2011 12:07 PM | OTP File | 55 KB |
| tpm.dll | 2/16/2011 12:07 PM | Application extens... | 42 KB |
| ushbip32 | 8/14/2014 5:03 PM | Application | 167 KB |
| ushbip32.exe.config | 8/22/2012 8:25 AM | CONFIG File | 1 KB |
| ushbip64 | 8/14/2014 5:03 PM | Application | 192 KB |
| ushbip64.exe.config | 8/22/2012 8:25 AM | CONFIG File | 1 KB |
| ushcv32 | 2/16/2011 12:07 PM | Application | 223 KB |
| ushcv32.exe.config | 8/22/2012 8:25 AM | CONFIG File | 1 KB |
| ushcv64 | 2/16/2011 12:07 PM | Application | 270 KB |
| ushcv64.exe.config | 8/22/2012 8:25 AM | CONFIG File | 1 KB |
| ☑ ushupgrade | 8/14/2014 5:03 PM | Application | 70 KB |
| ushupgrade.exe.config | 8/22/2012 8:25 AM | CONFIG File | 1 KB |
| ushupgrade | 5/27/2014 9:38 AM | Text Document | 13 KB |
| vaidfg.dat | 2/16/2011 12:07 PM | DAT File | 1 KB |

ushupgrade Date modified: 8/14/2014 5:08 PM Date created: 8/27/2015 5:55 AM
Application Size: 69.3 KB

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

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



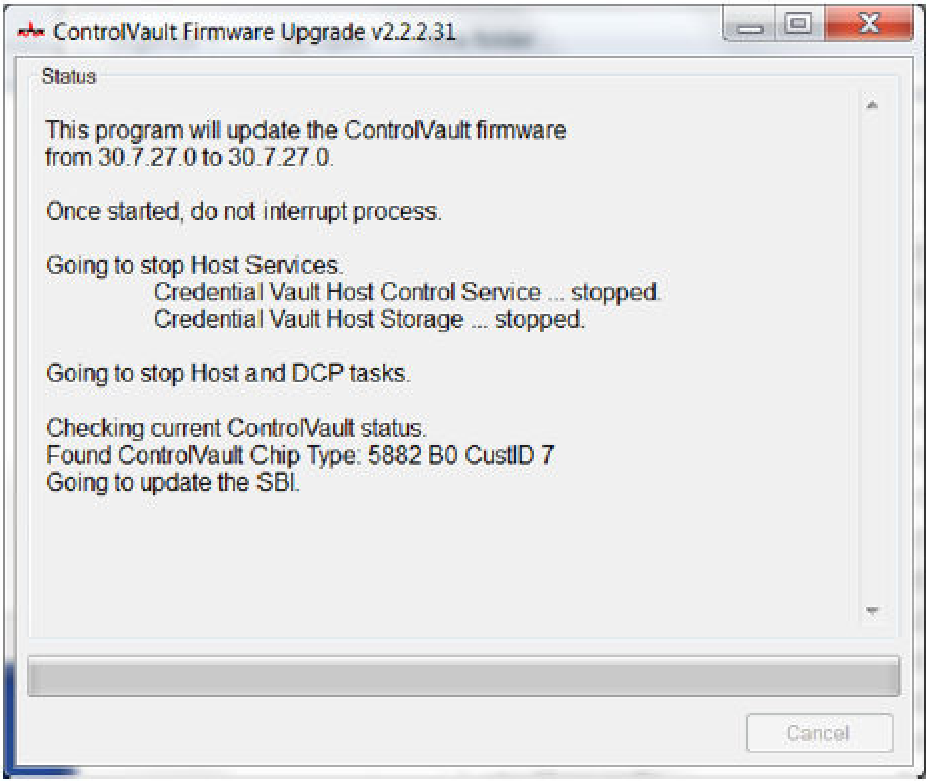
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

Once started, do not interrupt process.

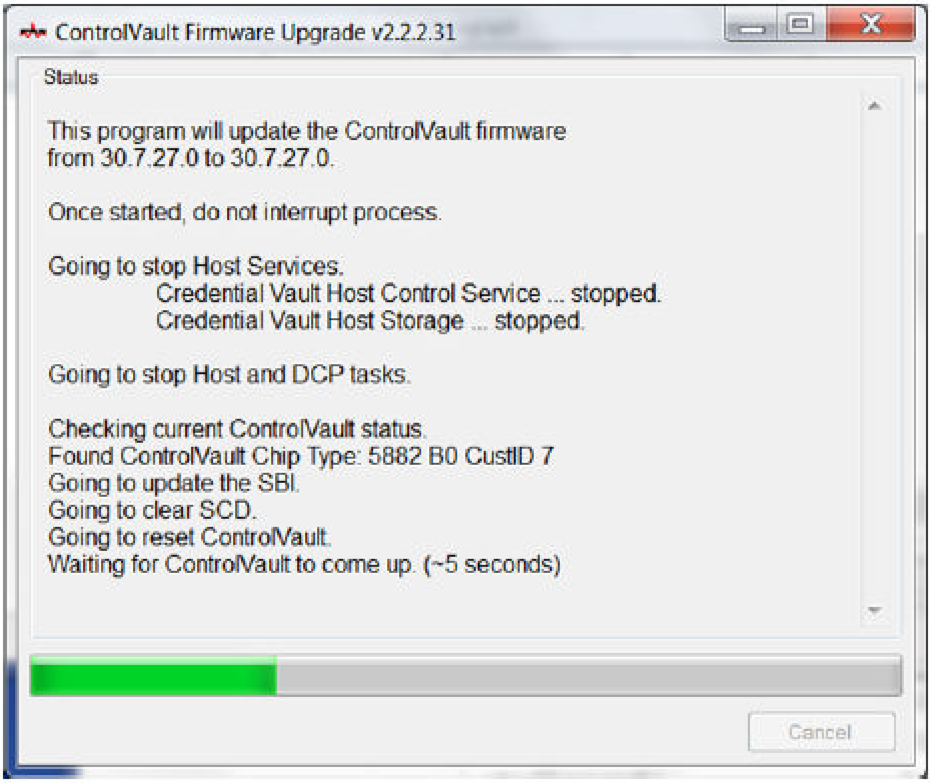
**IMPORTANT:**

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

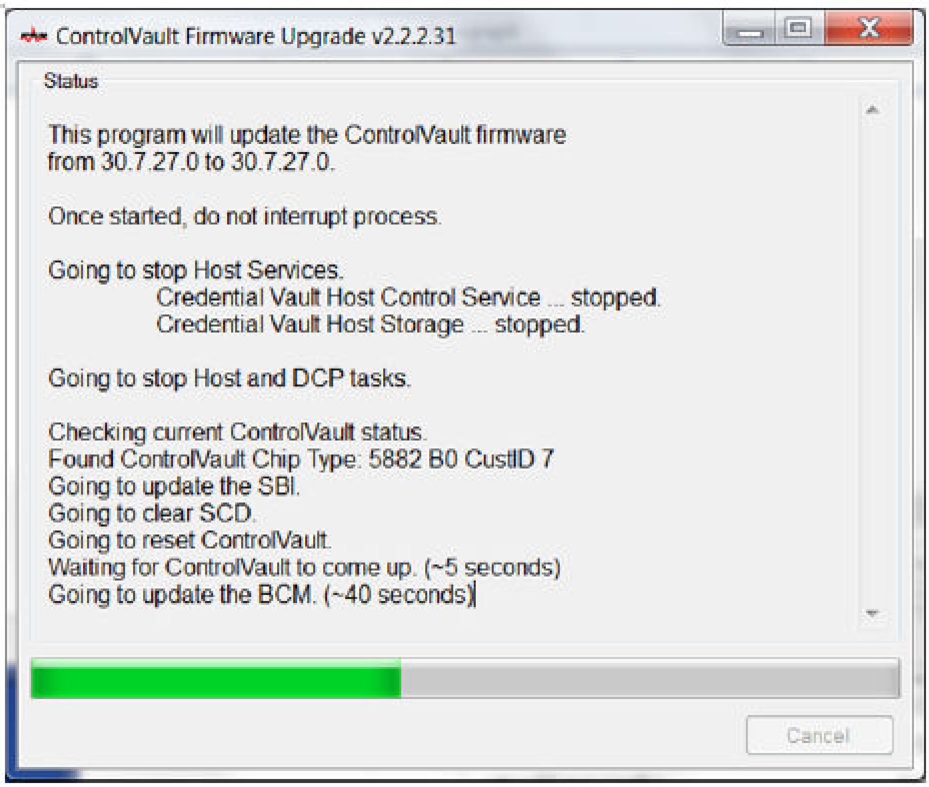
Several status messages display.



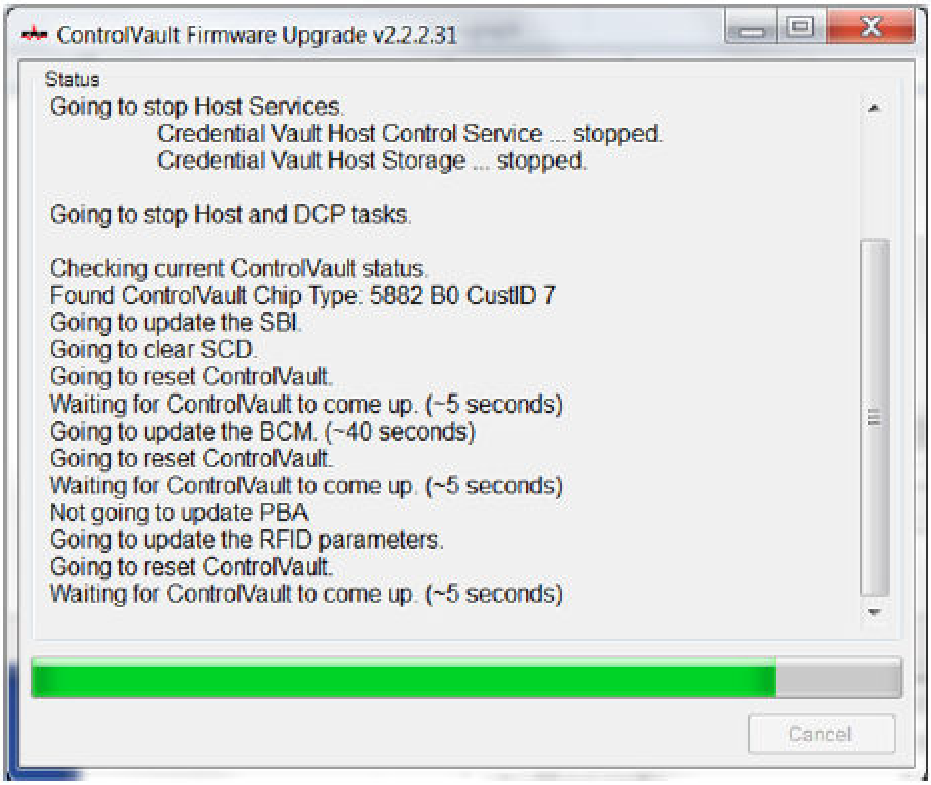
```
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

Once started, do not interrupt process.

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

Going to stop Host and DCP tasks.

Checking current ControlVault status.
Found ControlVault Chip Type: 5882 B0 CustID 7
Going to update the SBI.
```



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

Once started, do not interrupt process.

