

Dell Data Protection | Encryption

Enterprise Edition Administrator Guide

DDP|E Encryption Client, SED, Advanced Authentication,
BitLocker Manager, and Cloud Edition



© 2014 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

2014-08

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

- Introduction 11
- Requirements 13
 - Encryption Client 13
 - SED Client 17
 - Advanced Authentication Client 19
 - BitLocker Manager Client 21
 - Cloud Edition Client 22
 - Interoperability 25
- Pre-Installation Configuration to Enable DDP|HCA..... 27
 - Upgrade Legacy HCA Computers. 27
 - Requirements. 27
 - Upgrade Legacy HCA Computers 27
 - DDP|HCA Pre-Installation BIOS Configuration 29
 - Reset System Password 30
- Pre-Installation Configuration to Set Up a BitLocker PBA Partition 31
- Set GPO on Domain Controller to Enable Entitlements 33

Extract the Child Installers from the Master Installer	37
Commonly Used Scenarios	39
DDP E Client and Advanced Authentication	40
SED Client (including Advanced Authentication) and External Media Edition	41
SED Client (including Advanced Authentication), External Media Edition, and Cloud Edition	42
DDP E Client and Cloud Edition	44
BitLocker Manager and External Media Edition	45
BitLocker Manager, External Media Edition, and Cloud Edition	45
SED Client (including Advanced Authentication), DDP E Client, and Cloud Edition	46
DDP E Client and Advanced Authentication for Computers with HCA	48
Section I. Dell Data Protection Installer (Master Installer).	51
Dell Data Protection Master Installer	53
Install DDP E Interactively	54
Install DDP E Using the Command Line	59
Uninstallation Process	60

Section II.	Drivers	61
	Drivers Installation Tasks	63
	Install Drivers	63
	Command Line Installation	63
Section III.	DDP E Encryption Client	65
	Encryption Client Installation Tasks	67
	Best Practices.	67
	Install Encryption Client.	67
	Command Line Installation	68
	Install External Media Edition (EME)	69
	Convert External Media Edition to Enterprise Edition	70
	Create a Custom Transform File	70
	Encryption Client Uninstallation and Decryption Tasks	73
	Best Practices.	73
	Prerequisites	73
	Uninstall Encryption Client.	74
	Command Line Uninstallation	74
	Uninstall External Media Edition.	76
	How to Create an Encryption Removal Agent Log File (Optional).	77
	Check Encryption Removal Agent Status.	77
	Encryption Client Data Recovery.	79
	Prerequisites	79
	Retrieve the Recovery Bundle.	79
	Recover Data	79

Troubleshooting HCA Recovery	83
Check the Recovery Log File	83
When Escrow Cannot Be Completed during the WinPE Recovery (HCA)	83
Reset TPM Security (HCA)	83
Recover User Access to a Computer Equipped with HCA	84
Self-Recovery	84
Recover Access using Challenge/Response Codes.	86
Assisted Recovery.	86
Configure Dell Key Server	87
Windows Service Instructions	87
Key Server Config File Instructions	87
Sample Configuration File	88
Windows Service Instructions	88
Remote Management Console Instructions	89
Use WSScan	91
Section IV. SED Management and Advanced Authentication	93
SED Management and Advanced Authentication Installation Tasks	95
Best Practices.	95
Install SED Management and Advanced Authentication.	95
Command Line Installation	96
SED and Advanced Authentication Deactivation and Uninstallation Tasks	99
Prerequisites	99
Deactivate the PBA	99

Uninstall SED Client	100
Command Line Uninstallation	100
SED and OS Recovery	103
Self-Recovery, OS Logon	103
Self-Recovery, PBA	106
Assisted Recovery, PBA	108
Prerequisites	108
Retrieve the Recovery Bundle	108
How to Turn Off Manager SSL Trust Validation	109
How to Use the Initial Access Code Policy	111
How to Create a PBA Log File for Troubleshooting.	112
Section V. User Experience - Credential Management and Authentication Applications	113
Configure Credentials in the Security Console	115
Use the Authentication Applications.	123
Credentials.	124
Enrollment Status	124
Backup and Restore	126
Back up Data	127
Restore Data	129
Password Manager	131
Website and Application Logon Training	131
Add Logon	132
Icon Context Menu	134
Web Domain Support	135

	Logging on to Trained Logon Screens	135
	Filling in with Windows Credentials	136
	Use Old Password	137
	Password Change	138
	Password Manager Page.	139
	Settings Page.	141
Section VI.	BitLocker Manager	143
	BitLocker Manager Installation Tasks.	145
	Best Practices.	145
	Install BitLocker Manager	145
	Command Line Installation	145
	BitLocker Manager Uninstallation Tasks.	147
	Prerequisites	147
	Uninstall BitLocker Manager	147
	Command Line Uninstallation	147
	BitLocker Manager Recovery	149
	Recover Data	149
	How to Turn Off Manager SSL Trust Validation.	151
Section VII.	Cloud Edition	153
	Cloud Edition Installation Tasks.	155
	DDP Server Tasks	155
	Configure DDP Enterprise Server - VE for Cloud Edition	155
	Configure Dell Enterprise Server for Cloud Edition	155
	Allow/Deny Users on Whitelist /Blacklist.	156

Use Dropbox for Business	158
Run Reports.	160
Provide Temporary Folder Management Rights	160
Update Cloud Edition Policy	160
Client Tasks	161
Before Installing	161
Best Practices	161
Install Cloud Edition	161
Notify End Users	162
Activate Cloud Edition and Install a Cloud Sync Client	162
Cloud Edition Uninstallation Tasks	163
Prerequisites	163
Remove Protected Files.	163
Dropbox	163
Box.	164
OneDrive	164
Uninstall Cloud Edition	164
Command Line Uninstallation	164

Section VIII. User Experience - Cloud Edition 167

Cloud Edition Activation and User Experience	169
Activate Cloud Edition.	169
Install a Cloud Sync Client	169
Authenticate Dropbox for Business	170
Sync Folders.	170
Dropbox for Business	170
Box.	171
OneDrive	171
Work with Folders and Files	171
Cloud Storage Provider Help	171


Pre-existing Folders with Unencrypted Files.	171
Access a Cloud Storage Provider	172
Dropbox for Business	173
Connect Cloud Edition and Dropbox.	173
Use Dropbox for Business Context Menu	173
Use Business and Personal Dropbox Accounts.	173
Understand the Cloud Edition System Tray Menu Items	174
Details Screen	174
Cloud Edition Manage Folders Menu	175
Using Cloud Edition with iOS or Android	176
Prerequisite.	176
Cloud Edition on an iOS device.	176
Cloud Edition on an Android device	176
Share Files With External Users	177
Administrator Tasks	177
External User Tasks	177
Cloud Edition Frequently Asked Questions (FAQs)	178
Administrator FAQs	178
Folder Management FAQs	179
Dropbox FAQs	180
Box Sync Client FAQs	180
Miscellaneous FAQs.	181
Appendix A Change Secure Boot/UEFI to Legacy Boot Mode in BIOS	183
Glossary	185

Introduction

This guide details how to install and configure the DDP|E encryption client, SED management client, Advanced Authentication (and its drivers), BitLocker Manager, and Cloud Edition.

You can install all the clients together using the master installer user interface or individually by extracting the child installers out of the master installer and then installing them by command line (or user interface). The clients can be installed using any push technology available to your organization.

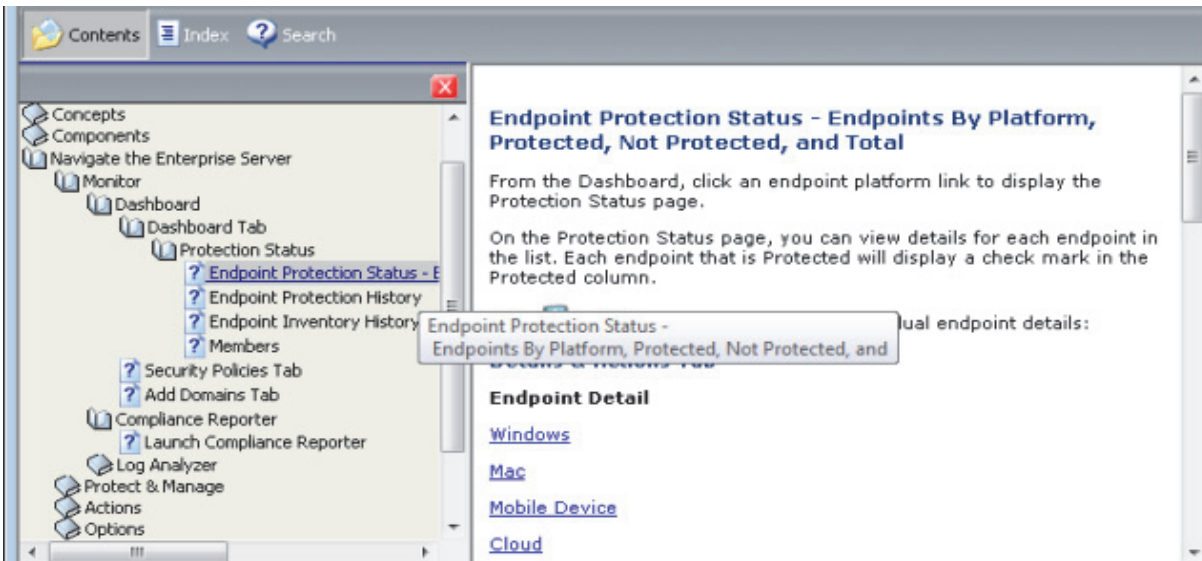
Generally, the best practice is to follow this order:

- 1 Install the Dell Enterprise Server or DDP Enterprise Server – VE (Virtual Edition) before deploying clients. If you have not yet installed the Server, locate the appropriate guide as shown below, follow the instructions, and then return to this guide.
 - *DDP Enterprise Server Installation and Migration Guide*
After Server installation, either apply a policy template at the Enterprise level or apply policies individually as appropriate to specific domains, user groups, endpoint groups, users, or endpoints.
 - *DDP Enterprise Server – Virtual Edition Quick Start Guide and Installation Guide*
After Server installation, verify that policies are set as desired for Enterprise, domains, user groups, endpoint groups, users, and endpoint levels.
- 2 Access the AdminHelp from  in the Remote Management Console. From the Table of Contents, go to *Manage Policies* to learn about platforms and how to use each policy.



- 3 Deploy the appropriate client (or clients) to end users.
- 4 Learn how to monitor your Enterprise and issue commands.

From the AdminHelp Table of Contents, go to Navigate the Enterprise Server > Monitor > Dashboard > Dashboard Tab > Protection Status > *Endpoint Protection Status - Endpoints By Platform, Protected, Not Protected, and Total*.



Be sure to periodically check www.dell.com/support for updated documentation.

Use this guide in the following order:

- [Requirements](#)
- If needed, see [Pre-Installation Configuration to Enable DDP|HCA](#)
- If needed, see [Pre-Installation Configuration to Set Up a BitLocker PBA Partition](#)
- If your clients will be entitled from the Dell factory or if you purchase licenses from the Dell factory, see [Set GPO on Domain Controller to Enable Entitlements](#)

NOTE: If your clients will be entitled from the Dell factory or if you purchase licenses from the Dell factory, ensure that outbound port 443 is available to communicate with the Server. If port 443 is blocked (for any reason), the entitlement functionality will not work.

- If you intend to install the clients together from the master installer user interface, see [Dell Data Protection Master Installer](#)
- If you intend to install the clients individually, see [Extract the Child Installers from the Master Installer](#) and then:

Select the client or clients to deploy:

- [Encryption Client Installation Tasks](#)
- [Drivers Installation Tasks](#) (required if using Advanced Authentication on Dell hardware or if installing the encryption client)
- [SED Management and Advanced Authentication Installation Tasks](#)
- [BitLocker Manager Installation Tasks](#)
- [Cloud Edition Installation Tasks](#)
- If you already understand the products and want to work with a list of our most commonly used scenarios, see [Commonly Used Scenarios](#).

Requirements

Encryption Client

- The user account performing the installation must be a local or domain Admin user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or KACE. A non-Admin user that has elevated privileges is not supported.
- To successfully install DDP|E, the computer must have network connectivity.
- If you intend to use [Hardware Crypto Accelerator \(HCA\) policies](#), you must first set up the [Trusted Platform Module \(TPM\)](#), and if setting up a computer with [legacy HCA](#), create a System password. Follow the instructions detailed in [Pre-Installation Configuration to Enable DDP|HCA](#) prior to DDP|E installation.
- The features available as of v8.3 with HCA are supported on legacy BIOS non-UEFI computers. If running **Windows 8** or **Windows 8.1**, follow the instructions detailed in [Change Secure Boot/UEFI to Legacy Boot Mode in BIOS](#) prior to client installation.
- Windows 8.1 should not be installed on drive 1 on HCA-enabled computers. This operating system configuration is not supported because Windows 8.1 creates a recovery partition on drive 0 which in turn, breaks Preboot Authentication. Instead, either install Windows 8.1 on the drive configured as drive 0, or restore Windows 8.1 as an image to any of the drives.
- Non-UEFI computers can have up to four primary partitions. When the PBA is installed on a client computer, it needs to create and use one of the four partitions for the startup partition, also called the [Preboot Authentication \(PBA\)](#) partition. If all four partitions are already in use on a client computer, then the HCA card will fail to activate on it.
- Before configuring Preboot Authentication (PBA) on a computer equipped with an HCA card, ensure that the computer has a network connection to the DDP Server.
- HCA features for v8.3 and later do not support RAID configuration. *Legacy* HCA features (pre-v8.3) can be configured using RAID.

Client Prerequisites

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

Prerequisites
• Microsoft Visual C++ 2012 Update 3 or later Redistributable Package (x86 and x64)
• Microsoft SQL Server Compact 3.5 SP2 (x86 and x64)
• Microsoft .NET Framework v4.0

BEST PRACTICE: Potential installation problems can be avoided if Microsoft .NET Framework is installed on the target computer prior to client installation.

Hardware Requirements

The following table details supported hardware.

Windows Hardware
• Intel Pentium-class or AMD processor
• 512 MB-1GB RAM
• +110 MB of free disk space plus
• 250 MB free space in Preboot Authentication partition

Optional Embedded Hardware
• Trusted Platform Module (TPM) chipset with TCG Software Stack (TSS) version 1.2.1.42

NOTE: TSS is a component that interfaces with the Trusted Platform Module (TPM). To find the TSS version, go to (default location) C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcscd_win32.exe. Right-click the file and select **Properties**. Verify the file version on the *Details* tab.

• Dell Data Protection Hardware Crypto Accelerator
--

NOTE: Enterprise PBA is supported on Microsoft Windows 7, Microsoft Windows 8, and Microsoft Windows 8.1 on Dell X5 and X4 computers, model numbers listed below.

Legacy PBA is not supported on Microsoft Windows 8 or Microsoft Windows 8.1. Legacy PBA is supported on Microsoft Windows 7 only, on Dell X4 computers, model numbers listed below.

Model Name	Enterprise PBA	Legacy PBA
Latitude E6420 ATG		✓
Latitude E6420 XFR		✓
Latitude XT3		✓
Latitude E6430u		✓
Latitude E6530		✓
Latitude E6230		✓
Latitude E6330		✓
Latitude E6430s		✓
Latitude E6430		✓
Latitude E6430 ATG		✓
Latitude E5430		✓
Latitude E5530		✓
Latitude E7240	✓	✓
Latitude E7440	✓	✓
Latitude E6440	✓	✓
Latitude E6540	✓	✓
Precision M4600		✓
Precision M6600		✓
Precision M4700		✓

Windows Hardware		
Precision M6700		✓
Precision M4800	✓	✓
Precision M6800	✓	✓
Precision T3600		✓
Precision T3610	✓	
Precision T5600		✓
Precision T5610	✓	
Precision T7600		✓
Precision T7610	✓	
Precision T1650		✓
Precision T1700	✓	✓
OptiPlex 9010 AIO		✓
OptiPlex 9010		✓
OptiPlex 7010	✓	✓
OptiPlex 7020	✓	
OptiPlex XE2	✓	✓
OptiPlex 9020 AIO	✓	✓
OptiPlex 9020	✓	✓
OptiPlex 9020 Micro	✓	
OptiPlex 9030 AIO	✓	

Operating Systems

The following table details supported operating systems.

NOTE: The Encryption client does not support dual boot configurations as it is possible to encrypt system files of the other operating system, which would interfere with its operation.
XP Mode is not compatible with the Encryption client, it is designed to run Microsoft Windows 7 or later natively.

Windows Operating Systems (32- and 64-bit)
<ul style="list-style-type: none"> • Microsoft Windows XP SP3 <ul style="list-style-type: none"> - Professional Edition
NOTE: Software encryption only is supported on Microsoft Windows XP SP3.
<ul style="list-style-type: none"> • Microsoft Windows 7 SP0-SP1 <ul style="list-style-type: none"> - Enterprise - Professional - Ultimate

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 8
 - Enterprise
 - Pro
 - Microsoft Windows 8.1 - Windows 8.1 Update 1
 - Enterprise Edition
 - Pro Edition
 - Windows Embedded 8.1
 - Industry Enterprise
 - VMware Workstation 5.5 and higher
 - Windows Embedded Standard 7 in Application Compatibility Mode
-

Operating Systems for External Media Edition (EME)

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

NOTE: To host External Media Shield (EMS), removable storage must have approximately 55MB available plus open space on the media that is equal to the largest file to be encrypted.

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

- Microsoft Windows XP SP3
 - Professional Edition
 - Home Edition
 - Media Center Edition

NOTE: Software encryption **only** is supported on Microsoft Windows XP SP3.

- Microsoft Windows 7 SP0-SP1
 - Enterprise
 - Professional
 - Ultimate
 - Home Premium

- Microsoft Windows 8
 - Enterprise
 - Pro
 - Windows 8 (Consumer)

- Microsoft Windows 8.1 - Windows 8.1 Update 1
 - Enterprise Edition
 - Pro Edition
-

Language Support

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

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

SED Client

- The user account performing the installation must be a local or domain Admin user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or KACE.
- To successfully install SED management, the computer must have network connectivity.
- Be prepared to shutdown and restart the computer after you apply policies and are ready to begin enforcing them.
- Windows 8.1 should not be installed on drive 1 on self-encrypting drives. This operating system configuration is not supported because Windows 8.1 creates a recovery partition on drive 0 which in turn, breaks Preboot Authentication. Instead, either install Windows 8.1 on the drive configured as drive 0, or restore Windows 8.1 as an image to any of the drives.
- The SED management client does not support UEFI Secure Boot with self-encrypting drives on Windows 8 or Windows 8.1. For more information about UEFI, see http://en.community.dell.com/techcenter/extras/m/white_papers/20278835.aspx.
- Supported Opal compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at <http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA>.

NOTE: IPv6 is not supported.