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

Going to stop Host and DCP tasks.

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

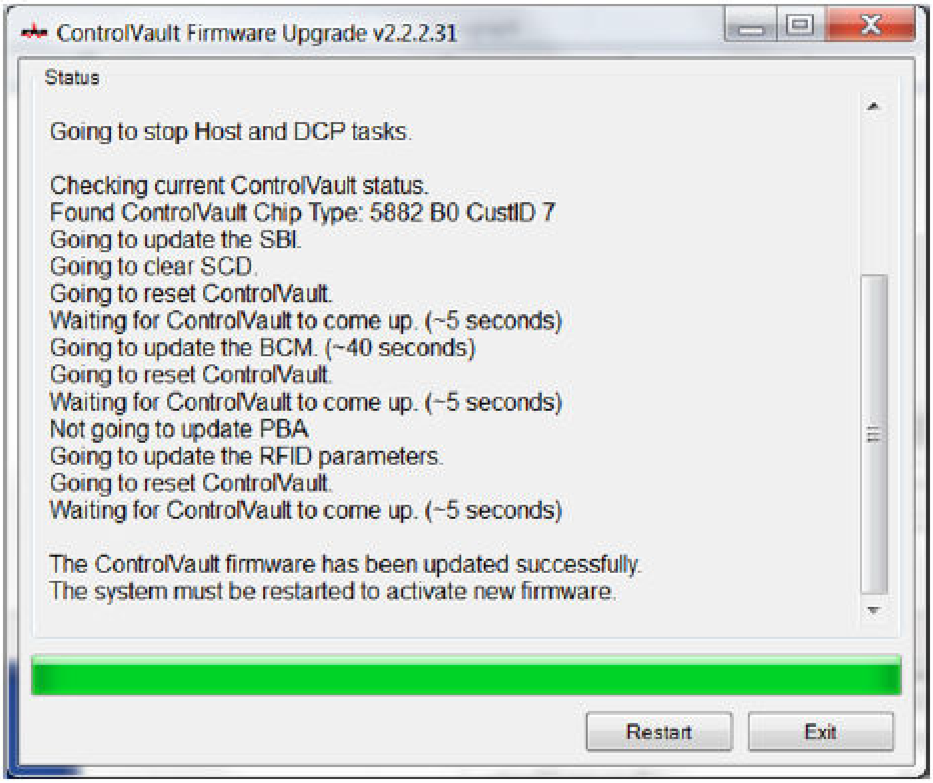


```
This program will update the ControlVault firmware
from 30.7.27.0 to 30.7.27.0.

Once started, do not interrupt process.

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

Going to stop Host and DCP tasks.

Checking current ControlVault status.
Found ControlVault Chip Type: 5882 B0 CustID 7
Going to update the SBI.
Going to clear SCD.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Going to update the BCM. (~40 seconds)
```



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

Going to stop Host and DCP tasks.

Checking current ControlVault status.
Found ControlVault Chip Type: 5882 B0 CustID 7
Going to update the SBI.
Going to clear SCD.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Going to update the BCM. (~40 seconds)
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Not going to update PBA
Going to update the RFID parameters.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
```

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



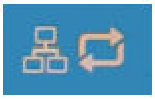
```
Going to stop Host and DCP tasks.

Checking current ControlVault status.
Found ControlVault Chip Type: 5882 B0 CustID 7
Going to update the SBI.
Going to clear SCD.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Going to update the BCM. (~40 seconds)
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)
Not going to update PBA
Going to update the RFID parameters.
Going to reset ControlVault.
Waiting for ControlVault to come up. (~5 seconds)

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

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

# UEFI Computers

## Troubleshoot Network Connection

- In order for preboot authentication to succeed on a computer with UEFI firmware, the PBA mode must have network connectivity. By default, computers with UEFI firmware do not have network connectivity until the operating system is loaded, which occurs after PBA mode. If the computer procedure outlined in Pre-Installation Configuration for UEFI Computers is successful and is configured properly, the network connection icon displays on the preboot authentication screen when the computer is connected to the network.



- Check the network cable to ensure it is connected to the computer if the network connection icon still does not display during preboot authentication. Restart the computer to restart PBA mode if it was not connected or was loose.

# TPM and BitLocker

## TPM and BitLocker Error Codes

| Constant/Value | Description |
|---|---|
| TPM_E_ERROR_MASK<br>0x80280000 | This is an error mask to convert TPM hardware errors to win errors. |
| TPM_E_AUTHFAIL<br>0x80280001 | Authentication failed. |
| TPM_E_BADINDEX<br>0x80280002 | The index to a PCR, DIR or other register is incorrect. |
| TPM_E_BAD_PARAMETER<br>0x80280003 | One or more parameters is bad. |
| TPM_E_AUDITFAILURE<br>0x80280004 | An operation completed successfully but the auditing of that operation failed. |
| TPM_E_CLEAR_DISABLED<br>0x80280005 | The clear disable flag is set and all clear operations now require physical access. |
| TPM_E_DEACTIVATED<br>0x80280006 | Activate the TPM. |
| TPM_E_DISABLED<br>0x80280007 | Enable the TPM. |
| TPM_E_DISABLED_CMD | The target command has been disabled. |

| Constant/Value | Description |
|---|---|
| 0x80280008 | |
| TPM_E_FAIL<br>0x80280009 | The operation failed. |
| TPM_E_BAD_ORDINAL<br>0x8028000A | The ordinal was unknown or inconsistent. |
| TPM_E_INSTALL_DISABLED<br>0x8028000B | The ability to install an owner is disabled. |
| TPM_E_INVALID_KEYHANDLE<br>0x8028000C | The key handle cannot be interpreted. |
| TPM_E_KEYNOTFOUND<br>0x8028000D | The key handle points to an invalid key. |
| TPM_E_INAPPROPRIATE_ENC<br>0x8028000E | Unacceptable encryption scheme. |
| TPM_E_MIGRATEFAIL<br>0x8028000F | Migration authorization failed. |
| TPM_E_INVALID_PCR_INFO<br>0x80280010 | PCR information could not be interpreted. |
| TPM_E_NOSPACE<br>0x80280011 | No room to load key. |
| TPM_E_NOSRK<br>0x80280012 | There is no Storage Root Key (SRK) set. |
| TPM_E_NOTSEALED_BLOB<br>0x80280013 | An encrypted blob is invalid or was not created by this TPM. |
| TPM_E_OWNER_SET<br>0x80280014 | The TPM already has an owner. |
| TPM_E_RESOURCES<br>0x80280015 | The TPM has insufficient internal resources to perform the requested action. |
| TPM_E_SHORTRANDOM<br>0x80280016 | A random string was too short. |
| TPM_E_SIZE | The TPM does not have the space to perform the operation. |

| Constant/Value | Description |
|---|---|
| 0x80280017 | |
| TPM_E_WRONGPCRVAL<br>0x80280018 | The named PCR value does not match the current PCR value. |
| TPM_E_BAD_PARAM_SIZE<br>0x80280019 | The paramSize argument to the command has the incorrect value |
| TPM_E_SHA_THREAD<br>0x8028001A | There is no existing SHA-1 thread. |
| TPM_E_SHA_ERROR<br>0x8028001B | The calculation is unable to proceed because the existing SHA-1 thread has already encountered an error. |
| TPM_E_FAILEDSELFTEST<br>0x8028001C | The TPM hardware device reported a failure during its internal self test. Try restarting the computer to resolve the problem. If the problem continues, you might need to replace your TPM hardware or motherboard. |
| TPM_E_AUTH2FAIL<br>0x8028001D | The authorization for the second key in a 2 key function failed authorization. |
| TPM_E_BADTAG<br>0x8028001E | The tag value sent to for a command is invalid. |
| TPM_E_IOERROR<br>0x8028001F | An IO error occurred transmitting information to the TPM. |
| TPM_E_ENCRYPT_ERROR<br>0x80280020 | The encryption process had a problem. |
| TPM_E_DECRYPT_ERROR<br>0x80280021 | The decryption process did not complete. |
| TPM_E_INVALID_AUTHHANDLE<br>0x80280022 | An invalid handle was used. |
| TPM_E_NO_ENDORSEMENT<br>0x80280023 | The TPM does not have an Endorsement Key (EK) installed. |
| TPM_E_INVALID_KEYUSAGE<br>0x80280024 | The usage of a key is not allowed. |
| TPM_E_WRONG_ENTITYTYPE<br>0x80280025 | The submitted entity type is not allowed. |