IMPORTANT: Due to the nature of RAID and SEDs, SED management supports RAID only with the Intel Rapid Storage Technology Driver configured to use a single disk. 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."

Drivers

- Intel Rapid Storage Technology Driver
<http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA>

Client Prerequisites

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

Prerequisites

- Microsoft Visual C++ 2012 Update 3 or later Redistributable Package (x86 and x64)
- Microsoft .NET Framework v4.0

BEST PRACTICE: Potential installation problems can be avoided if Microsoft .NET Framework is installed on the target computer prior to client installation.

Opal Compliant SEDs

Drives with “X” are supported for SED management but are not qualified for or shipped in Dell systems.

Drive	Availability	Standard
Seagate ST320LT009 (FIPS Julius)	✓	Opal 1
Seagate ST500LT015 (Yarra 1D FIPS 500)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D non-FIPS 500)	X	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS)	✓	Opal 2
Travelstar 5K750 series	X	Opal
Travelstar 7K750 series	X	Opal
Travelstar Z5K320 series	X	Opal
MKxx61GSYD series	X	
MKxx61GSYG series	X	
Samsung SM841 OPAL SSD	✓	Opal 2
Samsung SM841N OPAL SSD	✓	Opal 2
LiteOn L9M OPAL SSD (Model: LMT-256L9M-41)	✓	Opal 2
LiteOn M3 series SSD	✓	Opal 1
LiteOn M6 series SSD	✓	Opal 2
Micron RealSSD C400 SSD	X	Opal 1

Operating Systems

The following table details the supported operating system.

Windows Operating Systems (32- and 64-bit)
<ul style="list-style-type: none">• Microsoft Windows 7 SP0-SP1<ul style="list-style-type: none">- Enterprise- Professional
<ul style="list-style-type: none">• Microsoft Windows 8<ul style="list-style-type: none">- Enterprise- Professional- Windows 8 (Consumer)
<ul style="list-style-type: none">• Microsoft Windows 8.1<ul style="list-style-type: none">- Enterprise Edition- Pro Edition

Language Support

The SED client is Multilingual User Interface (MUI) compliant and supports the following languages.

NOTE: PBA localization is not supported in Russian, Traditional Chinese, or Simplified Chinese.

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

Advanced Authentication Client

Hardware

The following table details supported Dell hardware. Drivers for fingerprint readers and smart cards are located in the client installation package. Other hardware vendors may require their own drivers.

Fingerprint and Smart Card Readers
<ul style="list-style-type: none">• Validity VFS495 in Secure Mode
<ul style="list-style-type: none">• Broadcom ControlVault Swipe Reader
<ul style="list-style-type: none">• UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
<ul style="list-style-type: none">• Authentec Eikon and Eikon To Go USB Readers

Smart Cards

- PKCS #11 Smart Cards using the [ActivIdentity](#) client

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

- CSP Cards

- Common Access Cards (CACs)

NOTE: With CACs that have more than one certificate, at logon, the user selects the correct certificate from a list.

Contactless Cards

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

Operating Systems

The following table details supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 7 SP0-SP1
 - Enterprise
 - Professional
 - Ultimate

- Microsoft Windows 8
 - Enterprise
 - Pro

- Microsoft Windows 8.1 - Windows 8.1 Update 1
 - Enterprise Edition
 - Pro Edition

Language Support

The Advanced Authentication client is Multilingual User Interface (MUI) compliant and supports the following languages.

Language Support

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

BitLocker Manager Client

- If Windows BitLocker is not yet deployed in your environment, consider reviewing [BitLocker requirements](#).
- The user account performing the installation must be a local or domain Admin user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or KACE.
- 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](#).
- Turn on and enable the TPM. BitLocker Manager will take ownership of the TPM and will not require a reboot. However, if 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 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.

Client Prerequisites

The installer installs this component if not already installed on the computer.

Prerequisites
<ul style="list-style-type: none">• Microsoft .NET Framework v4.0
BEST PRACTICE: Potential installation problems can be avoided if Microsoft .NET Framework is installed on the target computer prior to client installation.

Hardware

The following table details supported hardware.

Hardware
<ul style="list-style-type: none">• Intel Pentium-class processors

Operating Systems

The following table details supported operating systems.

Windows Operating Systems
<ul style="list-style-type: none">• Microsoft Windows 7 SP0-SP1 (32- and 64-bit)<ul style="list-style-type: none">- Enterprise- Ultimate
<ul style="list-style-type: none">• Microsoft Windows 8 (64-bit)<ul style="list-style-type: none">- Enterprise Edition
<ul style="list-style-type: none">• Microsoft Windows 8.1 (64-bit)<ul style="list-style-type: none">- Enterprise Edition- Pro Edition
<ul style="list-style-type: none">• Microsoft Windows Server 2008 R2 (64-bit)<ul style="list-style-type: none">- Standard Edition- Enterprise Edition

Language Support

BitLocker Manager is Multilingual User Interface (MUI) compliant and supports the following languages.

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

Cloud Edition Client

- The user account performing the installation must be a local or domain Admin user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or KACE.
- Cloud Edition can be used with DDP|E v7.2.4 or later.
- Ensure that target devices have connectivity to <https://yoursecurityservername.domain.com:8443/cloudweb/register> and <https://yoursecurityservername.domain.com:8443/cloudweb>.
- Before deploying Cloud Edition, it is best if the target devices do not yet have Dropbox, Box, or OneDrive accounts set up. This is not essential, but it prevents problems with data ownership.

Should end users decide to keep their existing accounts, they should ensure that any files that are to remain *unencrypted* are moved out of Dropbox, Box, or OneDrive before installing Cloud Edition.

- End users should be prepared to restart Windows computers after the client is installed.
- Cloud Edition does not interfere with the behavior of Dropbox, Box, or OneDrive. Therefore, Administrators and end users should familiarize themselves with how these applications work prior to deploying Cloud Edition. For more information, see Box support at <https://support.box.com/home>, Dropbox support at <https://www.dropbox.com/help>, or OneDrive support at <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.

NOTE: IPv6 is not supported.

Client Prerequisites

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

Prerequisites
• Microsoft Visual C++ 2010 SP1 Redistributable Package (x86 and x64)
• Microsoft .NET Framework 4.0 Client Profile

Cloud Sync Clients

The following table details the latest tested sync clients. Sync clients release updates fairly frequently; later released versions may work properly with DDP|CE, but should be tested prior to rolling out in a production environment.

Cloud Sync Clients
<ul style="list-style-type: none">Dropbox 2.4-2.12 <p>- Dropbox for Business requires Dropbox version 2.8 or later plus the DDP Enterprise Server - Virtual Edition (VE) v8.4 or later</p> <p>NOTE: With a pre-v8.4 VE Server or a Dell Enterprise Server, the client protects all files and folders. With VE v8.4 or later, a user can upload files to a personal Dropbox account; based on policy, those files can remain unprotected.</p>
<ul style="list-style-type: none">Box 3.4, 4.0
<ul style="list-style-type: none">OneDrive 17.0

Hardware

The following table details supported hardware for the Windows client.

Windows Hardware
<ul style="list-style-type: none">Intel Pentium-class or AMD processor
<ul style="list-style-type: none">512 MB-2 GB RAM, depending on operating system
<ul style="list-style-type: none">15 GB-20 GB free disk space, depending on operating system
<ul style="list-style-type: none">10/100/1000 or Wi-Fi network interface card
<ul style="list-style-type: none">TCP/IP installed and activated

Operating Systems

The following table details supported operating systems.

Windows Operating Systems (32-bit and 64-bit)
• Microsoft Windows 7 SP0-SP1
• Microsoft Windows 8
• Microsoft Windows 8.1 (Box and Dropbox only)
Android Operating Systems
• 4.0 Ice Cream Sandwich
• 4.1 - 4.3 Jelly Bean
• 4.4 KitKat
iOS Operating Systems
• iOS 5.x
• iOS 6.x
• iOS 7.x

Interoperability

Deprovision and Uninstall Dell Data Protection | Access

If DDP|A is installed now or has been installed in the past on your computer, **before** installing the Encryption client, SED, or Advanced Authentication, you must deprovision the DDP|A-managed hardware and then uninstall DDP|A. If DDP|A has not been used, you may simply uninstall DDP|A and restart the installation process.

Deprovisioning DDP|A-managed hardware includes the fingerprint reader, smart card reader, BIOS passwords, TPM, and the Self-Encrypting Drive.

NOTE: If running DDP|E encryption products, stop or pause an encryption sweep. If running Microsoft BitLocker, suspend the encryption policy. Once DDP|A is uninstalled and Microsoft BitLocker policy is unsuspended, initialize the TPM by following the instructions located at <http://technet.microsoft.com/en-us/library/cc753140.aspx>.

Deprovision DDP|A-Managed Hardware

- 1 Launch DDP|A and click the *Advanced* tab.
- 2 Select **Reset System**. This will require that you enter any provisioned credentials to verify your identity. After DDP|A verifies the credentials, DDP|A will perform the following actions:
 - Remove all provisioned credentials from Dell ControlVault (if present)
 - Remove Dell ControlVault owner password (if present)
 - Remove all provisioned fingerprints from integrated fingerprint reader (if present)
 - Remove all BIOS passwords (BIOS System, BIOS Admin, and HDD passwords)
 - Clear the Trusted Platform Module
 - Remove the DDP|A Credential ProviderOnce the computer is deprovisioned, DDP|A reboots the computer to restore the Windows default credential provider.

Uninstall DDP|A

Once the authentication hardware is deprovisioned, uninstall DDP|A.

- 1 Launch DDP|A and perform a Reset System.
This will remove all DDP|A managed credentials and passwords and will clear the Trusted Platform Module (TPM).
- 2 Click **Uninstall** to launch the installer.
- 3 When the uninstall finishes, click **Yes** to restart.

NOTE: If using a self-encrypting drive, removing DDP|A will also unlock the SED and remove the Preboot Authentication.

Initialize the TPM

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

Pre-Installation Configuration to Enable DDP|HCA

If the computer targeted for encryption is equipped with a Dell Data Protection | Hardware Crypto Accelerator (HCA) and you intend to use Hardware Crypto Accelerator (HCA) policies, you must first set up and activate the TPM. If using legacy HCA, you need to set up a System password.

Follow the instructions detailed in this section to configure DDP|HCA **prior** to the Encryption client installation.

NOTE: The features available as of v8.3 with Enterprise PBA are supported on legacy BIOS non-UEFI computers. If running Windows 8 or Windows 8.1, follow the instructions detailed in [Change Secure Boot/UEFI to Legacy Boot Mode in BIOS](#) prior to performing these steps.

Upgrade Legacy HCA Computers

Requirements

- Computers running legacy BIOS must upgrade to an enterprise BIOS.
- The computer must have at least one partition free to accommodate the Preboot Authentication (PBA) partition.

Upgrade Legacy HCA Computers

To upgrade legacy HCA computers, follow these steps:

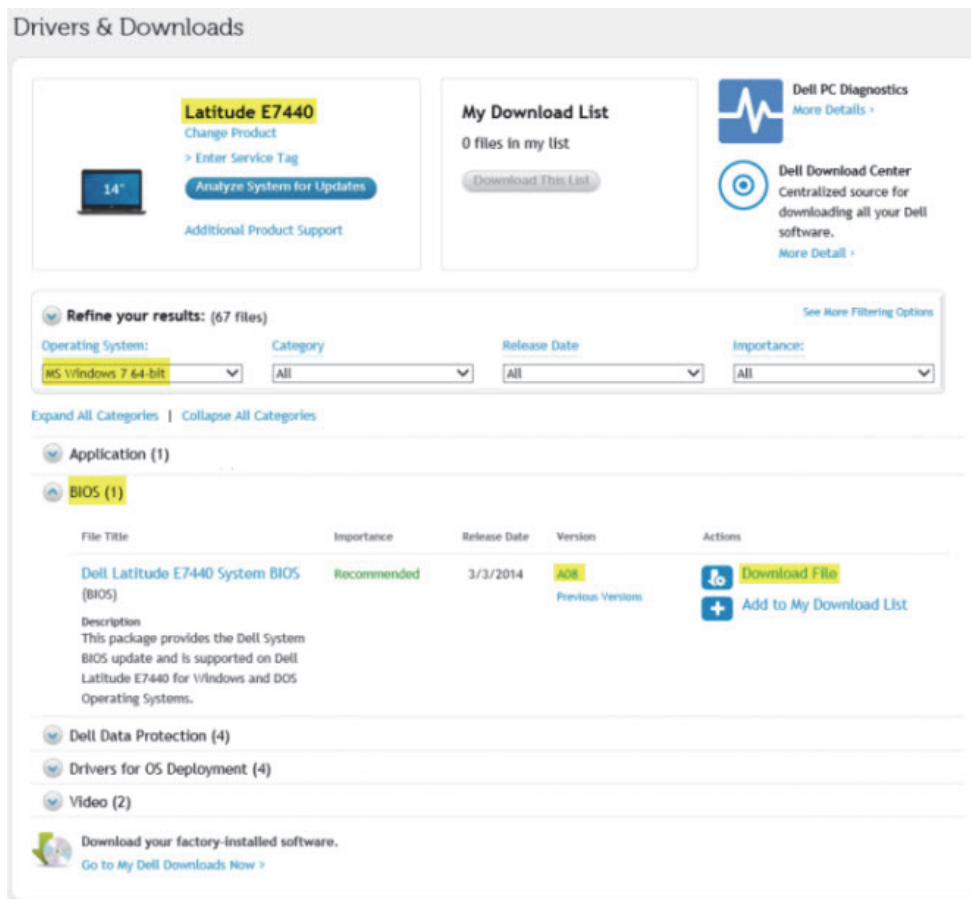
- 1 Disable HCA policies and apply the policy change.
- 2 Wait for hard drives to be decrypted.
- 3 Uninstall the Encryption client and Security Tools (if needed).
- 4 Upgrade the BIOS.
 - a Close all applications.
 - b Go to support.dell.com.
 - c In **General support > Select a product**, click **Laptops** if Latitude or **Desktops & All-in-Ones** if Precision or Optiplex.
 - d Select your model.

TIP: The following computers need the updated BIOS versions to run Enterprise PBA.

Computer	BIOS Needed
Latitude E6440	A05
Latitude E6540	A08
Latitude E7240	A08
Latitude E7440	A08
OptiPlex 7010	A16
OptiPlex 9020	A05
OptiPlex 9020 AIO	A06

Computer	BIOS Needed
OptiPlex XE2	A05
Precision M4800	A07
Precision M6800	A07
Precision T1700	A06

- e Select **Get drivers and downloads** in the left menu.
- f Click **View All Drivers**.
- g Scroll down to **Refine your results** and expand the **BIOS** drop-down. Download and install the updated BIOS, following the prompts in the BIOS installer package. The following example displays a Latitude E7440.



- 5 Install the product using the DDPSetup.exe file. Using DDPSetup.exe installs the Encryption client and Advanced Authentication.
- 6 Re-apply HCA policies and apply the change.

DDP|HCA Pre-Installation BIOS Configuration

If the following hardware and BIOS instructions are not completed, are inaccurate, or are otherwise not met, the Encryption client ignores HCA policies and software encryption is implemented.

1 Boot into the BIOS Configuration:

- Press F2 or F12 continuously during boot until a message in the upper right screen is similar to “preparing to enter setup” (F2) or “preparing one-time boot menu” (F12). Enter **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.

2 If the computer is equipped with legacy HCA, follow this step. Otherwise, skip to [step 4](#).

Define the BIOS Administrator Password if not already configured:

- Under **Settings**, click the + (plus) sign next to **Security**, and then click **Admin Password**. You must complete this step before you can create a System (Preboot) password.
- Enter your new Admin password information and click **Apply**.

3 If the computer is equipped with legacy HCA, follow this step. Otherwise, skip to [step 4](#).

Define a System (Preboot) Password if not already configured:

- Click **System Password** in the same menu.
- Enter your new System Password information and click **Apply**.

IMPORTANT: Before performing **Steps 4 and 5**, understand that you should **never** clear TPM or DDP|HCA ownership after HCA policies have been implemented. If you ignore the BIOS warning and clear the TPM or HCA after policies have been implemented, you will lose access to the encrypted hard drive and must complete a recovery process to regain access.

4 Clear and activate the TPM:

- Click **TPM Security** in the same menu.
- Select the **Clear** option and click **Apply**.
- Select the **Activate** option and click **Apply**.

5 Clear HCA ownership:

- Click **Dell Encryption** in the same menu.
- Select the **Clear Owner** check box.
- Click **Yes** at the warning dialog and then click **Apply**.
- Click **Exit**.

NOTE: If the check box is grayed out, it is *Owned*. If the HCA ownership check box will not clear, select **Load Default** and then **Exit**.

6 If the computer is equipped with legacy HCA, enter the System (Preboot) Password:

- After exiting the BIOS configuration you will be prompted for the System (Preboot) password defined in [step 3](#).
- DDP|HCA pre-installation configuration is complete.

7 Log in to Windows:

- Log in with local or domain Admin credentials when the computer boots to Windows.

Reset System Password

If the computer is equipped with legacy HCA, and you forget your System password, log in with the BIOS Admin password and assign a new System password as described in [DDP|HCA Pre-Installation BIOS Configuration](#). If the BIOS password is also unknown, you must contact Dell support to reset the passwords (refer to your Welcome Letter for contact information).