| Constant/Value | Description |
|---|---|
| TPM_E_INVALID_POSTINIT<br>0x80280026 | The command was received in the wrong sequence relative to TPM_Init and a subsequent TPM_Startup. |
| TPM_E_INAPPROPRIATE_SIG<br>0x80280027 | Signed data cannot include additional DER information. |
| TPM_E_BAD_KEY_PROPERTY<br>0x80280028 | The key properties in TPM_KEY_PARMs are not supported by this TPM. |
| TPM_E_BAD_MIGRATION<br>0x80280029 | The migration properties of this key are incorrect. |
| TPM_E_BAD_SCHEME<br>0x8028002A | The signature or encryption scheme for this key is incorrect or not permitted in this situation. |
| TPM_E_BAD_DATASIZE<br>0x8028002B | The size of the data (or blob) parameter is bad or inconsistent with the referenced key. |
| TPM_E_BAD_MODE<br>0x8028002C | A mode parameter is bad, such as capArea or subCapArea for TPM_GetCapability, phsicalPresence parameter for TPM_PhysicalPresence, or migrationType for TPM_CreateMigrationBlob. |
| TPM_E_BAD_PRESENCE<br>0x8028002D | Either the physicalPresence or physicalPresenceLock bits have the wrong value. |
| TPM_E_BAD_VERSION<br>0x8028002E | The TPM cannot perform this version of the capability. |
| TPM_E_NO_WRAP_TRANSPORT<br>0x8028002F | The TPM does not allow for wrapped transport sessions. |
| TPM_E_AUDITFAIL_UNSUCCESSFUL<br>0x80280030 | TPM audit construction failed and the underlying command was returning a failure code also. |
| TPM_E_AUDITFAIL_SUCCESSFUL<br>0x80280031 | TPM audit construction failed and the underlying command was returning success. |
| TPM_E_NOTRESETABLE<br>0x80280032 | Attempt to reset a PCR register that does not have the resettable attribute. |
| TPM_E_NOTLOCAL<br>0x80280033 | Attempt to reset a PCR register that requires locality and locality modifier not part of command transport. |
| TPM_E_BAD_TYPE<br>0x80280034 | Make identity blob not properly typed. |

| Constant/Value | Description |
|---|---|
| TPM_E_INVALID_RESOURCE<br>0x80280035 | When saving context identified resource type does not match actual resource. |
| TPM_E_NOTFIPS<br>0x80280036 | The TPM is attempting to execute a command only available when in FIPS mode. |
| TPM_E_INVALID_FAMILY<br>0x80280037 | The command is attempting to use an invalid family ID. |
| TPM_E_NO_NV_PERMISSION<br>0x80280038 | The permission to manipulate the NV storage is not available. |
| TPM_E_REQUIRES_SIGN<br>0x80280039 | The operation requires a signed command. |
| TPM_E_KEY_NOTSUPPORTED<br>0x8028003A | Wrong operation to load an NV key. |
| TPM_E_AUTH_CONFLICT<br>0x8028003B | NV_LoadKey blob requires both owner and blob authorization. |
| TPM_E_AREA_LOCKED<br>0x8028003C | The NV area is locked and not writtable. |
| TPM_E_BAD_LOCALITY<br>0x8028003D | The locality is incorrect for the attempted operation. |
| TPM_E_READ_ONLY<br>0x8028003E | The NV area is read only and cannot be written to. |
| TPM_E_PER_NOWRITE<br>0x8028003F | There is no protection on the write to the NV area. |
| TPM_E_FAMILYCOUNT<br>0x80280040 | The family count value does not match. |
| TPM_E_WRITE_LOCKED<br>0x80280041 | The NV area has already been written to. |
| TPM_E_BAD_ATTRIBUTES<br>0x80280042 | The NV area attributes conflict. |
| TPM_E_INVALID_STRUCTURE<br>0x80280043 | The structure tag and version are invalid or inconsistent. |

| Constant/Value | Description |
|---|---|
| TPM_E_KEY_OWNER_CONTROL<br>0x80280044 | The key is under control of the TPM Owner and can only be evicted by the TPM Owner. |
| TPM_E_BAD_COUNTER<br>0x80280045 | The counter handle is incorrect. |
| TPM_E_NOT_FULLWRITE<br>0x80280046 | The write is not a complete write of the area. |
| TPM_E_CONTEXT_GAP<br>0x80280047 | The gap between saved context counts is too large. |
| TPM_E_MAXNVWRITES<br>0x80280048 | The maximum number of NV writes without an owner has been exceeded. |
| TPM_E_NOOPERATOR<br>0x80280049 | No operator AuthData value is set. |
| TPM_E_RESOURCEMISSING<br>0x8028004A | The resource pointed to by context is not loaded. |
| TPM_E_DELEGATE_LOCK<br>0x8028004B | The delegate administration is locked. |
| TPM_E_DELEGATE_FAMILY<br>0x8028004C | Attempt to manage a family other than the delegated family. |
| TPM_E_DELEGATE_ADMIN<br>0x8028004D | Delegation table management not enabled. |
| TPM_E_TRANSPORT_NOTEXCLUSIVE<br>0x8028004E | There was a command executed outside of an exclusive transport session. |
| TPM_E_OWNER_CONTROL<br>0x8028004F | Attempt to context save a owner evict controlled key. |
| TPM_E_DAA_RESOURCES<br>0x80280050 | The DAA command has no resources available to execute the command. |
| TPM_E_DAA_INPUT_DATA0<br>0x80280051 | The consistency check on DAA parameter inputData0 has failed. |
| TPM_E_DAA_INPUT_DATA1<br>0x80280052 | The consistency check on DAA parameter inputData1 has failed. |

| Constant/Value | Description |
|---|---|
| TPM_E_DAA_ISSUER_SETTINGS<br>0x80280053 | The consistency check on DAA_issuerSettings has failed. |
| TPM_E_DAA_TPM_SETTINGS<br>0x80280054 | The consistency check on DAA_tpmSpecific has failed. |
| TPM_E_DAA_STAGE<br>0x80280055 | The atomic process indicated by the submitted DAA command is not the expected process. |
| TPM_E_DAA_ISSUER_VALIDITY<br>0x80280056 | The issuer's validity check has detected an inconsistency. |
| TPM_E_DAA_WRONG_W<br>0x80280057 | The consistency check on w has failed. |
| TPM_E_BAD_HANDLE<br>0x80280058 | The handle is incorrect. |
| TPM_E_BAD_DELEGATE<br>0x80280059 | Delegation is not correct. |
| TPM_E_BADCONTEXT<br>0x8028005A | The context blob is invalid. |
| TPM_E_TOOMANYCONTEXTS<br>0x8028005B | Too many contexts held by the TPM. |
| TPM_E_MA_TICKET_SIGNATURE<br>0x8028005C | Migration authority signature validation failure. |
| TPM_E_MA_DESTINATION<br>0x8028005D | Migration destination not authenticated. |
| TPM_E_MA_SOURCE<br>0x8028005E | Migration source incorrect. |
| TPM_E_MA_AUTHORITY<br>0x8028005F | Incorrect migration authority. |
| TPM_E_PERMANENTEK<br>0x80280061 | Attempt to revoke the EK and the EK is not revocable. |
| TPM_E_BAD_SIGNATURE<br>0x80280062 | Bad signature of CMK ticket. |

| Constant/Value | Description |
|---|---|
| TPM_E_NOCONTEXTSPACE<br>0x80280063 | There is no room in the context list for additional contexts. |
| TPM_E_COMMAND_BLOCKED<br>0x80280400 | The command was blocked. |
| TPM_E_INVALID_HANDLE<br>0x80280401 | The specified handle was not found. |
| TPM_E_DUPLICATE_VHANDLE<br>0x80280402 | The TPM returned a duplicate handle and the command needs to be resubmitted. |
| TPM_E_EMBEDDED_COMMAND_BLOCKED<br>0x80280403 | The command within the transport was blocked. |
| TPM_E_EMBEDDED_COMMAND_UNSUPPORTED<br>0x80280404 | The command within the transport is not supported. |
| TPM_E_RETRY<br>0x80280800 | The TPM is too busy to respond to the command immediately, but the command could be resubmitted at a later time. |
| TPM_E_NEEDS_SELFTEST<br>0x80280801 | SelfTestFull has not been run. |
| TPM_E_DOING_SELFTEST<br>0x80280802 | The TPM is currently executing a full self test. |
| TPM_E_DEFEND_LOCK_RUNNING<br>0x80280803 | The TPM is defending against dictionary attacks and is in a time-out period. |
| TBS_E_INTERNAL_ERROR<br>0x80284001 | An internal software error has been detected. |
| TBS_E_BAD_PARAMETER<br>0x80284002 | One or more input parameters is bad. |
| TBS_E_INVALID_OUTPUT_POINTER<br>0x80284003 | A specified output pointer is bad. |
| TBS_E_INVALID_CONTEXT<br>0x80284004 | The specified context handle does not refer to a valid context. |
| TBS_E_INSUFFICIENT_BUFFER<br>0x80284005 | A specified output buffer is too small. |

| Constant/Value | Description |
|---|---|
| TBS_E_IOERROR<br>0x80284006 | An error occurred while communicating with the TPM. |
| TBS_E_INVALID_CONTEXT_PARAM<br>0x80284007 | One or more context parameters is invalid. |
| TBS_E_SERVICE_NOT_RUNNING<br>0x80284008 | The TBS service is not running and could not be started. |
| TBS_E_TOO_MANY_TBS_CONTEXTS<br>0x80284009 | A new context could not be created because there are too many open contexts. |
| TBS_E_TOO_MANY_RESOURCES<br>0x8028400A | A new virtual resource could not be created because there are too many open virtual resources. |
| TBS_E_SERVICE_START_PENDING<br>0x8028400B | The TBS service has been started but is not yet running. |
| TBS_E_PPI_NOT_SUPPORTED<br>0x8028400C | The physical presence interface is not supported. |
| TBS_E_COMMAND_CANCELED<br>0x8028400D | The command was canceled. |
| TBS_E_BUFFER_TOO_LARGE<br>0x8028400E | The input or output buffer is too large. |
| TBS_E_TPM_NOT_FOUND<br>0x8028400F | A compatible TPM Security Device cannot be found on this computer. |
| TBS_E_SERVICE_DISABLED<br>0x80284010 | The TBS service has been disabled. |
| TBS_E_NO_EVENT_LOG<br>0x80284011 | No TCG event log is available. |
| TBS_E_ACCESS_DENIED<br>0x80284012 | The caller does not have the appropriate rights to perform the requested operation. |
| TBS_E_PROVISIONING_NOT_ALLOWED<br>0x80284013 | The TPM provisioning action is not allowed by the specified flags. For provisioning to be successful, one of several actions may be required. The TPM management console (tpm.msc) action to make the TPM Ready may help. For further information, see the documentation for the Win32_Tpm WMI method 'Provision'. (The actions that may be required include importing the TPM Owner Authorization value into the system, calling the Win32_Tpm WMI method for provisioning the TPM and specifying TRUE for either 'ForceClear_Allowed' or 'PhysicalPresencePrompts_Allowed' (as |