Pre-Installation Configuration to Set Up a BitLocker PBA Partition

- You must create the PBA partition **before** installing BitLocker Manager.
- 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
```

For more options available for the BdeHdCfg command, see [Microsoft's BdeHdCfg.exe Parameter Reference](#).

NOTE: You may need to partition the disk manually. See [Microsoft's Description of the BitLocker Drive Preparation Tool](#) for further instructions.

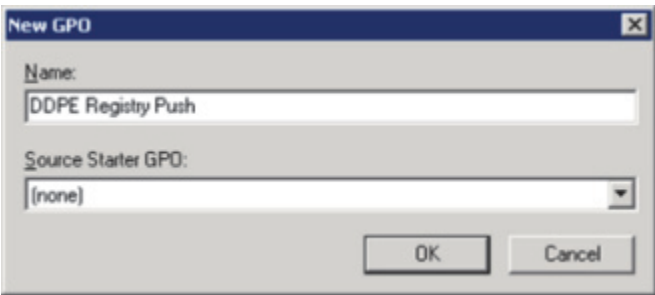
Before installing BitLocker Manager, turn on and activate the TPM. BitLocker Manager will take ownership of the TPM and will not require a reboot. However, if TPM ownership already exists, BitLocker Manager will begin the encryption setup process. The point is that the TPM must be “owned”.

Set GPO on Domain Controller to Enable Entitlements

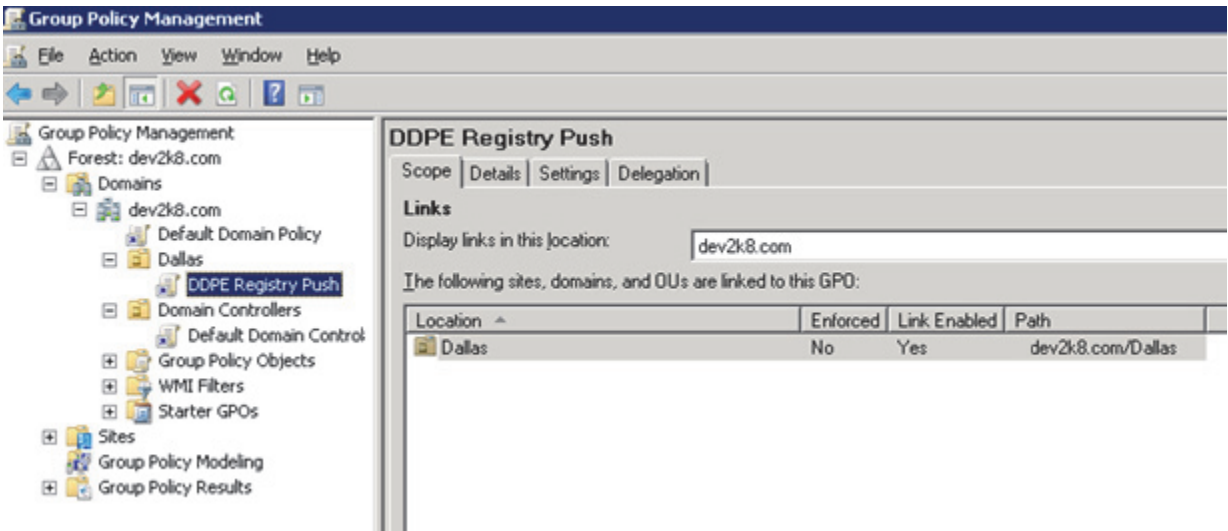
- If your clients will be entitled from the factory or you purchase licenses from the factory, follow these instructions to set the GPO on the domain controller to enable entitlements (this may not be the same server running Enterprise Edition).
- The workstation must be a member of the OU where the GPO is applied.

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

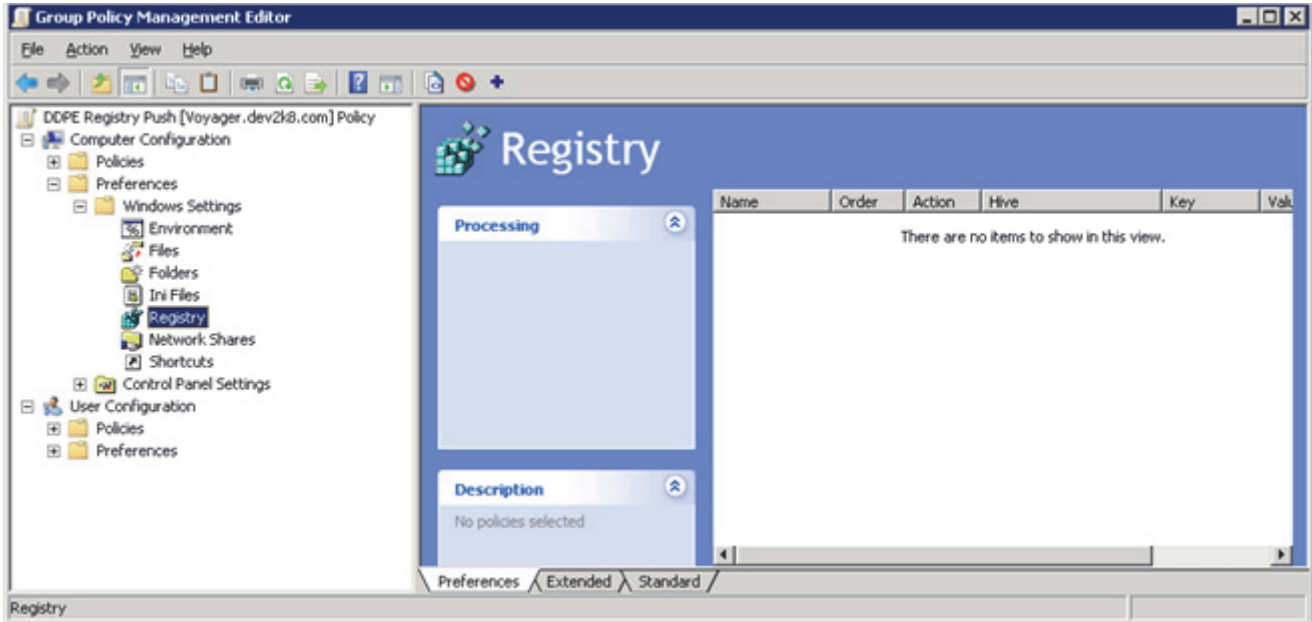
- 1 On the Domain Controller to manage the clients, click **Start > Administrative Tools > Group Policy Management**.
- 2 Right-click the OU where the policy should be applied and select **Create a GPO in this domain, and Link it here....**
- 3 Enter a name for the new GPO, select (none) for Source Starter GPO, and click **OK**.



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



- 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

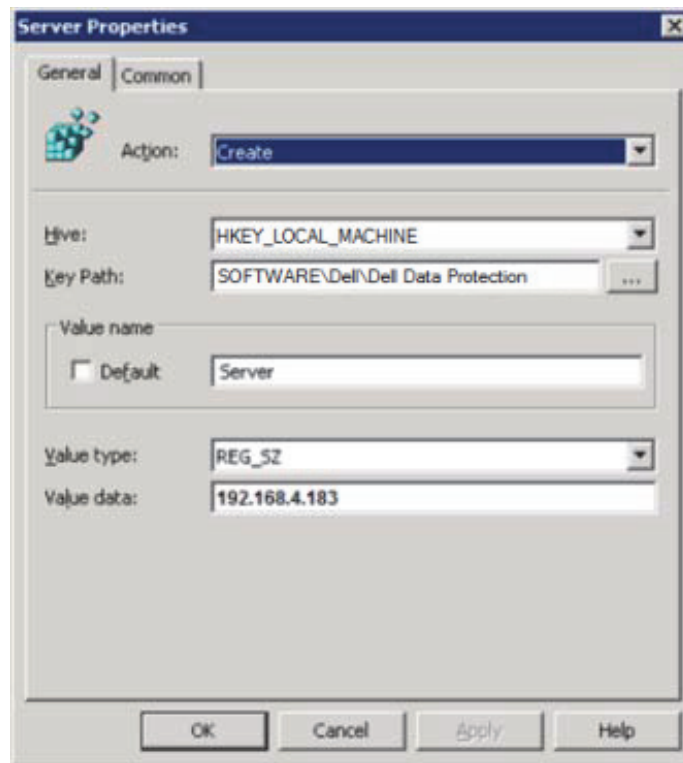
Key Path: SOFTWARE\Dell\Dell Data Protection

Value name: Server

Value type: REG_SZ

Value data: <IP address of Server>

7 Click OK.



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

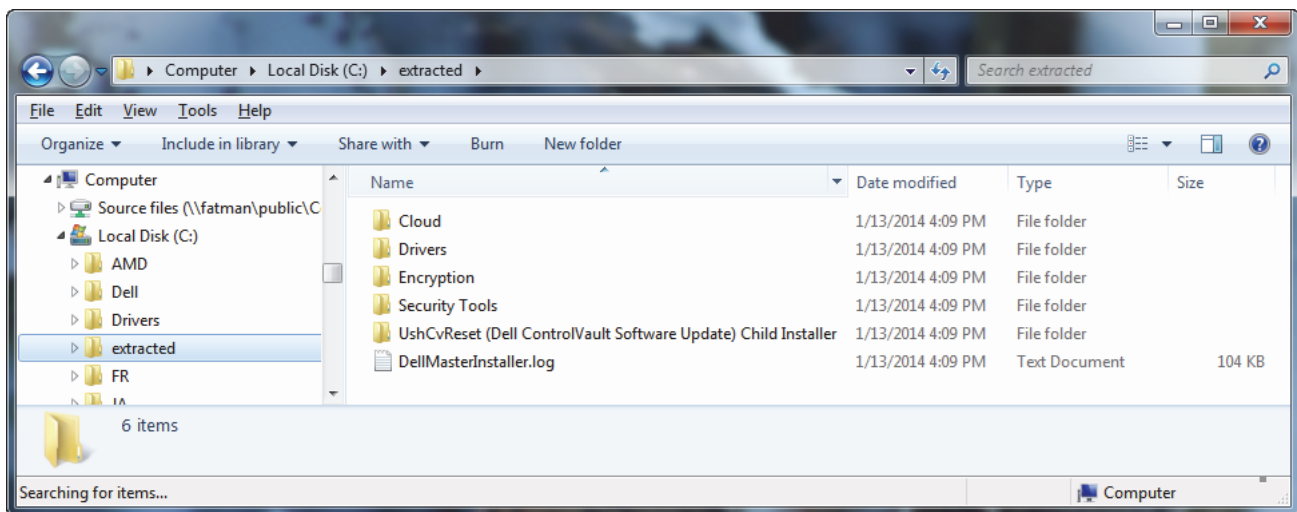
Extract the Child Installers from the Master Installer

To install each client individually, first extract the child executable files from the master installer.

- 1 From the Dell installation media, copy the master installer's **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 extracted child installers are located at C:\extracted\.



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 default location of log files is: C:\ProgramData\Dell\Dell Data Protection.
- If your computer has DDP|A installed now or has had it installed in the past, be sure to follow the steps in [Interoperability](#) before you continue.
- The computer restart has been suppressed in these examples but is eventually required for completion of the installation process.
- You will be securing access to this computer using advanced authentication credentials that are managed and enrolled using Dell Data Protection | Security Tools. DDP|ST is now the primary manager of your authentication credentials for Windows Sign-in, including Windows password, fingerprints, 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 your credentials, uninstall DDP|ST.

- If the computer targeted for encryption is equipped with a Hardware Crypto Accelerator or 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 Preboot Authentication has been activated (SED) or HCA policy has been set to True (HCA). If you must switch to a different authentication method, you must either:
 - Remove all the users from the PBA, and then re-enroll the users.
 - or
 - Deactivate the PBA (SED) or set the HCA policy to False (HCA), change the authentication method, and then re-activate the PBA (SED) or set the HCA policy to True (HCA).
- On computers equipped with a Hardware Crypto Accelerator or a self-encrypting drive, to use smart cards with Preboot Authentication, the following registry value must be set on the client computer:

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

"MSSmartcardSupport"=dword:1

0 or no key = Smart Card Support Off, 1 = Smart Card Support On

DDP|E Client and Advanced Authentication

See [Configure Credentials in the Security Console](#) and [Use the Authentication Applications](#) to learn how to use the features of Advanced Authentication.

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM. The ControlVault driver and firmware update is installed as part of this scenario.

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

SED Client - C:\extracted\Security Tools

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, no entry in the Control Panel Programs list, and is 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

NOTE: The SED client is required for Advanced Authentication in v8.x.

Then:

Advanced Authentication Client - C:\extracted\Security Tools\Authentication

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

```
DP_XXbit_setup.exe /s /v "/norestart /l*v DPinstall.log /qn"
```

Then:

Dell ControlVault - C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_XXX.exe /s /v "/norestart /l*v CVinstall.log /qn"
```


Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTERVERURL=https://server.organization.com:8081/xapi /norestart /l*v  
Shieldinstall.log /qn"
```

If your DDP Server is v7.7 or later:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ /norestart /l*v  
Shieldinstall.log /qn"
```

SED Client (including Advanced Authentication) and External Media Edition

See [Configure Credentials in the Security Console](#) and [Use the Authentication Applications](#) to learn how to use the features of Advanced Authentication.

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

SED Client - C:\extracted\Security Tools

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

Then:

Advanced Authentication Client - C:\extracted\Security Tools\Authentication

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

```
DP_XXbit_setup.exe /s /v"/norestart /l*v DPinstall.log /qn"
```

Then:

Dell ControlVault - C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_xXX.exe /s /v"/norestart /l*v CVinstall.log /qn"
```

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERVERURL=  
https://server.organization.com:8081/xapi MANAGEDDOMAIN=ORGANIZATION /norestart  
/l*v EMEinstall.log /qn"
```

If your DDP Server is v7.7 or later:

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

SED Client (including Advanced Authentication), External Media Edition, and Cloud Edition

See [Cloud Edition Activation and User Experience](#) to learn how to use Cloud Edition.

See [Configure Credentials in the Security Console](#) and [Use the Authentication Applications](#) to learn how to use the features of Advanced Authentication.

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

SED Client - C:\extracted\Security Tools

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

Then:

Advanced Authentication Client - C:\extracted\Security Tools\Authentication

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

```
DP_XXbit_setup.exe /s /v"/norestart /l*v DPinstall.log /qn"
```

Then:

Dell ControlVault - C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_XXX.exe /s /v"/norestart /l*v CVinstall.log /qn"
```

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERVERURL=  
https://server.organization.com:8081/xapi MANAGEDDOMAIN=ORGANIZATION /norestart  
/l*v EMEinstall.log /qn"
```

If your DDP Server is v7.7 or later:

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

Then:

Cloud Client - C:\extracted\Cloud

- The following example installs Cloud Edition (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /l*v Cloudinstall.log /qn"
```

DDP|E Client and Cloud Edition

See [Cloud Edition Activation and User Experience](#) to learn how to use Cloud Edition.

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi /norestart /l*v  
Shieldinstall.log /qn"
```

If your DDP Server is v7.7 or later:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8443/xapi/ /norestart /l*v  
Shieldinstall.log /qn"
```

Then:

Cloud Client - C:\extracted\Cloud

- The following example installs Cloud Edition (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /l*v Cloudinstall.log /qn"
```

BitLocker Manager and External Media Edition

BitLocker Manager Client - C:\extracted\Security Tools

- The following example installs BitLocker Manager (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 ADDLOCAL=  
DELL_Security_Tools,BITLOCKER FEATURE=BLM /l*v Bitlockerinstall.log /norestart  
/qn"
```

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERVERURL=  
https://server.organization.com:8081/xapi MANAGEDDOMAIN=ORGANIZATION /norestart  
/l*v EMEinstall.log /qn"
```

If your DDP Server is v7.7 or later:

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

BitLocker Manager, External Media Edition, and Cloud Edition

See [Cloud Edition Activation and User Experience](#) to learn how to use Cloud Edition.

BitLocker Manager Client - C:\extracted\Security Tools

- The following example installs BitLocker Manager (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 ADDLOCAL=  
DELL_Security_Tools,BITLOCKER FEATURE=BLM /l*v Bitlockerinstall.log /norestart  
/qn"
```

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTRIVERURL=  
https://server.organization.com:8081/xapi MANAGEDDOMAIN=ORGANIZATION /norestart  
/l*v EMEinstall.log /qn"
```

If your DDP Server is v7.7 or later:

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

Then:

Cloud Client - C:\extracted\Cloud

- The following example installs Cloud Edition (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart  
/l*v Cloudinstall.log /qn"
```

SED Client (including Advanced Authentication), DDP|E Client, and Cloud Edition

See [Cloud Edition Activation and User Experience](#) to learn how to use Cloud Edition.

See [Configure Credentials in the Security Console](#) and [Use the Authentication Applications](#) to learn how to use the features of Advanced Authentication.

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

SED Client - C:\extracted\Security Tools

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

Then:

Advanced Authentication Client - C:\extracted\Security Tools\Authentication

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

```
DP_XXbit_setup.exe /s /v"/norestart /l*v DPinstall.log /qn"
```

Then:

Dell ControlVault - C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_XXX.exe /s /v"/norestart /l*v CVinstall.log /qn"
```

Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi /norestart /l*v  
Shieldinstall.log /qn"
```

If your DDP Server is v7.7 or later:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8443/xapi/ /norestart /l*v  
Shieldinstall.log /qn"
```

Then:

Cloud Client - C:\extracted\Cloud

- The following example installs Cloud Edition (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart  
/l*v Cloudinstall.log /qn"
```

DDP|E Client and Advanced Authentication for Computers with HCA

NOTE: Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM. The ControlVault driver and firmware update is installed as part of the following scenario.

BIOS Configuration

- Complete the instructions in [DDP|HCA Pre-Installation BIOS Configuration](#).

Then:

Drivers - C:\extracted\Drivers

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, and suppresses the reboot.

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

Then:

SED Client - C:\extracted\Security Tools

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, no entry in the Control Panel Programs list, and is 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

NOTE: The SED client is required for Advanced Authentication in v8.x.

Then:

Advanced Authentication Client - C:\extracted\Security Tools\Authentication

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

```
DP_XXbit_setup.exe /s /v "/norestart /l*v DPinstall.log /qn"
```

Then:

Dell ControlVault - C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_xXX.exe /s /v "/norestart /l*v CVinstall.log /qn"
```


Then:

DDP|E Encryption Client - C:\extracted\Encryption

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi /norestart /l*v  
Shieldinstall.log /qn"
```

If your DDP Server is v7.7 or later:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8443/xapi/ /norestart /l*v  
Shieldinstall.log /qn"
```

Then:

- Configure user credentials and recovery questions in the Security Console.
See [Configure Credentials in the Security Console](#) and [Use the Authentication Applications](#) to learn how to use the features of Advanced Authentication.

Then:

- Enable hardware-based encryption by issuing a policy of Hardware Crypto Accelerator (HCA) = True. This step causes the PBA partition to be created. The computer will restart to complete the process.

Section I. Dell Data Protection Installer (Master Installer)

Dell Data Protection Master Installer

- The Dell Data Protection Master Installer is commonly known as the Master Installer, as it installs the Enterprise Edition suite of products.
- The master installer does not support upgrades from pre-v8.0 components. For upgrade needs, extract the appropriate child installer from the master installer. See [Extract the Child Installers from the Master Installer](#) for extraction instructions.
- You will be securing access to this computer using advanced authentication credentials that are managed and enrolled using Dell Data Protection | Security Tools. DDP|ST is now the primary manager of your authentication credentials for Windows Sign-in, including Windows password, fingerprints, 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 your credentials, uninstall DDP|ST.

- The default location of log files is: C:\ProgramData\Dell\Dell Data Protection
- If your computer has DDP|A installed now or has had it installed in the past, be sure to follow the steps in [Interoperability](#) before you continue.
- If the computer targeted for encryption is equipped with a Hardware Crypto Accelerator or a self-encrypting drive, ensure that the Active Directory option, *User Must Change Password at Next Logon*, is disabled. Preboot Authentication (PBA) does not support this Active Directory option.
- Dell recommends that you do not change the authentication method after Preboot Authentication has been activated (SED) or HCA policy has been set to True (HCA). If you must switch to a different authentication method, you must either:
 - Remove all the users from the PBA, and then re-enroll the users.
 - or
 - Deactivate the PBA (SED) or set the HCA policy to False (HCA), change the authentication method, and then re-activate the PBA (SED) or set the HCA policy to True (HCA).
- On computers equipped with a Hardware Crypto Accelerator or a self-encrypting drive, to use smart cards with Preboot Authentication, the following registry value must be set on the client computer:

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

"MSSmartcardSupport"=dword:1

0 or no key = Smart Card Support Off, 1 = Smart Card Support On

There are two methods available to install Dell Data Protection | Encryption using the master installer. Choose one of the following methods:

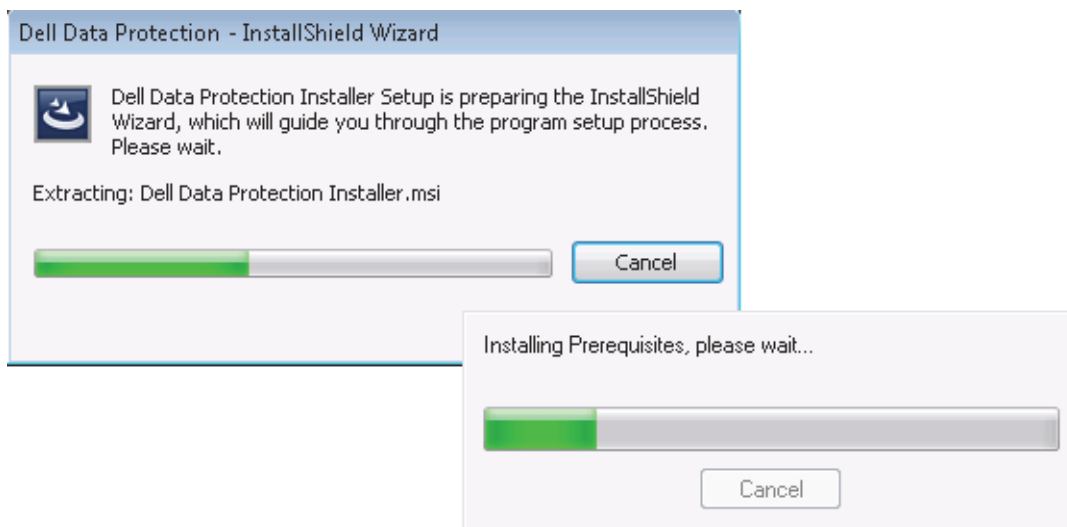
- [Install DDP|E Interactively](#)
- [Install DDP|E Using the Command Line](#)

Install DDP|E Interactively

- Use these instructions to install DDP|Enterprise Edition interactively. This method can be used to install the Enterprise Edition suite of products on one computer at a time. This installer includes the components you need for either software encryption or hardware encryption for computers equipped with Hardware Crypto Accelerator (HCA).

- 1 Locate **DDPSetup.exe** in the Dell installation media. Copy it to the local computer.
- 2 Double-click **DDPSetup.exe** to launch the installer.

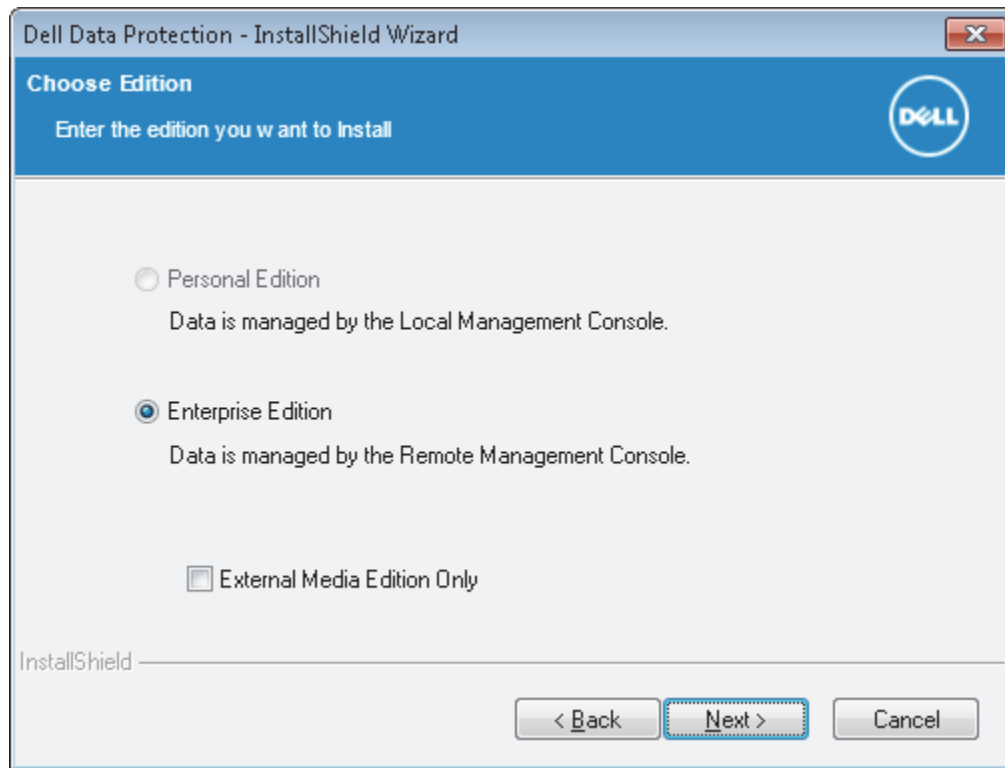
Dialogs display that alert you to the status of the installing the prerequisites. This may take several minutes.



- 3 Click **Next** when the Welcome screen displays.
- 4 Read the license agreement, agree to the terms, and click **Next**.
- 5 Select **Enterprise Edition** on the Choose Edition screen.

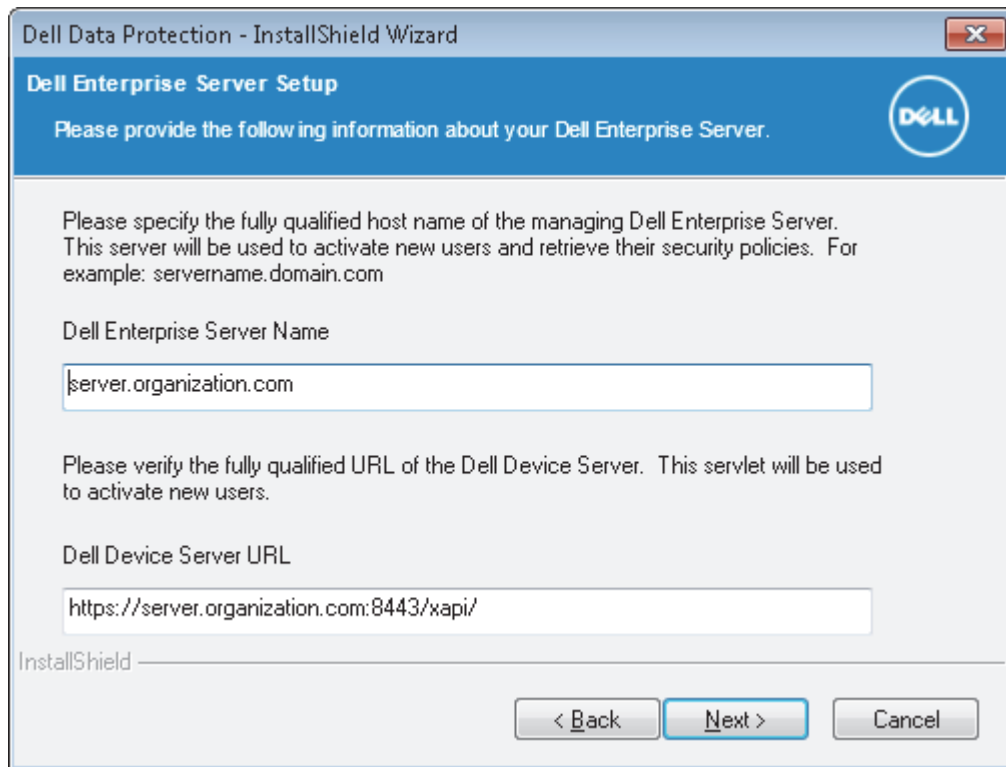
If you intend to install External Media Edition *only*, select the **External Media Edition only** check box.

6 Click **Next**.



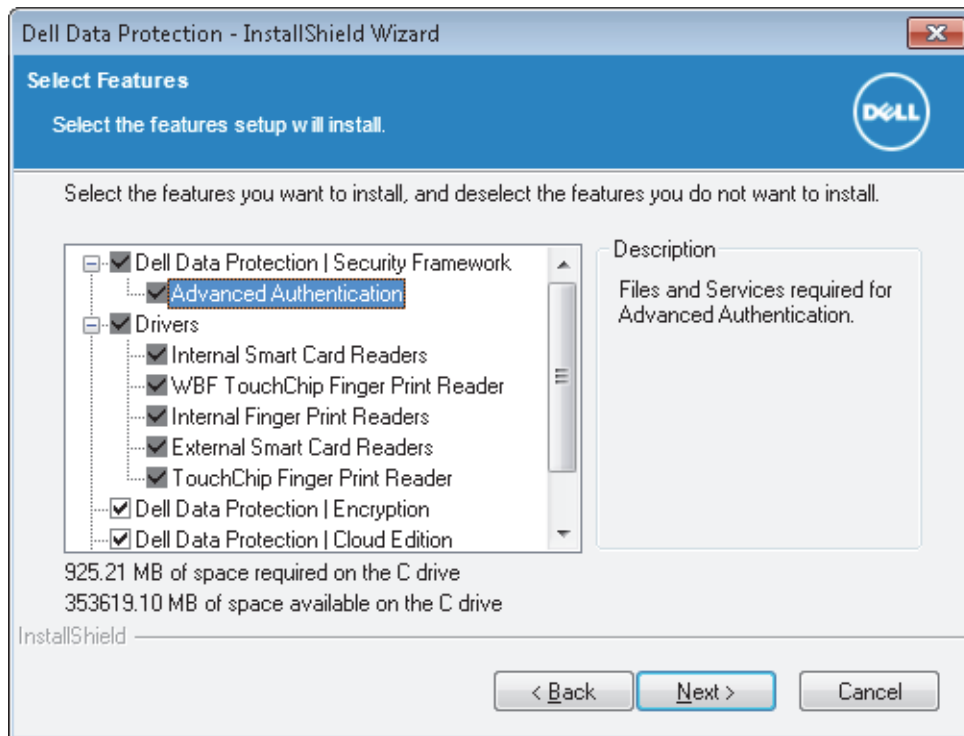
- 7 In the **Dell Enterprise Server Name** field, enter the fully qualified host name of the DDP Server that will manage the target user, such as server.organization.com.
- In the **Dell Device Server URL** field, enter the URL of the Device Server that the client will communicate with.
- If your DDP Server is pre-v7.7, the format is https://server.organization.com:8081/xapi.
- If your DDP Server is v7.7 or later, the format is https://server.organization.com:8443/xapi/ (including the trailing forward slash).

- 8 Click **Next**.

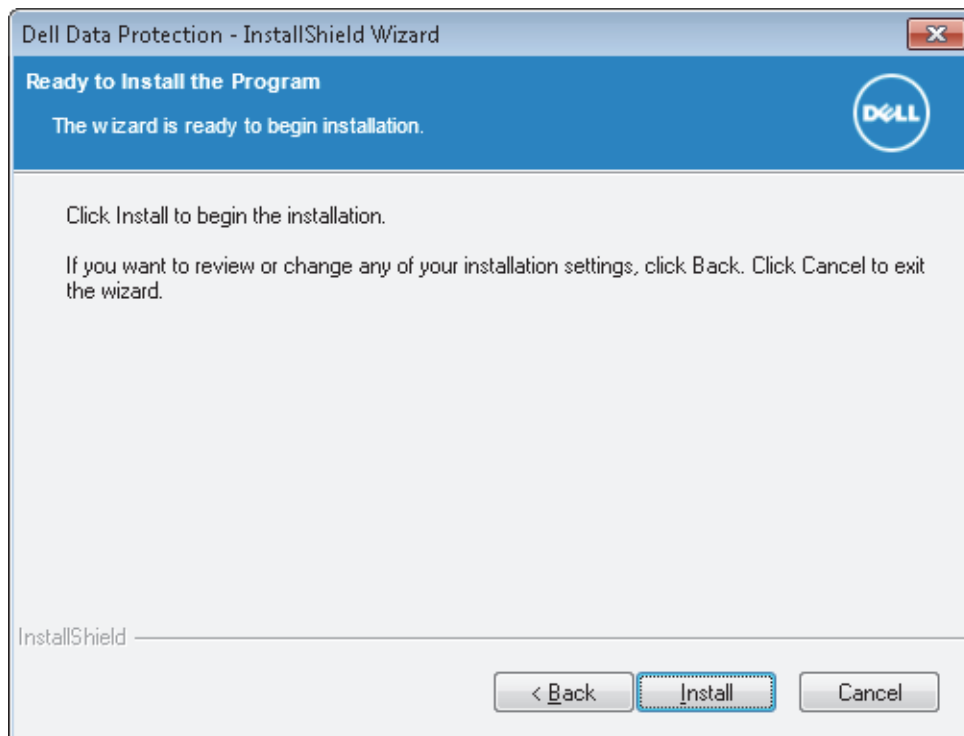


- 9 Click **Next** to install the products in the default location of C:\Program Files\Dell\Dell Data Protection\.
- 10 *Self-Encrypting Drive* management (your SED must be supported by Dell to be managed) and *Authentication* are installed by default and cannot be deselected. This is listed as Dell Data Protection | Security Framework in the installer. *Drivers* are installed by default and cannot be deselected. *Drivers* installs smart card, fingerprint reader, and other necessary drivers.
- Optionally, select the check box for *Dell Data Protection / Encryption* to install the encryption client for Windows computers.
- Optionally, select the check box for *Dell Data Protection / Cloud Edition* to install the Cloud client.
- Optionally, select the check box for *BitLocker Management* to install the BitLocker Manager client.

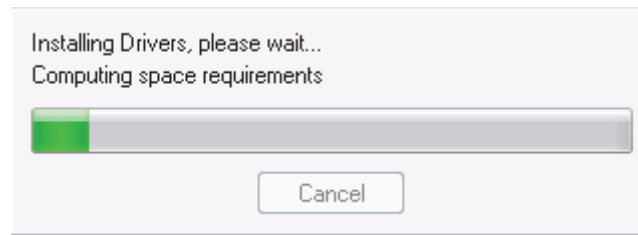
11 Click **Next**.



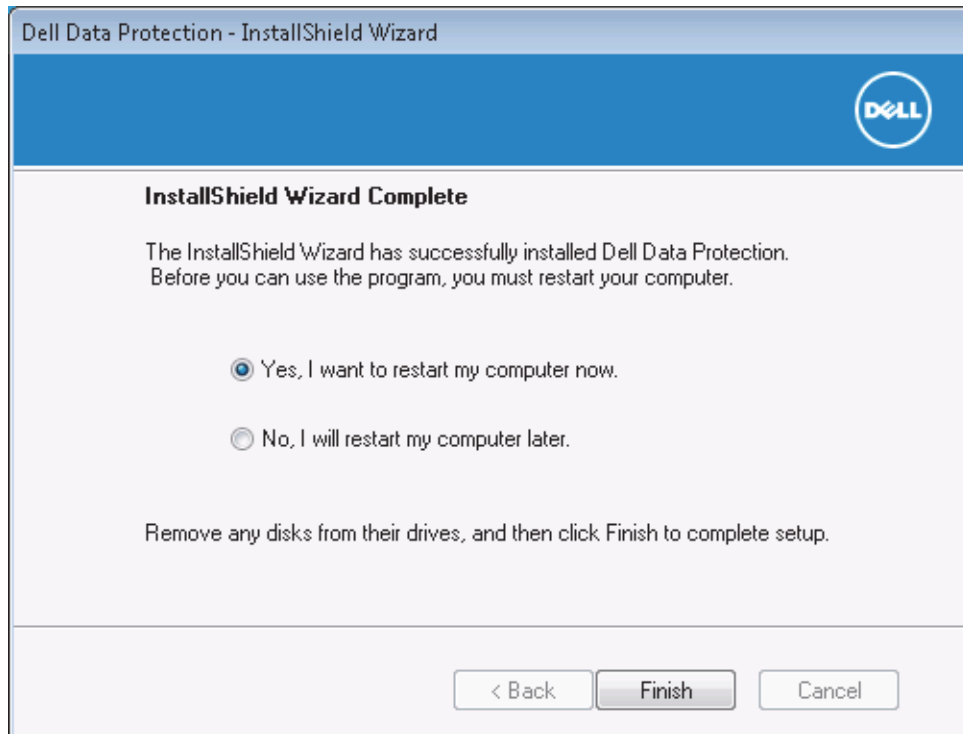
12 Click **Install** to begin the installation.



A status window displays. This may take several minutes.



- 13** Select **Yes, I want to restart my computer now** and click **Finish** when the InstallShield Wizard Complete dialog displays.



Installation of the selected products is complete.

Install DDP|E Using the Command Line

- Command line options are case-sensitive.

Switches

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

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

Parameters

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

Parameter	Description
SUPPRESSREBOOT	Silent mode. Suppresses the automatic reboot after the installation completes.
SERVER	UI mode. Specifies the URL of the Dell Enterprise Server (or Enterprise Server – VE).
InstallPath	Silent mode. Specifies the path for the installation.

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

Examples of Command Line Installation

- This example installs DDP|E using silent installation and installs it in the specified location of C:\Program Files\Dell\My_Directory:
`DDPSetup.exe -y -gm2 /S /z "\"InstallPath=C:\Program Files\Dell\My_Directory\""`
- This example installs DDP|E and configures it to use the specified Server:
`DDPSetup.exe -y -gm2 /S /z "\"SERVER=server.organization.com\""`
- This example suppresses rebooting at the end of an installation:
`DDPSetup.exe -y -gm2 /S /z "\"SUPPRESSREBOOT=1\""`

Uninstallation Process

To uninstall, each product must be uninstalled separately, in a specific order.

- 1** Extract the child installers, following the process in [Extract the Child Installers from the Master Installer](#).
- 2** When complete, go to C:\extracted\ to obtain each client installed on the computer.
- 3** Uninstall the clients in the following order:
 - DDP|E (DDPE_xxbit_setup.exe)
 - Security Framework (EMAgent_xxbit_setup.exe)
 - DDP|Authentication (DP_xxbit_setup.exe)
 - If Cloud Edition is installed, it can be uninstalled independently without uninstalling the clients listed above.
 - Cloud Edition (Cloud_xxbit_setup.exe)
- 4** When all clients are uninstalled, run the master installer's DDPSetup.exe to uninstall the master installer.