| Constant/Value | Description |
|---|---|
| | indicated by the value returned in the Additional Information), or enabling the TPM in the system BIOS.) |
| TBS_E_PPI_FUNCTION_UNSUPPORTED<br>0x80284014 | The Physical Presence Interface of this firmware does not support the requested method. |
| TBS_E_OWNERAUTH_NOT_FOUND<br>0x80284015 | The requested TPM OwnerAuth value was not found. |
| TBS_E_PROVISIONING_INCOMPLETE<br>0x80284016 | The TPM provisioning did not complete. For more information on completing the provisioning, call the Win32_Tpm WMI method for provisioning the TPM ('Provision') and check the returned Information. |
| TPMAPI_E_INVALID_STATE<br>0x80290100 | The command buffer is not in the correct state. |
| TPMAPI_E_NOT_ENOUGH_DATA<br>0x80290101 | The command buffer does not contain enough data to satisfy the request. |
| TPMAPI_E_TOO_MUCH_DATA<br>0x80290102 | The command buffer cannot contain any more data. |
| TPMAPI_E_INVALID_OUTPUT_POINTER<br>0x80290103 | One or more output parameters was NULL or invalid. |
| TPMAPI_E_INVALID_PARAMETER<br>0x80290104 | One or more input parameters is invalid. |
| TPMAPI_E_OUT_OF_MEMORY<br>0x80290105 | Not enough memory was available to satisfy the request. |
| TPMAPI_E_BUFFER_TOO_SMALL<br>0x80290106 | The specified buffer was too small. |
| TPMAPI_E_INTERNAL_ERROR<br>0x80290107 | An internal error was detected. |
| TPMAPI_E_ACCESS_DENIED<br>0x80290108 | The caller does not have the appropriate rights to perform the requested operation. |
| TPMAPI_E_AUTHORIZATION_FAILED<br>0x80290109 | The specified authorization information was invalid. |
| TPMAPI_E_INVALID_CONTEXT_HANDLE<br>0x8029010A | The specified context handle was not valid. |

| Constant/Value | Description |
|---|---|
| TPMAPI_E_TBS_COMMUNICATION_ERROR<br>0x8029010B | An error occurred while communicating with the TBS. |
| TPMAPI_E_TPM_COMMAND_ERROR<br>0x8029010C | The TPM returned an unexpected result. |
| TPMAPI_E_MESSAGE_TOO_LARGE<br>0x8029010D | The message was too large for the encoding scheme. |
| TPMAPI_E_INVALID_ENCODING<br>0x8029010E | The encoding in the blob was not recognized. |
| TPMAPI_E_INVALID_KEY_SIZE<br>0x8029010F | The key size is not valid. |
| TPMAPI_E_ENCRYPTION_FAILED<br>0x80290110 | The encryption operation failed. |
| TPMAPI_E_INVALID_KEY_PARAMS<br>0x80290111 | The key parameters structure was not valid |
| TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB<br>0x80290112 | The requested supplied data does not appear to be a valid migration authorization blob. |
| TPMAPI_E_INVALID_PCR_INDEX<br>0x80290113 | The specified PCR index was invalid |
| TPMAPI_E_INVALID_DELEGATE_BLOB<br>0x80290114 | The data given does not appear to be a valid delegate blob. |
| TPMAPI_E_INVALID_CONTEXT_PARAMS<br>0x80290115 | One or more of the specified context parameters was not valid. |
| TPMAPI_E_INVALID_KEY_BLOB<br>0x80290116 | The data given does not appear to be a valid key blob |
| TPMAPI_E_INVALID_PCR_DATA<br>0x80290117 | The specified PCR data was invalid. |
| TPMAPI_E_INVALID_OWNER_AUTH<br>0x80290118 | The format of the owner auth data was invalid. |
| TPMAPI_E_FIPS_RNG_CHECK_FAILED<br>0x80290119 | The random number generated did not pass FIPS RNG check. |

| Constant/Value | Description |
|---|---|
| TPMAPI_E_EMPTY_TCG_LOG<br>0x8029011A | The TCG Event Log does not contain any data. |
| TPMAPI_E_INVALID_TCG_LOG_ENTRY<br>0x8029011B | An entry in the TCG Event Log was invalid. |
| TPMAPI_E_TCG_SEPARATOR_ABSENT<br>0x8029011C | A TCG Separator was not found. |
| TPMAPI_E_TCG_INVALID_DIGEST_ENTRY<br>0x8029011D | A digest value in a TCG Log entry did not match hashed data. |
| TPMAPI_E_POLICY_DENIES_OPERATION<br>0x8029011E | The requested operation was blocked by current TPM policy. Please contact your system administrator for assistance. |
| TBSIMP_E_BUFFER_TOO_SMALL<br>0x80290200 | The specified buffer was too small. |
| TBSIMP_E_CLEANUP_FAILED<br>0x80290201 | The context could not be cleaned up. |
| TBSIMP_E_INVALID_CONTEXT_HANDLE<br>0x80290202 | The specified context handle is invalid. |
| TBSIMP_E_INVALID_CONTEXT_PARAM<br>0x80290203 | An invalid context parameter was specified. |
| TBSIMP_E_TPM_ERROR<br>0x80290204 | An error occurred while communicating with the TPM |
| TBSIMP_E_HASH_BAD_KEY<br>0x80290205 | No entry with the specified key was found. |
| TBSIMP_E_DUPLICATE_VHANDLE<br>0x80290206 | The specified virtual handle matches a virtual handle already in use. |
| TBSIMP_E_INVALID_OUTPUT_POINTER<br>0x80290207 | The pointer to the returned handle location was NULL or invalid |
| TBSIMP_E_INVALID_PARAMETER<br>0x80290208 | One or more parameters is invalid |
| TBSIMP_E_RPC_INIT_FAILED<br>0x80290209 | The RPC subsystem could not be initialized. |

| Constant/Value | Description |
|---|---|
| TBSIMP_E_SCHEDULER_NOT_RUNNING<br>0x8029020A | The TBS scheduler is not running. |
| TBSIMP_E_COMMAND_CANCELED<br>0x8029020B | The command was canceled. |
| TBSIMP_E_OUT_OF_MEMORY<br>0x8029020C | There was not enough memory to fulfill the request |
| TBSIMP_E_LIST_NO_MORE_ITEMS<br>0x8029020D | The specified list is empty, or the iteration has reached the end of the list. |
| TBSIMP_E_LIST_NOT_FOUND<br>0x8029020E | The specified item was not found in the list. |
| TBSIMP_E_NOT_ENOUGH_SPACE<br>0x8029020F | The TPM does not have enough space to load the requested resource. |
| TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS<br>0x80290210 | There are too many TPM contexts in use. |
| TBSIMP_E_COMMAND_FAILED<br>0x80290211 | The TPM command failed. |
| TBSIMP_E_UNKNOWN_ORDINAL<br>0x80290212 | The TBS does not recognize the specified ordinal. |
| TBSIMP_E_RESOURCE_EXPIRED<br>0x80290213 | The requested resource is no longer available. |
| TBSIMP_E_INVALID_RESOURCE<br>0x80290214 | The resource type did not match. |
| TBSIMP_E_NOTHING_TO_UNLOAD<br>0x80290215 | No resources can be unloaded. |
| TBSIMP_E_HASH_TABLE_FULL<br>0x80290216 | No new entries can be added to the hash table. |
| TBSIMP_E_TOO_MANY_TBS_CONTEXTS<br>0x80290217 | A new TBS context could not be created because there are too many open contexts. |
| TBSIMP_E_TOO_MANY_RESOURCES<br>0x80290218 | A new virtual resource could not be created because there are too many open virtual resources. |

| Constant/Value | Description |
|---|---|
| TBSIMP_E_PPI_NOT_SUPPORTED<br>0x80290219 | The physical presence interface is not supported. |
| TBSIMP_E_TPM_INCOMPATIBLE<br>0x8029021A | TBS is not compatible with the version of TPM found on the system. |
| TBSIMP_E_NO_EVENT_LOG<br>0x8029021B | No TCG event log is available. |
| TPM_E_PPI_ACPI_FAILURE<br>0x80290300 | A general error was detected when attempting to acquire the BIOS's response to a Physical Presence command. |
| TPM_E_PPI_USER_ABORT<br>0x80290301 | The user failed to confirm the TPM operation request. |
| TPM_E_PPI_BIOS_FAILURE<br>0x80290302 | The BIOS failure prevented the successful execution of the requested TPM operation (e.g. invalid TPM operation request, BIOS communication error with the TPM). |
| TPM_E_PPI_NOT_SUPPORTED<br>0x80290303 | The BIOS does not support the physical presence interface. |
| TPM_E_PPI_BLOCKED_IN_BIOS<br>0x80290304 | The Physical Presence command was blocked by current BIOS settings. The system owner may be able to reconfigure the BIOS settings to allow the command. |
| TPM_E_PCP_ERROR_MASK<br>0x80290400 | This is an error mask to convert Platform Crypto Provider errors to win errors. |
| TPM_E_PCP_DEVICE_NOT_READY<br>0x80290401 | The Platform Crypto Device is currently not ready. It needs to be fully provisioned to be operational. |
| TPM_E_PCP_INVALID_HANDLE<br>0x80290402 | The handle provided to the Platform Crypto Provider is invalid. |
| TPM_E_PCP_INVALID_PARAMETER<br>0x80290403 | A parameter provided to the Platform Crypto Provider is invalid. |
| TPM_E_PCP_FLAG_NOT_SUPPORTED<br>0x80290404 | A provided flag to the Platform Crypto Provider is not supported. |
| TPM_E_PCP_NOT_SUPPORTED<br>0x80290405 | The requested operation is not supported by this Platform Crypto Provider. |
| TPM_E_PCP_BUFFER_TOO_SMALL<br>0x80290406 | The buffer is too small to contain all data. No information has been written to the buffer. |