Section II. Drivers

Drivers Installation Tasks

- Drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor’s drivers.**

Drivers are also needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.
- If you have not extracted the individual installer yet, follow the procedure in [Extract the Child Installers from the Master Installer](#). The drivers can be installed by command line using any push technology available to your organization.

Install Drivers

Drivers - locate the installer at C:\extracted\Drivers

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

Command Line Installation

For a command line installation, 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.

Switches

The following table details the switches available for the installation.

Switch	Meaning
/v	Pass variables to the .msi inside the setup.exe
/s	Silent mode

Parameters

The following table details the parameters available for the installation.

NOTE: The /l*v parameter is not needed. A log is generated at %temp%\ DellDriverInstaller.log.

Parameters
SUPPRESSREBOOT=1
INSTALLPATH= <change the installation destination>
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Options

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

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

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

Example Command Line Installation

- The installation is performed using the **setup.exe** file located in the *C:\extracted\Drivers* folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

- The following example installs the drivers at the specified location, does not create an entry in the Control Panel Programs list, suppresses the reboot.

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


Section III. DDP|E Encryption Client

Encryption Client Installation Tasks

- You can install the Encryption client by itself by extracting the child installer out of the master installer. If you have not extracted the individual installer yet, follow the procedure in [Extract the Child Installers from the Master Installer](#). The Encryption client can be installed using the user interface or by command line using any push technology available to your organization.
- On computers equipped with a Hardware Crypto Accelerator, to use smart cards with Preboot Authentication, the following registry value must be set on the client computer:

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

```
"MSSmartcardSupport"=dword:1
```

0 or no key = Smart Card Support Off, 1 = Smart Card Support On

- Use these instructions to install software encryption or hardware encryption for computers equipped with an HCA card.

Best Practices

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.

- Back up any important data.
- To reduce encryption time, run the Windows Disk Cleanup Wizard to remove temporary files and any other unnecessary data.
- Turn off sleep mode to prevent an unattended computer from going to sleep. Encryption cannot occur on a sleeping computer.
- In environments where systems are installed with images, it is **strongly recommended** to install the Encryption client after image installation. If it is necessary to incorporate the Encryption client in an image, it should be done in an unencrypted state. Should you have questions or concerns, contact Dell Pro Support.
- When upgrading, Dell recommends doing so when no encryption sweep is running. Performing an upgrade during an encryption sweep may prevent the client from restarting normally after the installation finishes. If this occurs, a computer restart corrects the issue.

Install Encryption Client

DDP|E 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.

NOTE: Drivers are needed if installing the encryption client. Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.

Command Line Installation

For a command line installation, 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.

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= <ServerName>
		POLICYPROXYHOSTNAME= <RGKName>
		MANAGEDDOMAIN= <MyDomain>
		DEVICESTERVERURL= <ServerName>
		GKPORT= <NewGKPort>
		MACHINEID= <MachineName>
		RECOVERYID= <RecoveryID>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS= 1
		HIDESYSTRAYICON= 1
		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, to achieve your expected behavior.

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

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

Example Command Line Installation

- The installation is performed using the **DDPE_XXbit_setup.exe** file located in the *C:\extracted\Encryption* folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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"` will create install logs in a "C:\Logs" folder.

The Dell Device Server URL is case sensitive.

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

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi /l*v Shieldinstall.log  
/qn"
```

If your DDP Server is v7.7 or later:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8443/xapi/ /l*v  
Shieldinstall.log /qn"
```

- The following example installs the encryption client, Encrypt for Sharing, and CREDActivate, hides the DDP|E 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.

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi HIDESYSTRAYICON=1  
HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

If your DDP Server is v7.7 or later:

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

Install External Media Edition (EME)

- The following example installs **EME only** (silent installation, no progress bar, automatic restart, installed in the default location of C:\Program Files\Dell\Dell Data Protection).

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTRIVERURL=https://server.organization.com:8081/xapi EME=1 /qn"
```

If your DDP Server is v7.7 or later:

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

- The following example installs EME only (silent installation, no reboot, with logs at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection)

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERVERURL=
https://server.organization.com:8081/xapi MANAGEDDOMAIN=ORGANIZATION /norestart
/l*v EMEinstall.log /qn"
```

If your DDP Server is v7.7 or later:

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

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; on an XP, the path is C:\Documents and Settings\All Users\Application Data\Dell\Dell Data Protection\Encryption\CMGShield.log and locate the following entry:

```
[<date/timestamp> DeviceInfo: < >] Shield Information - SM=External Media Only, SB=DELL, UNF=FQUN, last sweep={0, 0}
```

Convert External Media Edition to Enterprise Edition

- Run a command line similar to the following:

If your DDP Server is pre-v7.7:

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERVERURL=https://server.organization.com:8081/xapi REINSTALL=ALL EME=0
REINSTALLMODE=vemus /qn"
```

If your DDP Server is v7.7 or later:

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

NOTE: A decrypt operation is not needed when converting External Media Edition to Enterprise Edition.

Create a Custom Transform File

The DDPE_XXbit_setup.exe file provides the ability to create custom transform files. Dell Pro Support is provided for issues relating to the use of the DDPE_XXbit_setup.exe file or the extraction of the .msi file. Creating transforms requires specialized knowledge of the tool used to create the transform and of the environment in which the transform will be deployed. Dell Pro Support cannot provide support for third-party tools. Once the transform file is created, issues related to troubleshooting or deployment should be handled by your in-house subject matter expert.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks. Do not run the extracted MSI. There is a high risk of installing components in the wrong order or missing an installation step. Run DDPE_XXbit_setup.exe for installation.

Follow the steps below to extract the necessary client files to create a custom transform file.

- 1 Enter the following command to create an administrative installation package.

```
DDPE_XXbit_setup.exe /a
```

- 2** In the Setup window, specify the network location where you want to store the extracted files, and click **Install**.
- 3** Consult the documentation of your specific transform tool to create the transform file to be used in the next step.
- 4** Use a command line similar to the following to pass the transform file to the DDPE_XXbit_setup.exe installer.

```
DDPE_XXbit_setup.exe /v"PROPERTY1=\"value with spaces\" PROPERTY2=
ValueWithoutSpaces INSTALLDIR=D:\Program Files\Destination TRANSFORMS=
NewTransform1.mst /qn"
```


Encryption Client Uninstallation and Decryption Tasks

When using [System Data Encryption \(SDE\)](#), [User](#), or [Common](#) encryption, file decryption optionally occurs at uninstallation if you choose to install the Encryption Removal Agent. This enables you to decide whether or not to decrypt files.

When using HCA encryption, all HCA-encrypted drives must be decrypted prior to uninstallation. The Encryption Removal Agent does not decrypt HCA encrypted drives. To decrypt HCA encrypted drives, publish the policy Hardware Crypto Accelerator=False, allow the decryption process to complete, and then initiate the uninstall process.

Before beginning the uninstall process, see [How to Create an Encryption Removal Agent Log File \(Optional\)](#). This log file is useful for troubleshooting an uninstall/decryption operation. If you do not intend to decrypt SDE, User, or Common encrypted files during the uninstall process, you do not need to create an Encryption Removal Agent log file.

Best Practices

- 1 Back up all data.
- 2 To reduce decryption time, run the Windows Disk Cleanup Wizard to remove temporary files and other unneeded data.
- 3 Disable UAC. UAC may prevent uninstallation of the Encryption client.
- 4 Plan to decrypt overnight, if possible.
- 5 Turn off sleep mode to prevent an unattended computer from going to sleep. Decryption cannot occur on a sleeping computer.
- 6 Ensure that you have the correct version of the DDPE_XXbit_setup.exe file. Use the same version to uninstall as was used to install.
- 7 Shut down all processes and applications to minimize decryption failures because of locked files.
- 8 Follow your existing process for decrypting data, such as issuing a policy update.
- 9 Before performing a restart, run WSScan to ensure that all data is decrypted. See [Use WSScan](#) for instructions.
- 10 Disable all network connectivity. Otherwise new policies may be acquired that would re-enable encryption.
- 11 Periodically [Check Encryption Removal Agent Status](#). If the Encryption Removal Agent Service exists, then data decryption is still in process.

Prerequisites

- When using the option **Encryption Removal Agent - Download Keys from Server**, you must first configure the Dell Key Server and DDP Enterprise Server. See [Configure Dell Key Server](#) for instructions. The Dell Key Server is not used with the DDP Enterprise Server - VE.
- When using the option **Encryption Removal Agent - Import Keys from a file**, you must 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)

- Optionally create an Encryption Removal Agent log file to aid in troubleshooting. See [How to Create an Encryption Removal Agent Log File \(Optional\)](#). If you do not intend to decrypt SDE, User, or Common encrypted files during the uninstall process, you do not need to create an Encryption Removal Agent log file.
- You must have a local or domain Admin user account to perform the uninstallation.
- Dell ControlVault is typically not uninstalled, as it is a driver for your fingerprint reader.

Uninstall Encryption Client

Before you begin, ensure the following items are complete:

- If the uninstallation target device is activated against a DDP Enterprise Server, ensure that a domain account is configured for the “Logon As” in the Dell Key Server service.
- If the uninstallation target device is activated against a DDP Enterprise Server, ensure that the DA_RUNAS user is in the Key Server list in the Remote Management Console.
- See [How to Create an Encryption Removal Agent Log File \(Optional\)](#) for instructions on how to create an Encryption Removal Agent log file.
- See [Check Encryption Removal Agent Status](#) for information on how to check decryption status following uninstallation.

NOTE: If performing a silent uninstall of a client that is activated against a **DDP Enterprise Server - VE** and using a password on the command line is a security concern, Dell recommends that the administrator:

1. Create a Forensic Administrator account in the VE 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.

Command Line Uninstallation

For a command line uninstallation, 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.

Switches

The following table details the switches available upon the uninstallation.

Switch	Meaning
/v	Pass variables to the .msi inside the DDPE_xxbit_setup.exe
/a	Administrative uninstallation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the uninstallation.

Parameter	Selection
CMG_DECRYPT - Property for selecting the type of Encryption Removal Agent installation	1 - Download keys from the DDP Server 0 - Do not install Encryption Removal Agent
CMGSILENTMODE - Property for silent uninstallation.	1 - Silent 0 - Not Silent
Required Properties	
DA_SERVER	FQHN for the DDP Enterprise Server hosting the negotiate session
DA_PORT*	Port on the DDP Enterprise Server for request (default is 8050)
SVCPN*	Username in UPN format that the Dell Key Server service is logged on as on the DDP Enterprise 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 DDP Enterprise Server
DA_RUNASPWD	Password for the runas user
FORENSIC_ADMIN *	The Forensic administrator account on the DDP Enterprise Server - VE. This account is used only when the Server is a DDP Enterprise Server - VE.
FORENSIC_ADMIN_PWD *	The password for the Forensic administrator account. This account is used only when the Server is a DDP Enterprise Server - VE.
Optional Properties	
SVCLOGONUN	Username in UPN format for Encryption Removal Agent service logon as parameter
SVCLOGONPWD	Password for logon as user

NOTE: * The Forensic administrator account is created in the VE Remote Management Console. Use the Forensic administrator's credentials only when the client to be uninstalled is activated against a DDP Enterprise Server - VE. When the Server is a non-VE Server, use the DA_PORT and SVCPN parameters.

Options

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

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

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

Example Command Line Uninstallation

- The uninstallation is performed using the `DDPE_XXbit_setup.exe` file located in the `C:\extracted\Encryption` folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

To specify a log location other than the default location where the executable is located, provide the complete path in the command. For example, `/I C:\Logs` will create install logs in a "C:\Logs" folder.

Dell does not recommend using verbose logging in a command line uninstallation, as the username/password is recorded in the log file. Should you decide to use verbose logging, ensure that the log file is deleted and the recycle bin is emptied.

The DA_Server URL is case-sensitive.

- The following example downloads the keys from the DDP Enterprise Server.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\"
SVC PN=\"administrator@organization.com\"
DA_RUNAS=\"ORGANIZATION\UserInKeyServerList\" DA_RUNASPWD=\"password\" /qn"
```

Allow the Encryption Removal Agent to run and check its status as needed (see [Check Encryption Removal Agent Status](#) for information).

- The following example uses a temporary Forensic Administrator account to uninstall DDP|EE when activated against DDP Enterprise Server - VE:

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\"
FORENSIC_ADMIN=\"temp superadmin\" FORENSIC_ADMIN_PWD=\"tempchangeit\" /qn /l
c:\ddpe_uninstall.log"
```

Uninstall External Media Edition

- Run a command line similar to the following:

```
DDPE_XXbit_setup.exe /s /x /v"/qn /l c:\ddpe_uninstall.log"
```

Allow the Encryption Removal Agent to run and check its status as needed (see [Check Encryption Removal Agent Status](#) for information).

NOTE: Windows and EME Shields update the DDP 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 DDP 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.

How to Create an Encryption Removal Agent Log File (Optional)

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 an Encryption Removal Agent log file.

Create the following Windows Registry entry on the computer targeted for decryption to create an Encryption Removal Agent log file.

- 1 Click **All Programs > Run** from the Windows Start menu.
- 2 Enter *regedit* in the Open: field.
- 3 Go to HKLM\Software\Credant\DecryptionAgent.
- 4 Right-click in the right pane and select **New > DWORD Value**.
- 5 Name the key **LogVerbosity**.
- 6 Double-click the key to open it.
- 7 Enter 0, 1, 2, 3, or 5 in the Value Data: field.
 - LogVerbosity 0: no logging
 - LogVerbosity 1: logs errors that prevent the Service from running
 - LogVerbosity 2: logs errors that prevent complete data decryption (recommended logging level)
 - LogVerbosity 3: logs information about all decrypting volumes and files
 - LogVerbosity 5: logs debugging information
- 8 Select **Hexadecimal** in the Base section.
- 9 Click **OK** to save and close the key.
- 10 Close the Registry Editor.

For Windows XP, the log file path is C:\Documents and Settings\All Users\Application Data\Dell\Dell Data Protection\Encryption.

For Windows 7, Windows 8, and Windows 8.1 the log file path is C:\ProgramData\Dell\Dell Data Protection\Encryption.

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.

Check Encryption Removal Agent Status

When the Encryption Removal Agent runs, its status displays in the description of the Windows Service panel (Start > Run... > services.msc > OK) as follows.

Waiting for Deactivation – DDP|E is still installed, is still configured, or both. Decryption does not start until DDP|E 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 [How to Create an Encryption Removal Agent Log File \(Optional\)](#) 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.

Periodically refresh the Service (highlight the Service > right-click > Refresh) to update its status.

Encryption Client Data Recovery

Situations such as operating system failure or hardware failure may cause encrypted data to become inaccessible. Data recovery allows you to regain access to encrypted data on computers encrypted by DDP|E software encryption or HCA encryption.

Prerequisites

- A recovery bundle is needed to recover data. The bundle is a recovery program that must be run with Administrative rights on the drive that it is recovering. In Windows XP, the user account under which the recovery program is run must at least be a member of the Administrator Group. In Windows 7, Windows 8, and Windows 8.1, the recovery program must be “Run as Administrator”.
- If the target computer is not bootable, data recovery must be performed on the computer booted into a pre-installed environment (or a slaved drive). Instructions to create pre-installed environments are located in the Dell installation media in “Windows Recovery Kit.” Several sets of instructions are included: for HCA, SED, and File/Folder Encryption (FFE). Once you have created your pre-installed environment and followed all instructions, return to this document.

Retrieve the Recovery Bundle

To perform data recovery, a recovery program containing the disk's encryption keys must first be retrieved from the Remote Management Console.

- 1 As a Dell Administrator, log in to the Remote Management Console.
- 2 In the left pane, click **Actions > Recover Endpoint**.
- 3 Select the appropriate Endpoint Type.
- 4 Enter the fully qualified Host Name of the computer, such as username.organization.com. You can find the Host Name on the Endpoint Detail page in the Endpoint Detail section. It is listed as the Unique ID.
- 5 Click **Download**.
- 6 When prompted, create a Recovery Password for this computer and click **Save**.
- 7 When prompted, save the file to a convenient and accessible location.

You may now use this recovery bundle to [Recover Data](#).

Recover Data

There are two methods to recover data:

- [Recover Data using Current Computer](#) - If the target computer is **still bootable**, data recovery can be accomplished **in-place**.
- [Recover Data using a Pre-Installed Environment \(or a Slaved Drive\)](#) - If the target computer is **not bootable**, data recovery must be accomplished on the computer booted into the pre-installed environment or a slaved drive. Instructions to create a pre-installed environment are located in the Dell installation media in the “Windows Recovery Kit” folder.

Recover Data using Current Computer

These instructions restore access to encrypted files by forcing DDP|E to re-acquire its keys from the server. Follow these instructions when the computer is bootable, but you are having problems accessing encrypted files.

- 1 Locate the recovery bundle downloaded from the Remote Management Console.
- 2 Copy the recovery bundle to the target computer (the computer to recover data).
- 3 Right-click the file and select **Run as Administrator** to launch the recovery utility.

The recovery bundle that you downloaded from the Server is in a compressed, self-extracting format. The compressed recovery file extracts to the same location as the compressed file, and executes. A dialog displays prompting you to select the scenario that best describes your problem:

- My system fails to boot and displays a message asking me to perform SDE recovery.
- **My system does not allow me to access encrypted data, edit policies, or is being reinstalled.**
- I want to decrypt my HCA encrypted drive.
- I want to restore access to my HCA encrypted drive.

- 4 Select the **second** option, **My system does not allow me to access encrypted data, edit policies, or is being reinstalled**, and click **Next**.
- 5 Click **Next** at the Backup\Recovery Information screen.
- 6 Select the disk to recover and click **Next**.
- 7 Enter the recovery password associated with this file. This is the Recovery Password defined when the recovery bundle was retrieved from the Remote Management Console. A dialog displays notifying you of the disk that is being recovered.
- 8 Click **Recover**.
A dialog displays notifying you that recovery was completed successfully.
- 9 Click **Finish**.
- 10 When recovery is finished, close the console.
The self-extracting file will delete the extracted files.

Recover Data using a Pre-Installed Environment (or a Slaved Drive)

This procedure covers these three scenarios:

Type of Recovery	Description
SDE recovery	My system fails to boot and displays a message asking me to perform SDE recovery.
HCA decryption	I want to decrypt my HCA encrypted drive.
HCA recovery	I want to restore access to my HCA encrypted drive.

Prerequisites

Ensure that the following prerequisites are met before beginning the recovery process.

- Ensure that you have physical access to the drive to be recovered.
- Ensure that you have access to the Dell installation media. The files in the “Windows Recovery Kit” folder contain the files needed for this process.
- Be prepared to create a WinPE image. All instructions and special drivers that are needed to create a WinPE image and recover the computer are included in the “Windows Recovery Kit” folder.

Prepare the Environment (or Slaved Drive)

SDE Environment Prerequisite

The computer must be booted into the appropriate recovery image or a slaved drive.

HCA Decryption Environment Prerequisites

The computer must be booted into any Windows-based alternate operating system environment on the computer to recover, with the hard drive you are trying to recover attached. This can be accomplished by booting to the appropriate recovery image or by booting from another drive or helper partition that has another version of Windows installed (but not HCA encrypted). This can be done on any computer running a compatible operating system as long as the drive to be decrypted is attached and accessible.

HCA Recovery Environment Prerequisites

- An HCA encrypted drive must be attached.
- The computer must be booted to the appropriate recovery image: the Win PE HCA recovery environment that has HCA drivers and other required components. HCA recovery outside of this environment will not work.
- The booted environment must have network connectivity to the Dell Device Server.

Establish HCA Card Ownership

When the HCA card is already owned, the recovery process can still be successful. The recovery process will try to use the existing backup of the HCA Critical Data and password to establish and maintain the HCA ownership of an already-owned HCA card. If this attempt fails, then the recovery operation fails. When it fails, reboot and clear the HCA card's ownership.

When Installing an HCA Card from Another Computer, you must clear HCA ownership on the swapped HCA card and establish new ownership. Since the HCA card from the other computer was previously owned, recovery cannot succeed until the HCA owner is cleared in the BIOS.

See [DDP|HCA Pre-Installation BIOS Configuration](#) for instructions on clearing HCA ownership.

CAUTION

Drives encrypted by HCA will become inaccessible if ownership is cleared. The user will need to perform an HCA recovery or an HCA decrypt in order to restore access.

Set up a System Password (Legacy HCA only)

Recovery of a computer equipped with legacy HCA requires a system password to be validated prior to recovery. If no system password is set, you will be prompted to go into the BIOS and set up a password. See [DDP|HCA Pre-Installation BIOS Configuration](#) for instructions on setting up the system password.

Extract the Recovery File (optional)

Running the recovery program at the command line with parameters gives you a little more control over the process and outcome. Because the compressed recovery bundle that you downloaded from the Server does not respond to command line switches, the LSARecovery file must be extracted from the bundle. Follow these steps to obtain the LSARecovery file:

- 1 Locate the downloaded recovery file.
- 2 Right-click it and select **Run as administrator**. The recovery program runs and displays a dialog box.
- 3 In Windows Explorer, check the directory where the recovery file is located to find a file called LSARecovery_ *machinename_domain.com.exe*.
- 4 Copy the LSARecovery file to another location to save it.

- 5 **Cancel** the recovery dialog box.

Now you can use the LSARecovery file to run the recovery from a command line.

Recover the Data

- 1 Locate the recovery file downloaded from the Remote Management Console.
- 2 Right-click the recovery file and select **Run as administrator**.

Or (if you extracted the recovery file in the previous procedure)

Run the LSARecovery executable from a command prompt:

```
LSARecovery.exe -server [https://my.Dell Enterprise Server.com] *
```

Or

```
LSARecovery.exe -server [IP address of the Dell Enterprise Server]
```

NOTE: * The Dell Enterprise Server can either be specified in the command line as the URL or as the IP address, or by creating the servlet URL registry entry that the Shield uses.

If the recovery is an SDE or HCA decryption recovery, no escrow takes place and the only parameter needed in the command line is the Dell Device Server's URL.

If the recovery is occurring on a computer equipped with an HCA card, as the recovery runs, it escrows the new HCA Critical Data back to the Dell Device Server.

NOTE: If the HCA card is already owned, no escrow step is performed (unless recovery generates new data).

A dialog displays prompting you to select the scenario that best describes your problem.

- 3 Select the appropriate option:

For SDE Recovery, select **My system fails to boot and displays a message asking me to perform SDE recovery** and click **Next**.

For HCA Decryption, select **I want to decrypt my HCA encrypted drive** and click **Next**.

For HCA Recovery, select **I want to restore access to my HCA encrypted drive** and click **Next**.

- 4 Click **Next** when the Backup\Recovery Information screen displays.
- 5 Select the disk to decrypt or recover and click **Next**.
- 6 Enter the recovery password. This is the recovery password defined when the recovery bundle was retrieved from the Remote Management Console. A dialog displays notifying you of the disk that is being recovered.
- 7 Click **Recover**.
A dialog displays notifying you that recovery was completed successfully.
- 8 Click **Finish**.
- 9 Restart the computer when prompted and log in to Windows.

HCA NOTES: At the end of an HCA decryption process, if an HCA card is detected, the HCA recovery process changes the boot order of the disk, bypassing the PBA so that the system boots directly to Windows.

If the HCA card was unowned prior to recovery, then the recovery process takes ownership of the HCA, and escrows the HCA Critical Data to the server.

When the computer restarts, it downloads the updated HCA Critical Data to complete the recovery. It will attempt to download the HCA Critical Data on every login until it succeeds in obtaining the new data. Once this has happened, the drive's device icon should be green again in the console.

After the escrow takes place, the local console requests the updated data from the server the next time anyone logs in.

If recovery fails, refer to [Troubleshooting HCA Recovery](#) for assistance.

Troubleshooting HCA Recovery

Check the Recovery Log File

The recovery log file is located in C:\ProgramData\Dell\Dell Data Protection\Encryption\LSARecovery.log

If you are booted into WinPE, the recovery log file path defaults to drive X:\ProgramData\Dell\Dell Data Protection\Encryption\LSARecovery.log. Drive X is in memory and will disappear after you restart the computer. If you want have the log file to examine later, save the log file to a permanent location.

When Escrow Cannot Be Completed during the WinPE Recovery (HCA)

If escrow cannot be completed during the WinPE recovery, the recovery saves a new copy of the backup file to the recovery directory specified after clicking Recover.

Use the extracted LSARecovery file and the following command line options to escrow the data to the server from any Windows computer that has network connectivity to the server.

```
LSARecovery.exe -escrowAll -server https://my.server.com:8443/xapi
```

Reset TPM Security (HCA)

If there is a problem with the TPM, recovery can fail. When this occurs, you need to reset TPM ownership.

TPM security must also be reset when a computer's motherboard is replaced. See [DDP|HCA Pre-Installation BIOS Configuration](#) for instructions.

Recover User Access to a Computer Equipped with HCA

Self-Recovery

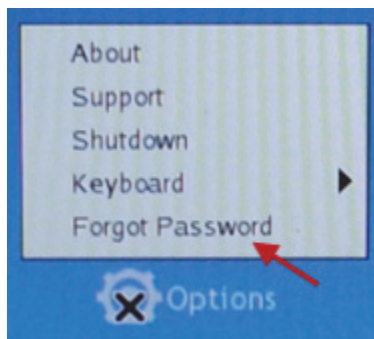
This workflow enables end users to log on with provisioned recovery questions.

Once the end user's recovery questions have been configured in the Security Console, then the option to use the recovery questions for self-recovery is available. See [Configure Credentials in the Security Console](#) for instructions on configuring recovery questions.

- 1 At the PBA login screen, the end user enters their user name and clicks the gear in lower left.



- 2 The end user selects **Forgot Password**.



- 3 The end user enters the correct answers to the recovery questions and clicks **Finish**.



The screenshot shows a blue background with the Dell logo at the top center. Below the logo, the text "Dell Data Protection - Security Tools" is displayed. Underneath, the heading "Recovery Questions" is centered. There are three text input fields, each with a question above it: "What is your mother's middle name?" with the answer "dell", "Who was your first employer?" with the answer "1234", and "Who was your first teacher?" with the answer "5678". A "Finish" button is located below the input fields. At the bottom, the text "Enter authentication answers." is displayed. A small "Tools" link is visible in the bottom left corner.

Recover Access using Challenge/Response Codes

- 1 As a Dell Administrator, open the Remote Management Console.
- 2 In the left pane, click **Actions > Recover Data**.
- 3 Select the **SED** tab on the top menu.
- 4 In the *Recover SED User Access* area, enter the Host Name of the computer to recover.
Enter the *Host Name* as a fully qualified host name. You can find the *Host Name* on the Endpoint Detail page in the Endpoint Detail section. It is listed as the Unique ID.
- 5 Click **Search**.
- 6 When the host is found, select the user name from the list.
- 7 Enter the challenge code obtained from the endpoint, and click **Generate Response**.
- 8 Instruct the user to enter the response code on his computer.

Assisted Recovery

- Assisted recovery will be needed if you need to bypass the PBA login for any reason.

Prerequisites

When contacting Dell Support for recovery assistance, ensure that the following prerequisites are met:

- Ensure that you have physical access to the drive to be recovered.
- Ensure that you have the recovery keys. Your recovery keys are saved on a network drive or on removable media.

- 1 Log on to www.dell.com/support > [Endpoint Security Solutions](#) and enter the Dell service tag number which is located on the bottom of the computer. After entering the service tag number, follow the instructions to contact Dell Support for recovery assistance and to obtain the necessary files.

Configure Dell Key Server

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

Dell 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 Dell Key Server then checks with the Dell 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.

NOTE: If Kerberos Authentication/Authorization is to be used, then the server that contains the Dell Key Server component will need to be part of the affected domain.

NOTE: The DDP Enterprise Server - VE does not use the Dell Key Server, which affects how the Encryption client is uninstalled. Uninstallation uses standard forensic key retrieval through the Dell Security Server instead of the Key Server's Kerberos method. For available parameters, see [Parameters](#).

Windows Service Instructions

- 1 Navigate to the Windows Service panel (Start > Run... > services.msc > OK).
- 2 Right-click Dell Key Server and select **Properties**.
- 3 Go to the Log On tab and select the **This account:** option button.
- 4 In the This account: field, add the desired domain user. This domain user must have at least local Admin 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).
- 5 Click **OK**. Restart the Service (leave the Windows Service panel open for further operation).
- 6 Navigate to <Key Server install dir> log.txt to verify that the Service started properly.

Key Server Config File Instructions

- 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 DDP Enterprise Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the DDP Enterprise 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 DDP Enterprise 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 DDP Enterprise 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 Dell Key Server will listen to. Default is 8050.]
    <add key="maxConnections" value="2000" /> [number of active socket connections the Dell Key Server will allow]
    <add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Dell Device Server URL (the format is 8081/xapi for a pre-v7.7 DDP Enterprise 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 Dell Device 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 DDP Enterprise Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the DDP Enterprise 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 DDP Enterprise 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 Dell Key Server needs to download authorized users from the Dell Device 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 Dell Device Server. If the superadmin password has been changed, it must be changed here.]
  </appSettings>
</configuration>
```

Windows Service Instructions

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

Remote Management Console Instructions

- 1 If needed, log on to the Remote Management Console.
- 2 Click **Domains** and click the **Detail** icon.
- 3 Click **Key Server**.
- 4 In the Key Server account list, add the user that will be performing the Admin activities. The format is Domain\username. Click **Add Account**.
- 5 Click **Users** in the left menu. In the search box, search for the username added in Step 4. Click **Search**.
- 6 Once the correct user is located, click the **Detail** icon.
- 7 Select *Admin*. Click **Update**.

The components are now configured for Kerberos Authentication/Authorization.

Use WSScan

When uninstalling the Encryption client, follow your existing process for decrypting data, such as issuing a policy update. After decrypting data, but before performing a restart in preparation for uninstall, run WSScan to ensure that all data is decrypted.

Administrator privileges are required to run this utility.

- 1 From the Dell installation media, copy WSScan.exe to the Windows device to scan.
- 2 Launch a command line at the location above.
- 3 At the command prompt, enter **wsscan.exe**.
- 4 Click **Advanced >>**.
- 5 From the drop-down box, select the type of drive to scan: *All Drives*, *Fixed Drives*, *Removable Drives*, or *CDROMs/DVDROMs*.

or

To only scan a particular folder, go to Scan Settings and enter the folder path in the *Search Path* field. If this field is used, the selection in the drop-down box is ignored.

- 6 If you do not want to write WSScan output to a file, clear the *Output to File* check box.
- 7 If desired, change the default path and filename in *Path*.
- 8 If you do not want to overwrite any existing WSScan output files, select *Add to Existing File*.
- 9 Choose your output format as follows:
 - 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.
- 10 Click **Search**. To stop your search, click Stop Searching. To clear displayed messages, click Clear.

WSScan Output

WSScan information about encrypted files contains the following information.

Example Output:

[2010-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: “c:\temp\Dell - test.log” is still AES256 encrypted

Output	Meaning
Date/time stamp	The date and time the file was scanned.
Encryption type	The type of encryption used to encrypt the file. SysData: SDE Encryption Key. User: User Encryption Key. Common: Common Encryption Key. WSScan does not report files encrypted using Encrypt for Sharing.
DCID	The Device ID. As shown in the example above, “7vdlxrsb” If you are scanning a mapped network drive, the scanning report does not return a DCID.
UCID	The User ID. As shown in the example above, “_SDENCR_” The UCID is shared by all the users of that computer.
File	The path of the encrypted file. As shown in the example above, “c:\temp\Dell - test.log”
Algorithm	The encryption algorithm being used to encrypt the file. As shown in the example above, “is still AES256 encrypted” RIJNDAEL 128 RIJNDAEL 256 AES 128 AES 256 3DES

Section IV. SED Management and Advanced Authentication

SED Management and Advanced Authentication Installation Tasks

- You can install the SED management client and Advanced Authentication clients by themselves by extracting the child installers out of the master installer. If you have not extracted the individual installers yet, follow the procedure in [Extract the Child Installers from the Master Installer](#). The SED management client and Advanced Authentication client can be installed using the user interfaces or by command line using any push technology available to your organization.

Before You Begin

- Ensure that the Active Directory option, User Must Change Password at Next Logon, is disabled. Preboot Authentication does not support this Active Directory option.
- A self-encrypting drive must be configured as the boot drive (drive 0) for Preboot Authentication to function properly.
- To use smart cards with Preboot Authentication, the following registry value must be set on the client computer:

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

"MSSmartcardSupport"=dword:1

0 or no key = Smart Card Support Off, 1 = Smart Card Support On

Best Practices

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.

Install SED Management and Advanced Authentication

NOTE: The SED client is required for Advanced Authentication in v8.x.

SED Client - locate the installer at C:\extracted\Security Tools

Advanced Authentication Client - locate the installer at C:\extracted\Security Tools\Authentication

Dell ControlVault Client - locate the installer at C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer

- Use **EMAgent_XXbit_setup.exe** to install SED management using a scripted installation, using batch files, or any other push technology available to your organization.
- Use **DP_XXbit_setup.exe** to install Advanced Authentication using a scripted installation, using batch files, or any other push technology available to your organization.
- Use **Dell_CV_SW_Update_xXX.exe** to install Dell ControlVault software updates used by Security Tools using a scripted installation, using batch files, or any other push technology available to your organization.

Command Line Installation

For a command line installation, 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.

Switches

The following table details the switches available for the installation.

Switch	Meaning
/v	Pass variables to the .msi inside the exe files(required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the installation.

Log File	Parameters
/!*v [fullpath][filename].log	CM_EDITION=1 <remote management>
	INSTALLDIR= <change the installation destination>
	SERVERHOST= <coreserver.organization.com>
	SERVERPORT=8888
	SECURITYSERVERHOST= <securityserver.organization.com>
	SECURITYSERVERPORT=8443
	ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Options

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

Options	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

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

Example Command Line Installation

- Special drivers are needed for Advanced Authentication if installing on Dell hardware. These are the drivers for the various smart cards and fingerprint readers for which Dell supplies drivers. **Installing these drivers should be omitted if using Advanced Authentication on non-Dell hardware, as they may interfere with other vendor's drivers.**
- Additional drivers and software stack are required for supporting Hardware Crypto Accelerator (HCA). This includes the HCA driver and the Trusted Software Stack (TSS) for TPM.
- The installation is performed using the **EMAgent_XXbit_setup.exe**, **DP_XXbit_setup.exe**, and **Dell_CV_SW_Update_xXX.exe** files located in the *C:\extracted\Security Tools*, *C:\extracted\Security Tools\Authentication*, and *C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer* folders.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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"` will create install logs in a "C:\Logs" folder.

- The following example installs remotely managed SED (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /l*v SEDinstall.log /norestart /qn"
```

Then:

- The following example installs Dell ControlVault software updates used by Security Tools (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection). If the target computer is not equipped with Dell ControlVault, installing this software is not harmful and will have no effect.

```
Dell_CV_SW_Update_xXX.exe /s /v"/norestart /l*v CVinstall.log /qn"
```

Then:

- The following example installs Advanced Authentication (silent installation, no reboot, log file at the specified location)

```
DP_XXbit_setup.exe /s /v"/norestart /l*v DPinstall.log /qn"
```

Once policies are applied at the endpoint and are ready to be enforced, the end user will be notified by the client that a computer shutdown and restart is required. End users will log in to the computer through the PBA using their Windows password. The drive is now managed by the DDP Server.

IMPORTANT:

Dell recommends that you do not change the authentication method after Preboot Authentication has been activated (SED) or HCA policy has been set to True (HCA). If you must switch to a different authentication method, you must either:

Remove all the users from the PBA, and then re-enroll the users.

or

Deactivate the PBA (SED) or set the HCA policy to False (HCA), change the authentication method, and then re-activate the PBA (SED) or set the HCA policy to True (HCA).

SED and Advanced Authentication Deactivation and Uninstallation Tasks

These instructions detail the process of:

- Deactivating the PBA, which removes all PBA data from the computer and unlocks the SED key.
- Uninstalling the SED client software.
- Uninstalling the Advanced Authentication client software.

Prerequisites

- You must have an Administrator account to perform the uninstallation.
- Network connection to the DDP Server is required for PBA deactivation.
- The PBA **must** be [deactivated](#) on the computer before uninstallation.
- Use the same EMAgent_XXbit_setup.exe and DP_XXbit_setup.exe files to uninstall that were used to install.

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 (wildcarding is supported). You may leave the field blank to display all computers. Click **Search**.
If you do not know the Hostname, scroll through the list of available computers 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 From the Policy Category drop-down menu select **Self-Encrypting Drives**.
- 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 DDP Server to the computer targeted for deactivation.
After the PBA is deactivated, you may uninstall the clients.

Uninstall SED Client

- The uninstallation is performed using the **EMAgent_XXbit_setup.exe**, **DP_XXbit_setup.exe**, and **Dell_CV_SW_Update_xXX.exe** files located in the *C:\extracted\Security Tools*, *C:\extracted\Security Tools\Authentication*, and *C:\extracted\UshCvReset (Dell ControlVault Software Update) Child Installer* folders.

Command Line Uninstallation

For a command line uninstallation, 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.

Switches

The following table details the switches available for the uninstallation.

Switch	Meaning
/v	Pass variables to the .msi inside the .exe files (required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the uninstallation.

Log File	Parameters
/l [fullpath][filename].log	CM_EDITION=1 <remote management>
	INSTALLDIR= <change the installation destination>
	SERVERHOST= <coreserver.organization.com>
	SERVERPORT=8888
	SECURITYSERVERHOST= <securityserver.organization.com>
	SECURITYSERVERPORT=8443
	ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Options

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

Options	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

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

Example Command Line Uninstallation

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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 C:\Logs` will create install logs in a `C:\Logs` folder.