| Constant/Value | Description |
|---|---|
| TPM_E_PCP_INTERNAL_ERROR<br>0x80290407 | An unexpected internal error has occurred in the Platform Crypto Provider. |
| TPM_E_PCP_AUTHENTICATION_FAILED<br>0x80290408 | The authorization to use a provider object has failed. |
| TPM_E_PCP_AUTHENTICATION_IGNORED<br>0x80290409 | The Platform Crypto Device has ignored the authorization for the provider object, to mitigate against a dictionary attack. |
| TPM_E_PCP_POLICY_NOT_FOUND<br>0x8029040A | The referenced policy was not found. |
| TPM_E_PCP_PROFILE_NOT_FOUND<br>0x8029040B | The referenced profile was not found. |
| TPM_E_PCP_VALIDATION_FAILED<br>0x8029040C | The validation was not successful. |
| PLA_E_DCS_NOT_FOUND<br>0x80300002 | Data Collector Set was not found. |
| PLA_E_DCS_IN_USE<br>0x803000AA | The Data Collector Set or one of its dependencies is already in use. |
| PLA_E_TOO_MANY_FOLDERS<br>0x80300045 | Unable to start Data Collector Set because there are too many folders. |
| PLA_E_NO_MIN_DISK<br>0x80300070 | Not enough free disk space to start Data Collector Set. |
| PLA_E_DCS_ALREADY_EXISTS<br>0x803000B7 | Data Collector Set already exists. |
| PLA_S_PROPERTY_IGNORED<br>0x00300100 | Property value will be ignored. |
| PLA_E_PROPERTY_CONFLICT<br>0x80300101 | Property value conflict. |
| PLA_E_DCS_SINGLETON_REQUIRED<br>0x80300102 | The current configuration for this Data Collector Set requires that it contain exactly one Data Collector. |
| PLA_E_CREDENTIALS_REQUIRED<br>0x80300103 | A user account is required in order to commit the current Data Collector Set properties. |

| Constant/Value | Description |
|---|---|
| PLA_E_DCS_NOT_RUNNING<br>0x80300104 | Data Collector Set is not running. |
| PLA_E_CONFLICT_INCL_EXCL_API<br>0x80300105 | A conflict was detected in the list of include/exclude APIs. Do not specify the same API in both the include list and the exclude list. |
| PLA_E_NETWORK_EXE_NOT_VALID<br>0x80300106 | The executable path you have specified refers to a network share or UNC path. |
| PLA_E_EXE_ALREADY_CONFIGURED<br>0x80300107 | The executable path you have specified is already configured for API tracing. |
| PLA_E_EXE_PATH_NOT_VALID<br>0x80300108 | The executable path you have specified does not exist. Verify that the specified path is correct. |
| PLA_E_DC_ALREADY_EXISTS<br>0x80300109 | Data Collector already exists. |
| PLA_E_DCS_START_WAIT_TIMEOUT<br>0x8030010A | The wait for the Data Collector Set start notification has timed out. |
| PLA_E_DC_START_WAIT_TIMEOUT<br>0x8030010B | The wait for the Data Collector to start has timed out. |
| PLA_E_REPORT_WAIT_TIMEOUT<br>0x8030010C | The wait for the report generation tool to finish has timed out. |
| PLA_E_NO_DUPLICATES<br>0x8030010D | Duplicate items are not allowed. |
| PLA_E_EXE_FULL_PATH_REQUIRED<br>0x8030010E | When specifying the executable that you want to trace, you must specify a full path to the executable and not just a filename. |
| PLA_E_INVALID_SESSION_NAME<br>0x8030010F | The session name provided is invalid. |
| PLA_E_PLA_CHANNEL_NOT_ENABLED<br>0x80300110 | The Event Log channel Microsoft-Windows-Diagnosis-PLA/Operational must be enabled to perform this operation. |
| PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED<br>0x80300111 | The Event Log channel Microsoft-Windows-TaskScheduler must be enabled to perform this operation. |
| PLA_E_RULES_MANAGER_FAILED<br>0x80300112 | The execution of the Rules Manager failed. |

| Constant/Value | Description |
|---|---|
| PLA_E_CABAPI_FAILURE<br>0x80300113 | An error occurred while attempting to compress or extract the data. |
| FVE_E_LOCKED_VOLUME<br>0x80310000 | This drive is locked by BitLocker Drive Encryption. You must unlock this drive from Control Panel. |
| FVE_E_NOT_ENCRYPTED<br>0x80310001 | The drive is not encrypted. |
| FVE_E_NO_TPM_BIOS<br>0x80310002 | The BIOS did not correctly communicate with the TPM. Contact the computer manufacturer for BIOS upgrade instructions. |
| FVE_E_NO_MBR_METRIC<br>0x80310003 | The BIOS did not correctly communicate with the master boot record (MBR). Contact the computer manufacturer for BIOS upgrade instructions. |
| FVE_E_NO_BOOTSECTOR_METRIC<br>0x80310004 | A required TPM measurement is missing. If there is a bootable CD or DVD in your computer, remove it, restart the computer, and turn on BitLocker again. If the problem persists, ensure the master boot record is up to date. |
| FVE_E_NO_BOOTMGR_METRIC<br>0x80310005 | The boot sector of this drive is not compatible with BitLocker Drive Encryption. Use the Bootrec.exe tool in the Windows Recovery Environment to update or repair the boot manager (BOOTMGR). |
| FVE_E_WRONG_BOOTMGR<br>0x80310006 | The boot manager of this operating system is not compatible with BitLocker Drive Encryption. Use the Bootrec.exe tool in the Windows Recovery Environment to update or repair the boot manager (BOOTMGR). |
| FVE_E_SECURE_KEY_REQUIRED<br>0x80310007 | At least one secure key protector is required for this operation to be performed. |
| FVE_E_NOT_ACTIVATED<br>0x80310008 | BitLocker Drive Encryption is not enabled on this drive. Turn on BitLocker. |
| FVE_E_ACTION_NOT_ALLOWED<br>0x80310009 | BitLocker Drive Encryption cannot perform requested action. This condition may occur when two requests are issued at the same time. Wait a few moments and then try the action again. |
| FVE_E_AD_SCHEMA_NOT_INSTALLED<br>0x8031000A | The Active Directory Domain Services forest does not contain the required attributes and classes to host BitLocker Drive Encryption or TPM information. Contact your domain administrator to verify that any required BitLocker Active Directory schema extensions have been installed. |
| FVE_E_AD_INVALID_DATATYPE<br>0x8031000B | The type of the data obtained from Active Directory was not expected. The BitLocker recovery information may be missing or corrupted. |
| FVE_E_AD_INVALID_DATASIZE<br>0x8031000C | The size of the data obtained from Active Directory was not expected. The BitLocker recovery information may be missing or corrupted. |

| Constant/Value | Description |
|---|---|
| FVE_E_AD_NO_VALUES<br>0x8031000D | The attribute read from Active Directory does not contain any values. The BitLocker recovery information may be missing or corrupted. |
| FVE_E_AD_ATTR_NOT_SET<br>0x8031000E | The attribute was not set. Verify that you are logged on with a domain account that has the ability to write information to Active Directory objects. |
| FVE_E_AD_GUID_NOT_FOUND<br>0x8031000F | The specified attribute cannot be found in Active Directory Domain Services. Contact your domain administrator to verify that any required BitLocker Active Directory schema extensions have been installed. |
| FVE_E_BAD_INFORMATION<br>0x80310010 | The BitLocker metadata for the encrypted drive is not valid. You can attempt to repair the drive to restore access. |
| FVE_E_TOO_SMALL<br>0x80310011 | The drive cannot be encrypted because it does not have enough free space. Delete any unnecessary data on the drive to create additional free space and then try again. |
| FVE_E_SYSTEM_VOLUME<br>0x80310012 | The drive cannot be encrypted because it contains system boot information. Create a separate partition for use as the system drive that contains the boot information and a second partition for use as the operating system drive and then encrypt the operating system drive. |
| FVE_E_FAILED_WRONG_FS<br>0x80310013 | The drive cannot be encrypted because the file system is not supported. |
| FVE_E_BAD_PARTITION_SIZE<br>0x80310014 | The file system size is larger than the partition size in the partition table. This drive may be corrupt or may have been tampered with. To use it with BitLocker, you must reformat the partition. |
| FVE_E_NOT_SUPPORTED<br>0x80310015 | This drive cannot be encrypted. |
| FVE_E_BAD_DATA<br>0x80310016 | The data is not valid. |
| FVE_E_VOLUME_NOT_BOUND<br>0x80310017 | The data drive specified is not set to automatically unlock on the current computer and cannot be unlocked automatically. |
| FVE_E_TPM_NOT_OWNED<br>0x80310018 | You must initialize the TPM before you can use BitLocker Drive Encryption. |
| FVE_E_NOT_DATA_VOLUME<br>0x80310019 | The operation attempted cannot be performed on an operating system drive. |
| FVE_E_AD_INSUFFICIENT_BUFFER<br>0x8031001A | The buffer supplied to a function was insufficient to contain the returned data. Increase the buffer size before running the function again. |
| FVE_E_CONV_READ | A read operation failed while converting the drive. The drive was not converted. Please re-enable BitLocker. |