```
EMAgent_XXbit_setup.exe /x /s /v"/l Uninstall.log /qn"
```

Shut down and restart the computer.

Then:

```
DP_XXbit_setup.exe /x /s /v"/l DPuninstall.log /qn"
```

Then:

```
Dell_CV_SW_Update_xXX.exe /x /s /v"/l CVuninstall.log /qn"
```

Reboot the computer.

The SED client and Advanced Authentication clients are uninstalled.

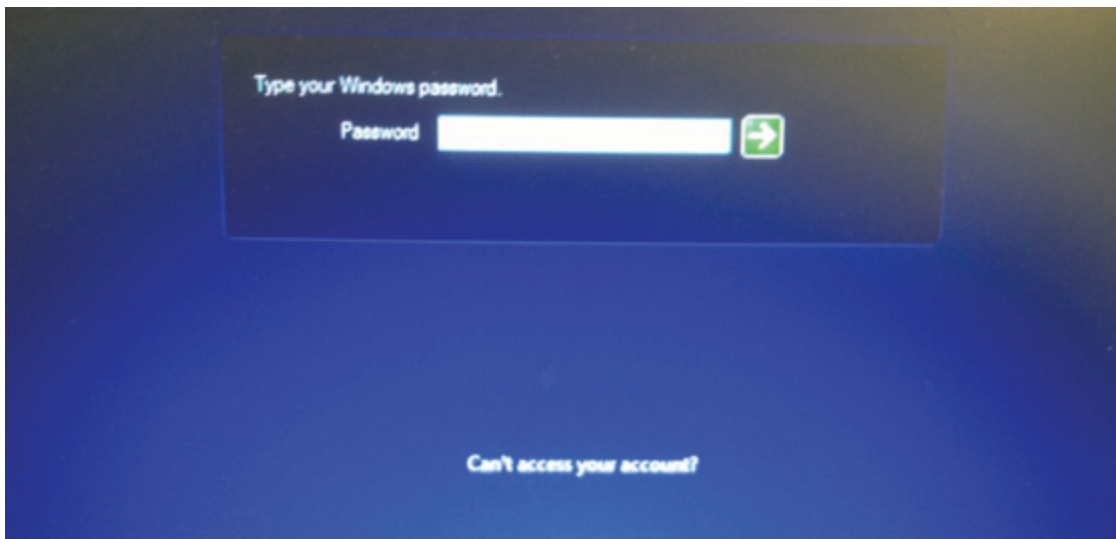
SED and OS Recovery

Self-Recovery, OS Logon

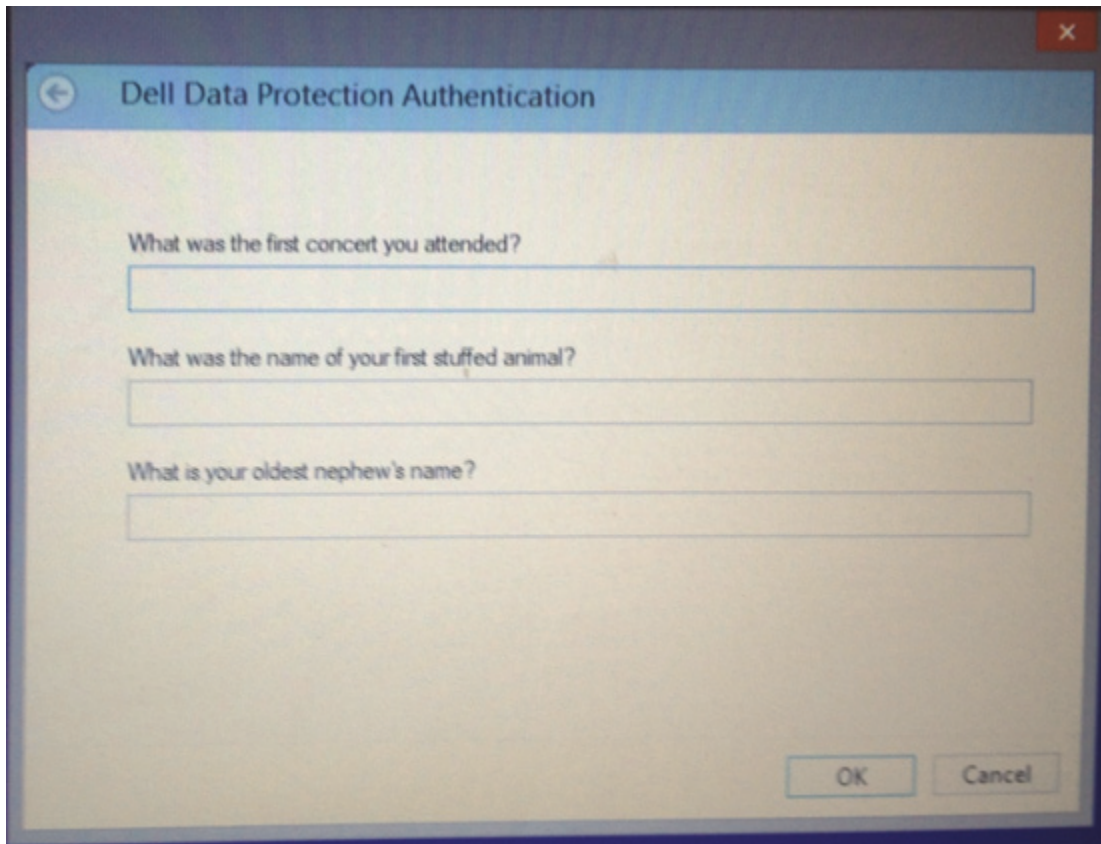
This workflow enables an end user to log on with provisioned recovery questions.

Once the end user's recovery questions have been set up, and if the *Allow recovery questions for Windows logon* setting is allowed by policy, then the option to use the recovery questions for Windows logon is available from the Windows Start screen.

- 1 The end user clicks **Can't access your account?** to use the Recovery Questions.

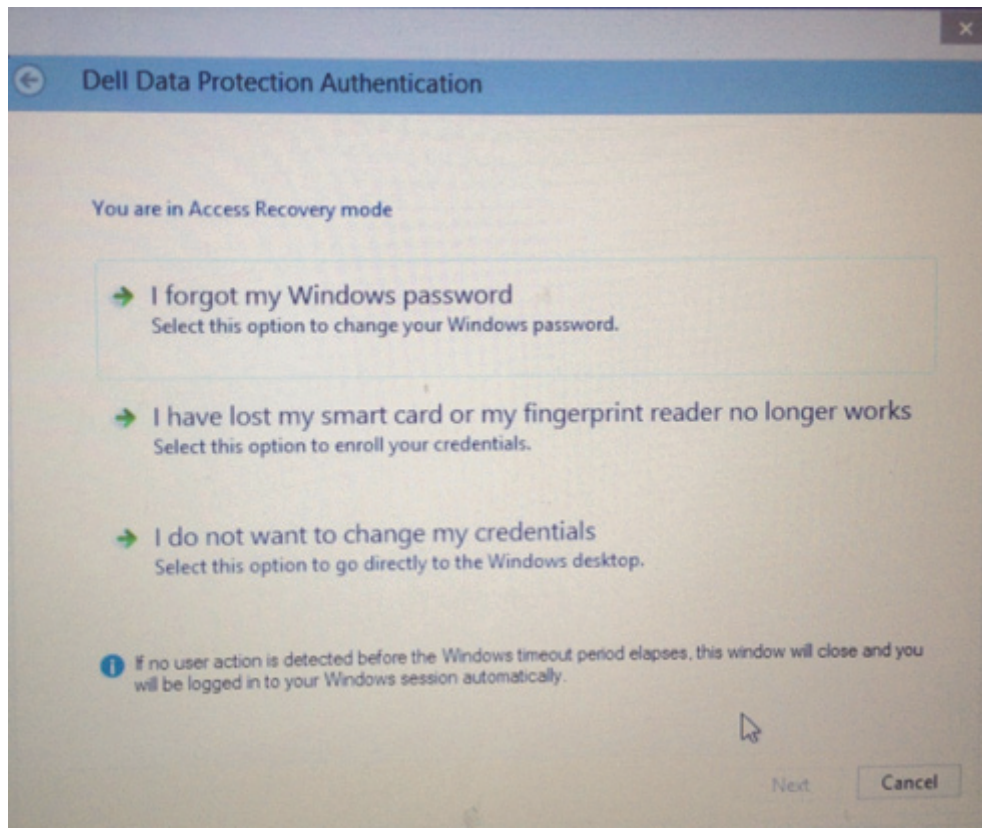


- 2 Clicking the link displays the questions selected by the end user during their initial setup in the Security Console. The end user enters the answers and clicks **OK**.

A screenshot of a Windows-style dialog box titled "Dell Data Protection Authentication". The dialog box has a blue header bar with a back arrow icon on the left and a close button (X) on the right. The main area is white and contains three text input fields, each preceded by a question: "What was the first concert you attended?", "What was the name of your first stuffed animal?", and "What is your oldest nephew's name?". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

- 3 Upon successful entry of the answers to the questions, the end user is in *Access Recovery* mode. The following options are available to end users:
- Change their Windows password
 - Re-enroll their credentials
 - Go directly into Windows

The end user selects one option and clicks **Next**.



NOTE: If none of the options are selected within the Windows timeout period, the end user is automatically logged into Windows without further action.

Self-Recovery, PBA

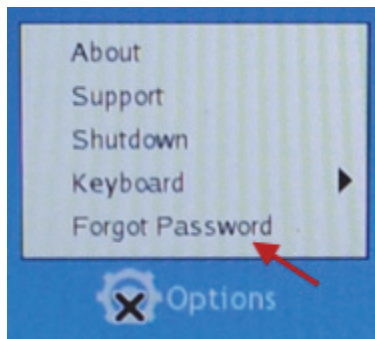
This workflow enables end users to log on with provisioned recovery questions.

Once the end user's recovery questions have been set up, then the option to use the recovery questions for PBA self-recovery is available.

- 1 At the PBA login screen, the end user enters their user name and clicks the gear in lower left.



- 2 The end user selects **Forgot Password**.



- 3 The end user enters the correct answers to the recovery questions and clicks **Finish**.



The screenshot shows a blue background with the Dell logo at the top center. Below the logo, the text "Dell Data Protection - Security Tools" is displayed. Underneath, the heading "Recovery Questions" is centered. There are three text input fields, each with a question above it: "What is your mother's middle name?" with the answer "dell", "Who was your first employer?" with the answer "1234", and "Who was your first teacher?" with the answer "5678". A "Finish" button is located below the input fields. At the bottom, the text "Enter authentication answers." is displayed. A small "Tools" link is visible in the bottom left corner.

Assisted Recovery, PBA

- Assisted recovery will be needed if you cannot gain access to the computer using any commands or policies and you need to bypass the PBA login. Some examples include:
 - You need to remove SED management because it is malfunctioning and you need to get to the Windows login screen.
 - You need to deactivate the computer, but cannot because:
 - a PBA failure has occurred.
 - the operating system has been accidentally re-imaged so there effectively is not an SED client.

Prerequisites

Ensure that the following prerequisites are met before beginning the recovery process.

- Ensure that you have physical access to the drive to be recovered.
- Ensure that you have USB media or a network drive available to save the recovery file downloaded from the Remote Management Console.
- Ensure that you have access to the Dell installation media. The files in the “Windows Recovery Kit” folder contain the files needed for this process.
- Be prepared to create a WinPE image. All instructions and special drivers that are needed to create a WinPE image and recover the computer are included in the “Windows Recovery Kit” folder.

Retrieve the Recovery Bundle

This section details part of the steps to take when data recovery is needed for an SED.

- 1 As a Dell Administrator, log in to the Remote Management Console.
- 2 In the left pane, click **Actions > Recover Data**.
- 3 Click the **SED** tab on the top menu.
- 4 In the *Recover SED Endpoint* area, enter the Host Name of the computer and click **Create Recovery File**.
The *Host Name* is typically the fully qualified host name. If not, you can find the *Host Name* on the Endpoint Detail page in the Endpoint Detail section. It is listed as the Unique ID.
- 5 When prompted, save this file to USB media or a network drive. Dell suggests using the default naming convention of [hostname].dat.
- 6 Go to the Dell installation media and locate the “Windows Recovery Kit” folder.
- 7 Open *Instructions for building the WinPe.txt* and follow the instructions to create the WinPE image that will be used to recover the computer.

How to Turn Off Manager SSL Trust Validation

When using SED or BitLocker Manager and you want to turn off Manager SSL trust validation, follow the steps below.

Dell Enterprise Server

NOTE: The Server Configuration Tool and the Remote Management Console cannot run simultaneously. Close the Remote Management Console before opening the Server Configuration Tool.

- 1 In the Server Configuration Tool on the *Settings* tab, check the box for **Disable Trust Chain Check**.
- 2 Save your changes and close the Server Configuration Tool.
- 3 On the client computer, add the following registry entry:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

NOTE: Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. Dell does not recommend the use of self-signed certificates for a production environment.

Manager SSL trust validation is now turned off.

DDP Enterprise Server - VE

If a self-signed certificate is used on VE for SED or Bitlocker Manager, SSL trust validation must be disabled on the client computer. On the VE Server, SSL trust validation is disabled by default.

On the client computer, add the following registry entry:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

NOTE: Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. Dell does not recommend the use of self-signed certificates for a production environment.

Manager SSL trust validation is now turned off.

How to 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 DDP 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 User Name, 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 DDP Server of that user activating on this computer. In turn, there is no way to generate a Response Code from the DDP 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 DDP Server.

- 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.
Click the **blue arrow**.
- 5 Click **OK** when the Legal Notice screen displays.
- 6 Log in to Windows with the user credentials for this computer. These credentials must be part of the domain.
- 7 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.
- 8 Shut down and restart the computer.
- 9 At the login screen, enter the User Name, Domain, and Password that was previously used to log in to Windows.

NOTE: You must match the UPN format that was used when creating the PBA user. Thus, if you used the format `username@domain.com`, you must enter `username@domain.com` for the Username.

- 10 Respond to the Question and Answer prompts.
Click the **blue arrow**.
- 11 Click **OK** when the Legal Notice screen displays.
Windows now launches and the computer can be used as usual.

How to 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 track down the issue.
- You are unable to see the Server connection icon. The log file contains information to help diagnose Server connectivity issues.
- Authentication fails even when entering correct credentials. The log file used with the Server logs can help diagnose the issue.

Follow these steps to capture logs when booting into the 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.

NOTE: 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 with the UPN user format. 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.

Section V. User Experience - Credential Management and Authentication Applications

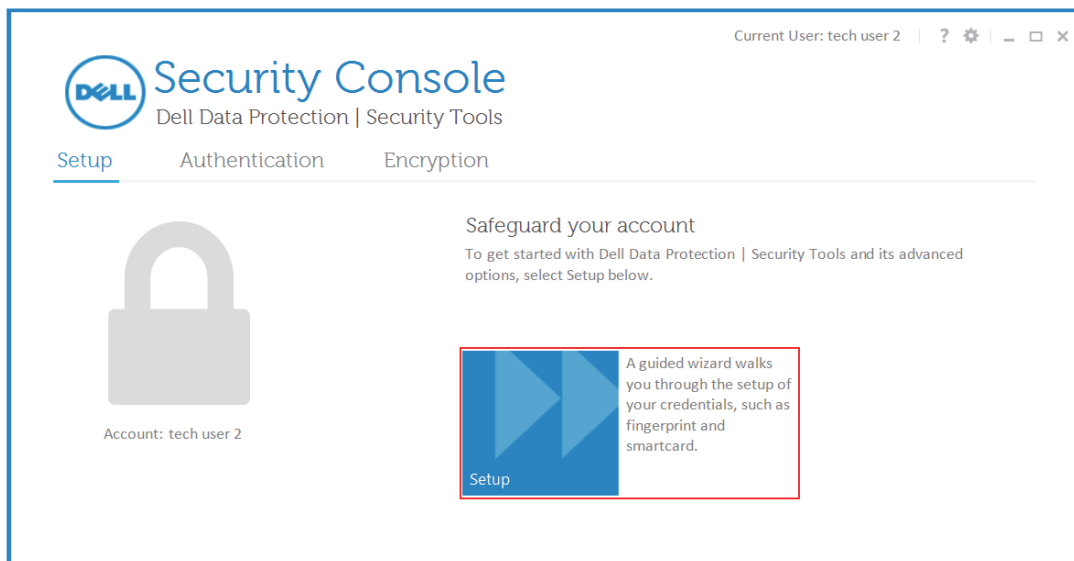
Configure Credentials in the Security Console

- The Security Console is the centralized user interface for all end users of the computer.

The Security Console is used to set up and manage users' credentials, view the enrollment status of their credentials, back up and restore program data as well as Password Manager logons and credentials for Windows. The Security Console provides a wizard-driven user interface to enable end users to configure their credentials and self-recovery questions.

The Security Console provides end users with an easy way to enroll their authentication credentials, manage their logons to websites, programs and network resources, back up and restore program data, and monitor encryption status. The Security Console contains three tabs: Setup, Authentication, and Encryption.

- 1 Instruct end users to launch the Security Console from the *Start Menu* or the *System Tray*.
- 2 When the Security Console launches, the **Setup** tab displays. The end user clicks **Setup** to launch the Setup wizard.



- 3 The end user clicks **Next** at the Welcome page.
- 4 Verify Your Identity

The end user enters their Windows password to verify their identity and clicks **Next**.

The screenshot shows the 'Verify Your Identity' page in the Dell Security Console. The top navigation bar includes 'Setup', 'Authentication', and 'Encryption'. The left sidebar lists 'Verify Your Identity' (selected), 'Recovery Questions', 'Choose Credentials', 'Enroll Credentials', and 'Summary'. The main content area has the heading 'Verify your identity with Windows password. This prevents other users from setting up Dell Data Protection | Security Tools under your account.' Below this is a 'Windows password' label and a text input field. At the bottom right are 'Back' and 'Next' buttons. The top right corner shows 'Current User: tech user 2' and window control icons.