| Constant/Value | Description |
|---|---|
| 0x8031001B | |
| FVE_E_CONV_WRITE<br>0x8031001C | A write operation failed while converting the drive. The drive was not converted. Please re-enable BitLocker. |
| FVE_E_KEY_REQUIRED<br>0x8031001D | One or more BitLocker key protectors are required. You cannot delete the last key on this drive. |
| FVE_E_CLUSTERING_NOT_SUPPORTED<br>0x8031001E | Cluster configurations are not supported by BitLocker Drive Encryption. |
| FVE_E_VOLUME_BOUND_ALREADY<br>0x8031001F | The drive specified is already configured to be automatically unlocked on the current computer. |
| FVE_E_OS_NOT_PROTECTED<br>0x80310020 | The operating system drive is not protected by BitLocker Drive Encryption. |
| FVE_E_PROTECTION_DISABLED<br>0x80310021 | BitLocker Drive Encryption has been suspended on this drive. All BitLocker key protectors configured for this drive are effectively disabled, and the drive will be automatically unlocked using an unencrypted (clear) key. |
| FVE_E_RECOVERY_KEY_REQUIRED<br>0x80310022 | The drive you are attempting to lock does not have any key protectors available for encryption because BitLocker protection is currently suspended. Re-enable BitLocker to lock this drive. |
| FVE_E_FOREIGN_VOLUME<br>0x80310023 | BitLocker cannot use the TPM to protect a data drive. TPM protection can only be used with the operating system drive. |
| FVE_E_OVERLAPPED_UPDATE<br>0x80310024 | The BitLocker metadata for the encrypted drive cannot be updated because it was locked for updating by another process. Please try this process again. |
| FVE_E_TPM_SRK_AUTH_NOT_ZERO<br>0x80310025 | The authorization data for the storage root key (SRK) of the TPM is not zero and is therefore incompatible with BitLocker. Please initialize the TPM before attempting to use it with BitLocker. |
| FVE_E_FAILED_SECTOR_SIZE<br>0x80310026 | The drive encryption algorithm cannot be used on this sector size. |
| FVE_E_FAILED_AUTHENTICATION<br>0x80310027 | The drive cannot be unlocked with the key provided. Confirm that you have provided the correct key and try again. |
| FVE_E_NOT_OS_VOLUME<br>0x80310028 | The drive specified is not the operating system drive. |
| FVE_E_AUTOUNLOCK_ENABLED<br>0x80310029 | BitLocker Drive Encryption cannot be turned off on the operating system drive until the auto unlock feature has been disabled for the fixed data drives and removable data drives associated with this computer. |

| Constant/Value | Description |
|---|---|
| FVE_E_WRONG_BOOTSECTOR<br>0x8031002A | The system partition boot sector does not perform TPM measurements. Use the Bootrec.exe tool in the Windows Recovery Environment to update or repair the boot sector. |
| FVE_E_WRONG_SYSTEM_FS<br>0x8031002B | BitLocker Drive Encryption operating system drives must be formatted with the NTFS file system in order to be encrypted. Convert the drive to NTFS, and then turn on BitLocker. |
| FVE_E_POLICY_PASSWORD_REQUIRED<br>0x8031002C | Group Policy settings require that a recovery password be specified before encrypting the drive. |
| FVE_E_CANNOT_SET_FVEK_ENCRYPTED<br>0x8031002D | The drive encryption algorithm and key cannot be set on a previously encrypted drive. To encrypt this drive with BitLocker Drive Encryption, remove the previous encryption and then turn on BitLocker. |
| FVE_E_CANNOT_ENCRYPT_NO_KEY<br>0x8031002E | BitLocker Drive Encryption cannot encrypt the specified drive because an encryption key is not available. Add a key protector to encrypt this drive. |
| FVE_E_BOOTABLE_CDDVD<br>0x80310030 | BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer. Remove the media and restart the computer before configuring BitLocker. |
| FVE_E_PROTECTOR_EXISTS<br>0x80310031 | This key protector cannot be added. Only one key protector of this type is allowed for this drive. |
| FVE_E_RELATIVE_PATH<br>0x80310032 | The recovery password file was not found because a relative path was specified. Recovery passwords must be saved to a fully qualified path. Environment variables configured on the computer can be used in the path. |
| FVE_E_PROTECTOR_NOT_FOUND<br>0x80310033 | The specified key protector was not found on the drive. Try another key protector. |
| FVE_E_INVALID_KEY_FORMAT<br>0x80310034 | The recovery key provided is corrupt and cannot be used to access the drive. An alternative recovery method, such as recovery password, a data recovery agent, or a backup version of the recovery key must be used to recover access to the drive. |
| FVE_E_INVALID_PASSWORD_FORMAT<br>0x80310035 | The format of the recovery password provided is invalid. BitLocker recovery passwords are 48 digits. Verify that the recovery password is in the correct format and then try again. |
| FVE_E_FIPS_RNG_CHECK_FAILED<br>0x80310036 | The random number generator check test failed. |
| FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD<br>0x80310037 | The Group Policy setting requiring FIPS compliance prevents a local recovery password from being generated or used by BitLocker Drive Encryption. When operating in FIPS-compliant mode, BitLocker recovery options can be either a recovery key stored on a USB drive or recovery through a data recovery agent. |
| FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT<br>0x80310038 | The Group Policy setting requiring FIPS compliance prevents the recovery password from being saved to Active Directory. When operating in FIPS-compliant mode, BitLocker recovery options can be either a recovery key stored on a USB drive or recovery through |

| Constant/Value | Description |
|---|---|
|  | a data recovery agent. Check your Group Policy settings configuration. |
| FVE_E_NOT_DECRYPTED<br>0x80310039 | The drive must be fully decrypted to complete this operation. |
| FVE_E_INVALID_PROTECTOR_TYPE<br>0x8031003A | The key protector specified cannot be used for this operation. |
| FVE_E_NO_PROTECTORS_TO_TEST<br>0x8031003B | No key protectors exist on the drive to perform the hardware test. |
| FVE_E_KEYFILE_NOT_FOUND<br>0x8031003C | The BitLocker startup key or recovery password cannot be found on the USB device. Verify that you have the correct USB device, that the USB device is plugged into the computer on an active USB port, restart the computer, and then try again. If the problem persists, contact the computer manufacturer for BIOS upgrade instructions. |
| FVE_E_KEYFILE_INVALID<br>0x8031003D | The BitLocker startup key or recovery password file provided is corrupt or invalid. Verify that you have the correct startup key or recovery password file and try again. |
| FVE_E_KEYFILE_NO_VMK<br>0x8031003E | The BitLocker encryption key cannot be obtained from the startup key or recovery password. Verify that you have the correct startup key or recovery password and try again. |
| FVE_E_TPM_DISABLED<br>0x8031003F | The TPM is disabled. The TPM must be enabled, initialized, and have valid ownership before it can be used with BitLocker Drive Encryption. |
| FVE_E_NOT_ALLOWED_IN_SAFE_MODE<br>0x80310040 | The BitLocker configuration of the specified drive cannot be managed because this computer is currently operating in Safe Mode. While in Safe Mode, BitLocker Drive Encryption can only be used for recovery purposes. |
| FVE_E_TPM_INVALID_PCR<br>0x80310041 | The TPM was not able to unlock the drive because the system boot information has changed or a PIN was not provided correctly. Verify that the drive has not been tampered with and that changes to the system boot information were caused by a trusted source. After verifying that the drive is safe to access, use the BitLocker recovery console to unlock the drive and then suspend and resume BitLocker to update system boot information that BitLocker associates with this drive. |
| FVE_E_TPM_NO_VMK<br>0x80310042 | The BitLocker encryption key cannot be obtained from the TPM. |
| FVE_E_PIN_INVALID<br>0x80310043 | The BitLocker encryption key cannot be obtained from the TPM and PIN. |
| FVE_E_AUTH_INVALID_APPLICATION<br>0x80310044 | A boot application has changed since BitLocker Drive Encryption was enabled. |

| Constant/Value | Description |
|---|---|
| FVE_E_AUTH_INVALID_CONFIG<br>0x80310045 | The Boot Configuration Data (BCD) settings have changed since BitLocker Drive Encryption was enabled. |
| FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED<br>0x80310046 | The Group Policy setting requiring FIPS compliance prohibits the use of unencrypted keys, which prevents BitLocker from being suspended on this drive. Please contact your domain administrator for more information. |
| FVE_E_FS_NOT_EXTENDED<br>0x80310047 | This drive cannot be encrypted by BitLocker Drive Encryption because the file system does not extend to the end of the drive. Repartition this drive and then try again. |
| FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED<br>0x80310048 | BitLocker Drive Encryption cannot be enabled on the operating system drive. Contact the computer manufacturer for BIOS upgrade instructions. |
| FVE_E_NO_LICENSE<br>0x80310049 | This version of Windows does not include BitLocker Drive Encryption. To use BitLocker Drive Encryption, please upgrade the operating system. |
| FVE_E_NOT_ON_STACK<br>0x8031004A | BitLocker Drive Encryption cannot be used because critical BitLocker system files are missing or corrupted. Use Windows Startup Repair to restore these files to your computer. |
| FVE_E_FS_MOUNTED<br>0x8031004B | The drive cannot be locked when the drive is in use. |
| FVE_E_TOKEN_NOT_IMPERSONATED<br>0x8031004C | The access token associated with the current thread is not an impersonated token. |
| FVE_E_DRY_RUN_FAILED<br>0x8031004D | The BitLocker encryption key cannot be obtained. Verify that the TPM is enabled and ownership has been taken. If this computer does not have a TPM, verify that the USB drive is inserted and available. |
| FVE_E_REBOOT_REQUIRED<br>0x8031004E | You must restart your computer before continuing with BitLocker Drive Encryption. |
| FVE_E_DEBUGGER_ENABLED<br>0x8031004F | Drive encryption cannot occur while boot debugging is enabled. Use the bcdedit command-line tool to turn off boot debugging. |
| FVE_E_RAW_ACCESS<br>0x80310050 | No action was taken as BitLocker Drive Encryption is in raw access mode. |
| FVE_E_RAW_BLOCKED<br>0x80310051 | BitLocker Drive Encryption cannot enter raw access mode for this drive because the drive is currently in use. |
| FVE_E_BCD_APPLICATIONS_PATH_INCORRECT<br>0x80310052 | The path specified in the Boot Configuration Data (BCD) for a BitLocker Drive Encryption integrity-protected application is incorrect. Please verify and correct your BCD settings and try again. |

| Constant/Value | Description |
|---|---|
| FVE_E_NOT_ALLOWED_IN_VERSION<br>0x80310053 | BitLocker Drive Encryption can only be used for limited provisioning or recovery purposes when the computer is running in pre-installation or recovery environments. |
| FVE_E_NO_AUTOUNLOCK_MASTER_KEY<br>0x80310054 | The auto-unlock master key was not available from the operating system drive. |
| FVE_E_MOR_FAILED<br>0x80310055 | The system firmware failed to enable clearing of system memory when the computer was restarted. |
| FVE_E_HIDDEN_VOLUME<br>0x80310056 | The hidden drive cannot be encrypted. |
| FVE_E_TRANSIENT_STATE<br>0x80310057 | BitLocker encryption keys were ignored because the drive was in a transient state. |
| FVE_E_PUBKEY_NOT_ALLOWED<br>0x80310058 | Public key based protectors are not allowed on this drive. |
| FVE_E_VOLUME_HANDLE_OPEN<br>0x80310059 | BitLocker Drive Encryption is already performing an operation on this drive. Please complete all operations before continuing. |
| FVE_E_NO_FEATURE_LICENSE<br>0x8031005A | This version of Windows does not support this feature of BitLocker Drive Encryption. To use this feature, upgrade the operating system. |
| FVE_E_INVALID_STARTUP_OPTIONS<br>0x8031005B | The Group Policy settings for BitLocker startup options are in conflict and cannot be applied. Contact your system administrator for more information. |
| FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED<br>0x8031005C | Group policy settings do not permit the creation of a recovery password. |
| FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED<br>0x8031005D | Group policy settings require the creation of a recovery password. |
| FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED<br>0x8031005E | Group policy settings do not permit the creation of a recovery key. |
| FVE_E_POLICY_RECOVERY_KEY_REQUIRED<br>0x8031005F | Group policy settings require the creation of a recovery key. |
| FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED<br>0x80310060 | Group policy settings do not permit the use of a PIN at startup. Please choose a different BitLocker startup option. |
| FVE_E_POLICY_STARTUP_PIN_REQUIRED<br>0x80310061 | Group policy settings require the use of a PIN at startup. Please choose this BitLocker startup option. |

| Constant/Value | Description |
|---|---|
| FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED<br>0x80310062 | Group policy settings do not permit the use of a startup key. Please choose a different BitLocker startup option. |
| FVE_E_POLICY_STARTUP_KEY_REQUIRED<br>0x80310063 | Group policy settings require the use of a startup key. Please choose this BitLocker startup option. |
| FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064 | Group policy settings do not permit the use of a startup key and PIN. Please choose a different BitLocker startup option. |
| FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED<br>0x80310065 | Group policy settings require the use of a startup key and PIN. Please choose this BitLocker startup option. |
| FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED<br>0x80310066 | Group policy does not permit the use of TPM-only at startup. Please choose a different BitLocker startup option. |
| FVE_E_POLICY_STARTUP_TPM_REQUIRED<br>0x80310067 | Group policy settings require the use of TPM-only at startup. Please choose this BitLocker startup option. |
| FVE_E_POLICY_INVALID_PIN_LENGTH<br>0x80310068 | The PIN provided does not meet minimum or maximum length requirements. |
| FVE_E_KEY_PROTECTOR_NOT_SUPPORTED<br>0x80310069 | The key protector is not supported by the version of BitLocker Drive Encryption currently on the drive. Upgrade the drive to add the key protector. |
| FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED<br>0x8031006A | Group policy settings do not permit the creation of a password. |
| FVE_E_POLICY_PASSPHRASE_REQUIRED<br>0x8031006B | Group policy settings require the creation of a password. |
| FVE_E_FIPS_PREVENTS_PASSPHRASE<br>0x8031006C | The group policy setting requiring FIPS compliance prevented the password from being generated or used. Please contact your domain administrator for more information. |
| FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED<br>0x8031006D | A password cannot be added to the operating system drive. |
| FVE_E_INVALID_BITLOCKER_OID<br>0x8031006E | The BitLocker object identifier (OID) on the drive appears to be invalid or corrupt. Use manage-BDE to reset the OID on this drive. |
| FVE_E_VOLUME_TOO_SMALL<br>0x8031006F | The drive is too small to be protected using BitLocker Drive Encryption. |
| FVE_E_DV_NOT_SUPPORTED_ON_FS<br>0x80310070 | The selected discovery drive type is incompatible with the file system on the drive. BitLocker To Go discovery drives must be created on FAT formatted drives. |

| Constant/Value | Description |
|---|---|
| FVE_E_DV_NOT_ALLOWED_BY_GP<br>0x80310071 | The selected discovery drive type is not allowed by the computer's Group Policy settings. Verify that Group Policy settings allow the creation of discovery drives for use with BitLocker To Go. |
| FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED<br>0x80310072 | Group Policy settings do not permit user certificates such as smart cards to be used with BitLocker Drive Encryption. |
| FVE_E_POLICY_USER_CERTIFICATE_REQUIRED<br>0x80310073 | Group Policy settings require that you have a valid user certificate, such as a smart card, to be used with BitLocker Drive Encryption. |
| FVE_E_POLICY_USER_CERT_MUST_BE_HW<br>0x80310074 | Group Policy settings requires that you use a smart card-based key protector with BitLocker Drive Encryption. |
| FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED<br>0x80310075 | Group Policy settings do not permit BitLocker-protected fixed data drives to be automatically unlocked. |
| FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED<br>0x80310076 | Group Policy settings do not permit BitLocker-protected removable data drives to be automatically unlocked. |
| FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED<br>0x80310077 | Group Policy settings do not permit you to configure BitLocker Drive Encryption on removable data drives. |
| FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED<br>0x80310078 | Group Policy settings do not permit you to turn on BitLocker Drive Encryption on removable data drives. Please contact your system administrator if you need to turn on BitLocker. |
| FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED<br>0x80310079 | Group Policy settings do not permit turning off BitLocker Drive Encryption on removable data drives. Please contact your system administrator if you need to turn off BitLocker. |
| FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH<br>0x80310080 | Your password does not meet minimum password length requirements. By default, passwords must be at least 8 characters in length. Check with your system administrator for the password length requirement in your organization. |
| FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE<br>0x80310081 | Your password does not meet the complexity requirements set by your system administrator. Try adding upper and lowercase characters, numbers, and symbols. |
| FVE_E_RECOVERY_PARTITION<br>0x80310082 | This drive cannot be encrypted because it is reserved for Windows System Recovery Options. |
| FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON<br>0x80310083 | BitLocker Drive Encryption cannot be applied to this drive because of conflicting Group Policy settings. BitLocker cannot be configured to automatically unlock fixed data drives when user recovery options are disabled. If you want BitLocker-protected fixed data drives to be automatically unlocked after key validation has occurred, please ask your system administrator to resolve the settings conflict before enabling BitLocker. |
| FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON | BitLocker Drive Encryption cannot be applied to this drive because of conflicting Group Policy settings. BitLocker cannot be configured |

| Constant/Value | Description |
|---|---|
| 0x80310084 | to automatically unlock removable data drives when user recovery option are disabled. If you want BitLocker-protected removable data drives to be automatically unlocked after key validation has occurred, please ask your system administrator to resolve the settings conflict before enabling BitLocker. |
| FVE_E_NON_BITLOCKER_OID<br>0x80310085 | The Enhanced Key Usage (EKU) attribute of the specified certificate does not permit it to be used for BitLocker Drive Encryption. BitLocker does not require that a certificate have an EKU attribute, but if one is configured it must be set to an object identifier (OID) that matches the OID configured for BitLocker. |
| FVE_E_POLICY_PROHIBITS_SELFSIGNED<br>0x80310086 | BitLocker Drive Encryption cannot be applied to this drive as currently configured because of Group Policy settings. The certificate you provided for drive encryption is self-signed. Current Group Policy settings do not permit the use of self-signed certificates. Obtain a new certificate from your certification authority before attempting to enable BitLocker. |
| FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED<br>0x80310087 | BitLocker Encryption cannot be applied to this drive because of conflicting Group Policy settings. When write access to drives not protected by BitLocker is denied, the use of a USB startup key cannot be required. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker. |
| FVE_E_CONV_RECOVERY_FAILED<br>0x80310088 | BitLocker Drive Encryption cannot be applied to this drive because there are conflicting Group Policy settings for recovery options on operating system drives. Storing recovery information to Active Directory Domain Services cannot be required when the generation of recovery passwords is not permitted. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker. |
| FVE_E_VIRTUALIZED_SPACE_TOO_BIG<br>0x80310089 | The requested virtualization size is too big. |
| FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON<br>0x80310090 | BitLocker Drive Encryption cannot be applied to this drive because there are conflicting Group Policy settings for recovery options on operating system drives. Storing recovery information to Active Directory Domain Services cannot be required when the generation of recovery passwords is not permitted. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker. |
| FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON<br>0x80310091 | BitLocker Drive Encryption cannot be applied to this drive because there are conflicting Group Policy settings for recovery options on fixed data drives. Storing recovery information to Active Directory Domain Services cannot be required when the generation of recovery passwords is not permitted. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker. |
| FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON<br>0x80310092 | BitLocker Drive Encryption cannot be applied to this drive because there are conflicting Group Policy settings for recovery options on removable data drives. Storing recovery information to Active Directory Domain Services cannot be required when the generation of recovery passwords is not permitted. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker. |

| Constant/Value | Description |
|---|---|
| FVE_E_NON_BITLOCKER_KU<br>0x80310093 | The Key Usage (KU) attribute of the specified certificate does not permit it to be used for BitLocker Drive Encryption. BitLocker does not require that a certificate have a KU attribute, but if one is configured it must be set to either Key Encipherment or Key Agreement. |
| FVE_E_PRIVATEKEY_AUTH_FAILED<br>0x80310094 | The private key associated with the specified certificate cannot be authorized. The private key authorization was either not provided or the provided authorization was invalid. |
| FVE_E_REMOVAL_OF_DRA_FAILED<br>0x80310095 | Removal of the data recovery agent certificate must be done using the Certificates snap-in. |
| FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME<br>0x80310096 | This drive was encrypted using the version of BitLocker Drive Encryption included with Windows Vista and Windows Server 2008 which does not support organizational identifiers. To specify organizational identifiers for this drive upgrade the drive encryption to the latest version using the "manage-bde -upgrade" command. |
| FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME<br>0x80310097 | The drive cannot be locked because it is automatically unlocked on this computer. Remove the automatic unlock protector to lock this drive. |
| FVE_E_FIPS_HASH_KDF_NOT_ALLOWED<br>0x80310098 | The default BitLocker Key Derivation Function SP800-56A for ECC smart cards is not supported by your smart card. The Group Policy setting requiring FIPS-compliance prevents BitLocker from using any other key derivation function for encryption. You have to use a FIPS compliant smart card in FIPS restricted environments. |
| FVE_E_ENH_PIN_INVALID<br>0x80310099 | The BitLocker encryption key could not be obtained from the TPM and enhanced PIN. Try using a PIN containing only numerals. |
| FVE_E_INVALID_PIN_CHARS<br>0x8031009A | The requested TPM PIN contains invalid characters. |
| FVE_E_INVALID_DATUM_TYPE<br>0x8031009B | The management information stored on the drive contained an unknown type. If you are using an old version of Windows, try accessing the drive from the latest version. |
| FVE_E_EFI_ONLY<br>0x8031009C | The feature is only supported on EFI systems. |
| FVE_E_MULTIPLE_NKP_CERTS<br>0x8031009D | More than one Network Key Protector certificate has been found on the system. |
| FVE_E_REMOVAL_OF_NKP_FAILED<br>0x8031009E | Removal of the Network Key Protector certificate must be done using the Certificates snap-in. |
| FVE_E_INVALID_NKP_CERT<br>0x8031009F | An invalid certificate has been found in the Network Key Protector certificate store. |
| FVE_E_NO_EXISTING_PIN<br>0x803100A0 | This drive is not protected with a PIN. |

| Constant/Value | Description |
|---|---|
| FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH<br>0x803100A1 | Please enter the correct current PIN. |
| FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100A2 | You must be logged on with an administrator account to change the PIN or password. Click the link to reset the PIN or password as an administrator. |
| FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED<br>0x803100A3 | BitLocker has disabled PIN and password changes after too many failed requests. Click the link to reset the PIN or password as an administrator. |
| FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII<br>0x803100A4 | Your system administrator requires that passwords contain only printable ASCII characters. This includes unaccented letters (A-Z, a-z), numbers (0-9), space, arithmetic signs, common punctuation, separators, and the following symbols: # $ & @ ^ _ ~ . |
| FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A5 | BitLocker Drive Encryption only supports used space only encryption on thin provisioned storage. |
| FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A6 | BitLocker Drive Encryption does not support wiping free space on thin provisioned storage. |
| FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE<br>0x803100A7 | The required authentication key length is not supported by the drive. |
| FVE_E_NO_EXISTING_PASSPHRASE<br>0x803100A8 | This drive is not protected with a password. |
| FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH<br>0x803100A9 | Please enter the correct current password. |
| FVE_E_PASSPHRASE_TOO_LONG<br>0x803100AA | The password cannot exceed 256 characters. |
| FVE_E_NO_PASSPHRASE_WITH_TPM<br>0x803100AB | A password key protector cannot be added because a TPM protector exists on the drive. |
| FVE_E_NO_TPM_WITH_PASSPHRASE<br>0x803100AC | A TPM key protector cannot be added because a password protector exists on the drive. |
| FVE_E_NOT_ALLOWED_ON_CSV_STACK<br>0x803100AD | This command can only be performed from the coordinator node for the specified CSV volume. |
| FVE_E_NOT_ALLOWED_ON_CLUSTER<br>0x803100AE | This command cannot be performed on a volume when it is part of a cluster. |
| FVE_E_EDRIVE_NO_FAILOVER_TO_SW | BitLocker did not revert to using BitLocker software encryption due to group policy configuration. |

| Constant/Value | Description |
|---|---|
| 0x803100AF | |
| FVE_E_EDRIVE_BAND_IN_USE<br>0x803100B0 | The drive cannot be managed by BitLocker because the drive's hardware encryption feature is already in use. |
| FVE_E_EDRIVE_DISALLOWED_BY_GP<br>0x803100B1 | Group Policy settings do not allow the use of hardware-based encryption. |
| FVE_E_EDRIVE_INCOMPATIBLE_VOLUME<br>0x803100B2 | The drive specified does not support hardware-based encryption. |
| FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING<br>0x803100B3 | BitLocker cannot be upgraded during disk encryption or decryption. |
| FVE_E_EDRIVE_DV_NOT_SUPPORTED<br>0x803100B4 | Discovery Volumes are not supported for volumes using hardware encryption. |
| FVE_E_NO_PREBOOT_KEYBOARD_DETECTED<br>0x803100B5 | No preboot keyboard detected. The user may not be able to provide required input to unlock the volume. |
| FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED<br>0x803100B6 | No preboot keyboard or Windows Recovery Environment detected. The user may not be able to provide required input to unlock the volume. |
| FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE<br>0x803100B7 | Group Policy settings require the creation of a startup PIN, but a preboot keyboard is not available on this device. The user may not be able to provide required input to unlock the volume. |
| FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE<br>0x803100B8 | Group Policy settings require the creation of a recovery password, but neither a preboot keyboard nor Windows Recovery Environment is available on this device. The user may not be able to provide required input to unlock the volume. |
| FVE_E_WIPE_CANCEL_NOT_APPLICABLE<br>0x803100B9 | Wipe of free space is not currently taking place. |
| FVE_E_SECUREBOOT_DISABLED<br>0x803100BA | BitLocker cannot use Secure Boot for platform integrity because Secure Boot has been disabled. |
| FVE_E_SECUREBOOT_CONFIGURATION_INVALID<br>0x803100BB | BitLocker cannot use Secure Boot for platform integrity because the Secure Boot configuration does not meet the requirements for BitLocker. |
| FVE_E_EDRIVE_DRY_RUN_FAILED<br>0x803100BC | Your computer does not support BitLocker hardware-based encryption. Check with your computer manufacturer for firmware updates. |
| FVE_E_SHADOW_COPY_PRESENT<br>0x803100BD | BitLocker cannot be enabled on the volume because it contains a Volume Shadow Copy. Remove all Volume Shadow Copies before encrypting the volume. |

| Constant/Value | Description |
|---|---|
| FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS<br>0x803100BE | BitLocker Drive Encryption cannot be applied to this drive because the Group Policy setting for Enhanced Boot Configuration Data contains invalid data. Please have your system administrator resolve this invalid configuration before attempting to enable BitLocker. |
| FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE<br>0x803100BF | This PC's firmware is not capable of supporting hardware encryption. |
| FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED<br>0x803100C0 | BitLocker has disabled password changes after too many failed requests. Click the link to reset the password as an administrator. |
| FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100C1 | You must be logged on with an administrator account to change the password. Click the link to reset the password as an administrator. |
| FVE_E_LIVEID_ACCOUNT_SUSPENDED<br>0x803100C2 | BitLocker cannot save the recovery password because the specified Microsoft account is Suspended. |
| FVE_E_LIVEID_ACCOUNT_BLOCKED<br>0x803100C3 | BitLocker cannot save the recovery password because the specified Microsoft account is Blocked. |
| FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES<br>0x803100C4 | This PC is not provisioned to support device encryption. Please enable BitLocker on all volumes to comply with device encryption policy. |
| FVE_E_DE_FIXED_DATA_NOT_SUPPORTED<br>0x803100C5 | This PC cannot support device encryption because unencrypted fixed data volumes are present. |
| FVE_E_DE_HARDWARE_NOT_COMPLIANT<br>0x803100C6 | This PC does not meet the hardware requirements to support device encryption. |
| FVE_E_DE_WINRE_NOT_CONFIGURED<br>0x803100C7 | This PC cannot support device encryption because WinRE is not properly configured. |
| FVE_E_DE_PROTECTION_SUSPENDED<br>0x803100C8 | Protection is enabled on the volume but has been suspended. This is likely to have happened due to an update being applied to your system. Please try again after a reboot. |
| FVE_E_DE_OS_VOLUME_NOT_PROTECTED<br>0x803100C9 | This PC is not provisioned to support device encryption. |
| FVE_E_DE_DEVICE_LOCKEDOUT<br>0x803100CA | Device Lock has been triggered due to too many incorrect password attempts. |
| FVE_E_DE_PROTECTION_NOT_YET_ENABLED<br>0x803100CB | Protection has not been enabled on the volume. Enabling protection requires a connected account. If you already have a connected account and are seeing this error, please refer to the event log for more information. |

| Constant/Value | Description |
|---|---|
| FVE_E_INVALID_PIN_CHARS_DETAILED<br>0x803100CC | Your PIN can only contain numbers from 0 to 9. |
| FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE<br>0x803100CD | BitLocker cannot use hardware replay protection because no counter is available on your PC. |
| FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH<br>0x803100CE | Device Lockout state validation failed due to counter mismatch. |
| FVE_E_BUFFER_TOO_LARGE<br>0x803100CF | The input buffer is too large. |

18

# Glossary

Activate - Activation occurs when the computer has been registered with the Dell Enterprise Server/VE and has received at least an initial set of policies.

Active Directory (AD) - A directory service created by Microsoft for Windows domain networks.

Advanced Authentication - The Advanced Authentication product provides fully-integrated fingerprint, smart card, and contactless smart card reader options. Advanced Authentication helps manage these multiple hardware authentication methods, supports login with self-encrypting drives, SSO, and manages user credentials and passwords. In addition, Advanced Authentication can be used to access not only PCs, but any website, SaaS, or application. Once users enroll their credentials, Advanced Authentication allows use of those credentials to logon to the device and perform password replacement.

Application Data Encryption - Application Data Encryption encrypts any file written by a protected application, using a category 2 override. This means that any directory that has a category 2 protection or better, or any location that has specific extensions protected with category 2 or better, will cause ADE to not encrypt those files.

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

Cached Credentials - Cached credentials are credentials that are added to the PBA database when a user successfully authenticates with Active Directory. This information about the user is retained so that a user can log in when they do not have a connection to Active Directory (for example, when taking their laptop home).

Common Encryption – The Common key makes encrypted files accessible to all managed users on the device where they were created.

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

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

EMS Access Code - This service within the Dell Enterprise Server/VE allows for recovery of External Media Shield protected devices where the user forgets their password and can no longer login. Completing this process allows the user to reset the password set on the removable media or external storage device.

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

Endpoint - a computer or mobile hardware device that is managed by Dell Enterprise Server/VE.

Encryption 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 Shielded Windows (or Mac) device.

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

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

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

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.

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

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

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 in order 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. The TPM is also required for use with BitLocker Manager and the One-time Password feature.

User Encryption – The User key makes files accessible only to the user who created them, only on the device where they were created. When running Dell Server Encryption, User Encryption is converted to Common Encryption. One exception is made for external media devices; when inserted into a server with Encryption installed, files are encrypted with the User Roaming key.