5 Recovery Questions

A question and answer-based method of authentication is provided for end users to access their Windows account if other credentials are unavailable (for example, if they forgot their password). The end user selects the Administrator's pre-defined questions (these questions were selected when policies were set up in the Remote Management Console) from the drop-down menu and then enters and confirms their answers. The end user may also click *Skip recovery questions setup* to bypass this page at this time. The end user clicks **Next** when finished.

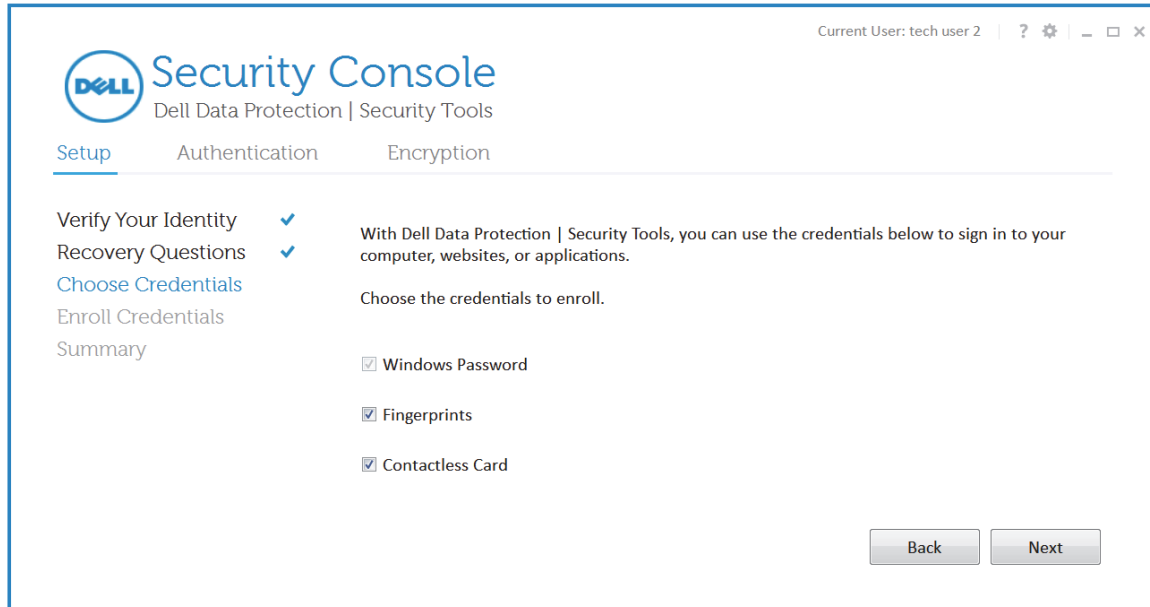
NOTE: After Recovery Questions have been set up, this page no longer displays the Recovery Questions. Instead, links to the *Re-enroll Recovery Questions* page and *Delete Recovery Questions* page display.

The screenshot shows the 'Recovery Questions' page in the Dell Security Console. The top navigation bar includes 'Setup', 'Authentication', and 'Encryption'. The left sidebar lists 'Verify Your Identity' (with a checkmark), 'Recovery Questions' (selected), 'Choose Credentials', 'Enroll Credentials', and 'Summary'. The main content area has the heading 'Recovery questions will be presented if you are unable to authenticate using a credential, like a password, fingerprint, or smartcard. To continue without creating your Recovery questions, click the Skip link below.' Below this are three question sets, each with a 'Choose your question' dropdown, an 'Answer' field, and a 'Confirm' field. At the bottom right is a 'Hide Answers' checkbox. At the bottom left is a 'Skip Recovery questions setup' link. At the bottom right are 'Back' and 'Next' buttons. The top right corner shows 'Current User: tech user 2' and window control icons.

6 Choose Credentials

On the *Choose Credentials* page, the end user can select which additional credentials to enroll at this time. By default, all credentials permitted by the Administrator and supported by the computer's hardware and software are listed on this page. Disconnected peripherals are not displayed until they are reconnected. The end user clicks **Next** to continue to enroll the selected credentials.

NOTE: Credentials may be enrolled at any time by re-launching the Setup Wizard.



7 Enroll Credentials

During the process of enrolling the credentials selected in the previous step, a series of pages are presented to the end user to enroll their credentials. The actual pages shown will vary, depending on the credentials selected by the end user.

a Fingerprint Enrollment

The end user enrolls their fingerprint credential on the *Choose Credentials* page.

The end user clicks the desired finger to enroll and clicks **Save**. The end user may also click *Skip fingerprint enrollment* to bypass this page at this time.

NOTE: The minimum and maximum number fingerprints to enroll is Administrator-configured in the Remote Management Console.



The number of swipes needed to complete fingerprint enrollment depends on the quality of the fingerprint scan. The end user clicks **Save** when finished with each finger.



To delete an enrolled fingerprint, click the highlighted fingerprint. A confirmation dialog displays, which ensures that the end user intends to delete the fingerprint. The end user clicks **Save** when finished.

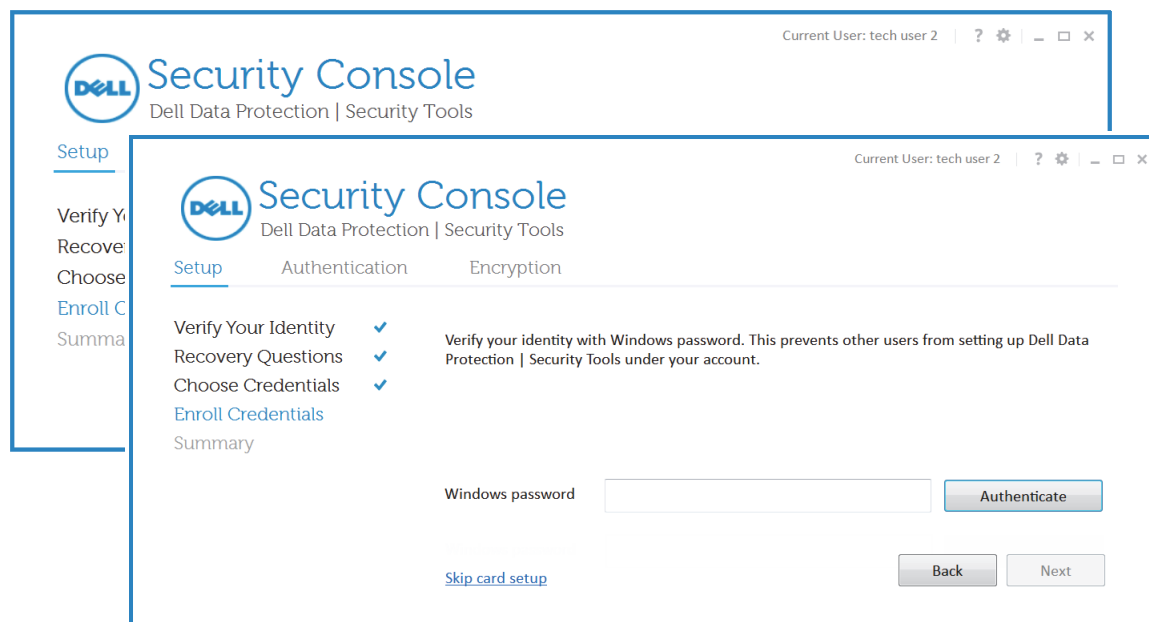


b Card Enrollment

To set up a built-in contactless card, place the card very close to the reader. Once the contactless card communicates with the reader, the end user is prompted to verify their identity. The end user enters their Windows password and clicks **Authenticate**.

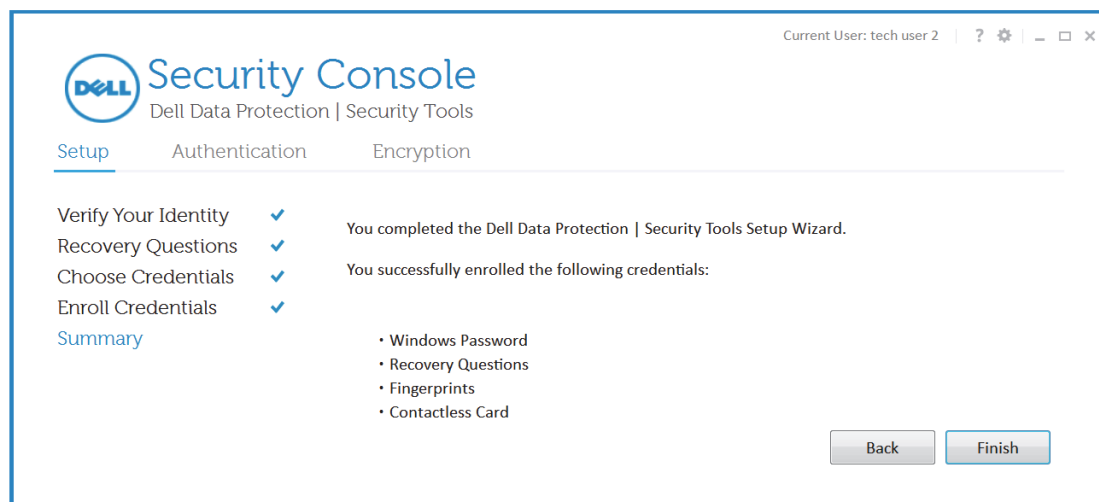
If authenticating with a CAC that has more than one certificate, the user selects the correct certificate from a list.

The end user is prompted to **Save** the credential information after authentication of the card.




c Enrollment summary

A summary of the credentials enrolled is shown after enrollment of required credentials is complete. The end user clicks **Finish** to close the wizard.



- 8 The **Encryption** tab displays the protection status of the computer. Once provisioned (encrypted), the status updates to **Protected**.



Security Console

Dell Data Protection | Security Tools

Current User: tech user 2 | ? ⚙️ □ ×

SetupAuthenticationEncryption

0110000
11011110111101111
000000000000000010000
000110000110000111001111
01111110111101111000001
000000000000000000000110
000001000000000000000000
0001000011000000000000110
011010000001000000000000
000000000100000000000000
000110000000000000000000
00000100000101101001
000001000001101100
01010101

Account: tech user 2
Status is: **Unprotected**

Protect your data

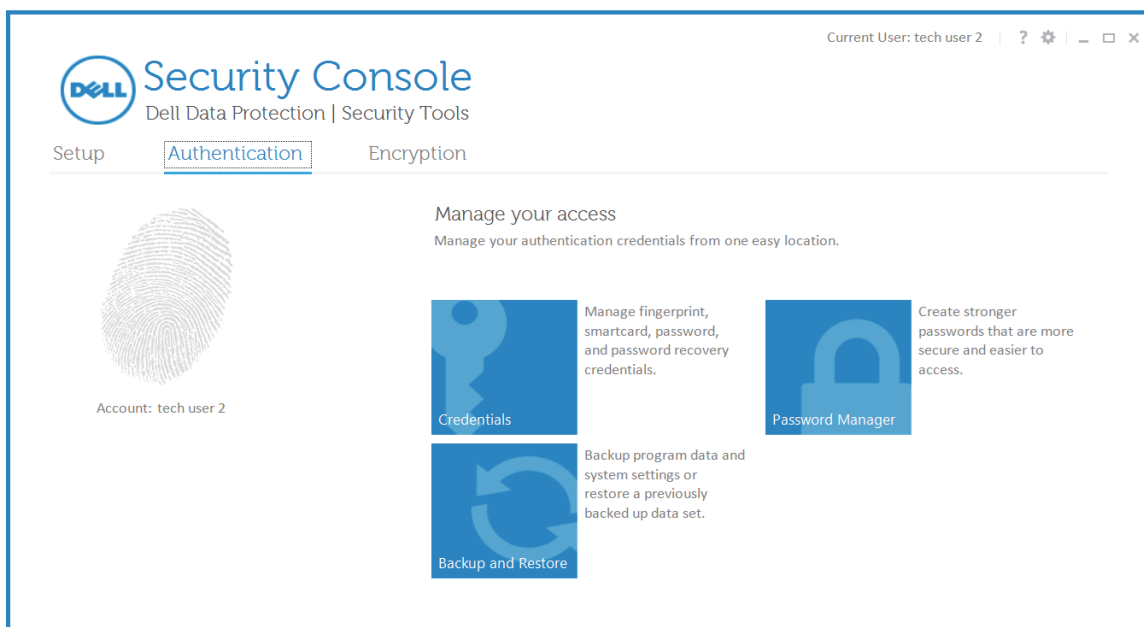
The encryption dashboard allows you to view the protection status of the computer.

Drive 0 238.47 GB Unprotected	Partition 0 140.82 GB Unprotected	Disk C: "os" 140.82 GB total, 104.56 GB free (74% available) Unprotected
	Partition 1 97.66 GB Unprotected	Disk D: "Images" 97.66 GB total, 88.98 GB free (91% available) Unprotected
Drive 1 958.8 MB Unprotected	Partition 0 958.8 MB Unprotected	Disk F: 958.5 MB total, 91.6 MB free (9% available) Unprotected

Use the Authentication Applications

The Security Console provides access to three applications through the tiles located on the **Authentication** tab. The applications are:

- [Credentials](#)
- [Backup and Restore](#)
- [Password Manager](#)



Credentials

The *Credentials* application provides a way to enroll end user credentials. By default, end users enroll and modify their own credentials. However, Administrators may limit the ability of the end user to enroll or manage credentials.

Enrollment Status

The *Enrollment Status* page is the default page shown when you click the Credentials tile. This page displays a list of all supported credentials and specifies their status: Required, Optional, or Disabled.

End users can access details about each credential by clicking the credential in the status list or through the navigation on the left menu.

However, if you have prohibited end users from **enrolling** their credentials, the navigation to the end users' credentials is hidden. The following message displays on the page: *No credentials allowed for setup. Please contact your administrator.*

If you have prohibited **modification** of credentials, the following message displays: *<type of credential> No credentials allowed for modification. Please contact your system administrator.* The end user clicks **OK** to dismiss the dialog.

Current User: tech user 2

?

⚙

▢

✕

Dell

Security Console

Dell Data Protection | Security Tools

Setup

Authentication

Encryption

Enrollment Status

Windows Password

Recovery Questions

Fingerprints

Cards

Enrollment Status

A credential is a means of verifying your identity. For example, your Windows password is a credential.

With Dell Data Protection | Security Tools you can use your credentials when signing in to your computer, websites, or applications. Credentials may be disabled, optional or required by your logon policy. Status of each credential is listed below.

Credentials	Requirements	Status
Windows Password	Optional	✔
Recovery Questions	Optional	✔
Fingerprints	Optional	✔
Contactless Card	Optional	✔

Windows Password

The *Windows Password* page allows end users to easily change their Windows password from within the Security Console. Password changes are effective immediately after clicking **Change**.

NOTE: End users should be instructed to change their Windows password **only** in the Security Console, rather than in Windows. If the Windows password is changed outside of the Security Console, a password mismatch will occur, requiring a recovery operation.

The screenshot shows the Dell Security Console interface. At the top left is the Dell logo. Below it are three tabs: 'Setup', 'Authentication' (which is selected and highlighted in blue), and 'Encryption'. Under the 'Authentication' tab, there is a list of options: 'Enrollment Status', 'Windows Password' (highlighted in blue), 'Recovery Questions', 'Fingerprints', and 'Cards'. The main content area is titled 'Windows Password'. It contains the following text: 'Changing the Windows password requires a correct entry of the existing password.' and 'New passwords may require password complexity requirements set by your administrator.' Below this text are three input fields labeled 'Current Windows password', 'New Windows password', and 'Confirm new password'. At the bottom right of the form are two buttons: 'Change' (in blue) and 'Cancel' (in grey). In the top right corner of the window, there is a label 'Current User:' followed by a small rectangular box.

Recovery Questions

The *Recovery Questions* page is as described in the Setup Wizard. See [Recovery Questions](#).

Fingerprints

Fingerprint enrollment is as described in the Setup wizard. See [Fingerprint Enrollment](#). You can grant permission to end users to enroll or modify fingerprint credentials in the Remote Management Console.

Cards

Card enrollment is as described in the Setup Wizard. See [Card Enrollment](#).

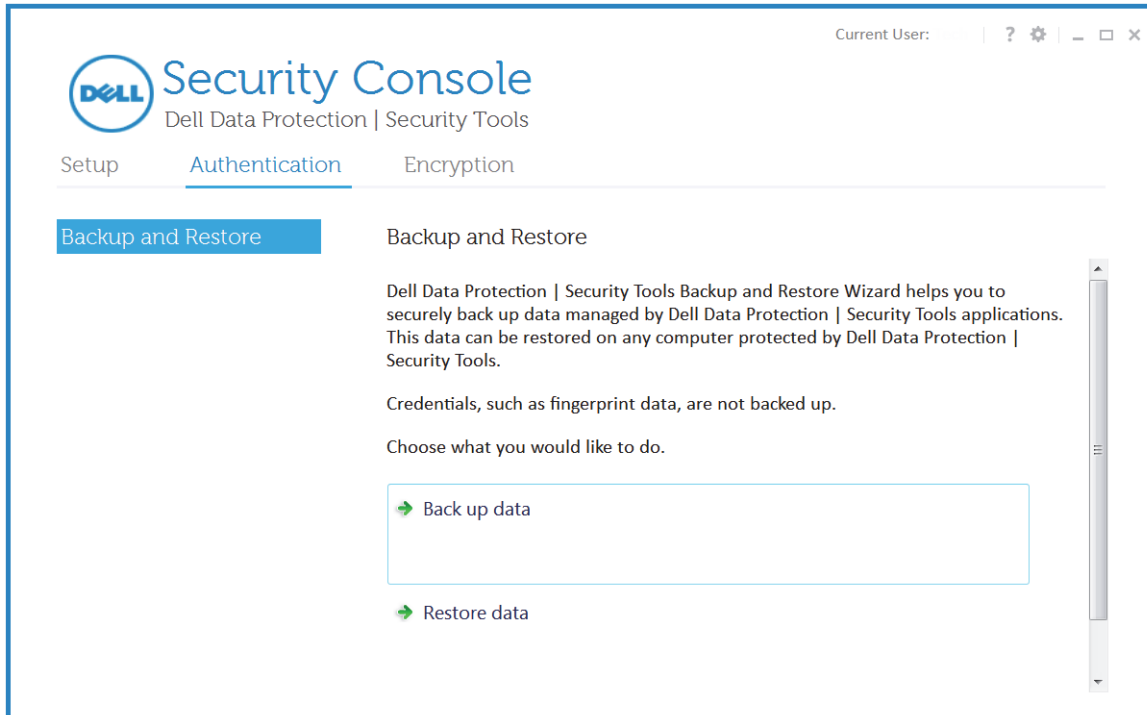
If authenticating with a CAC that has more than one certificate, the user selects the correct certificate from a list.

Backup and Restore

The Backup and Restore Wizard helps end users securely back up passwords managed by Password Manager. This data can be restored on any computer protected by Password Manager.

- 1 Click the **Backup and Restore** tile on the *Authentication* page.
- 2 Click either **Back up data** or **Restore data** to launch the Backup and Restore Wizard.
- 3 End users can also view a text log of backup and restore operations performed on this computer by clicking **View Backup and Restore log** at the bottom of the *Backup and Restore* page.

NOTE: The data backed up does not include operating system or PBA logon credentials or credential-specific information, such as the end user's fingerprints.

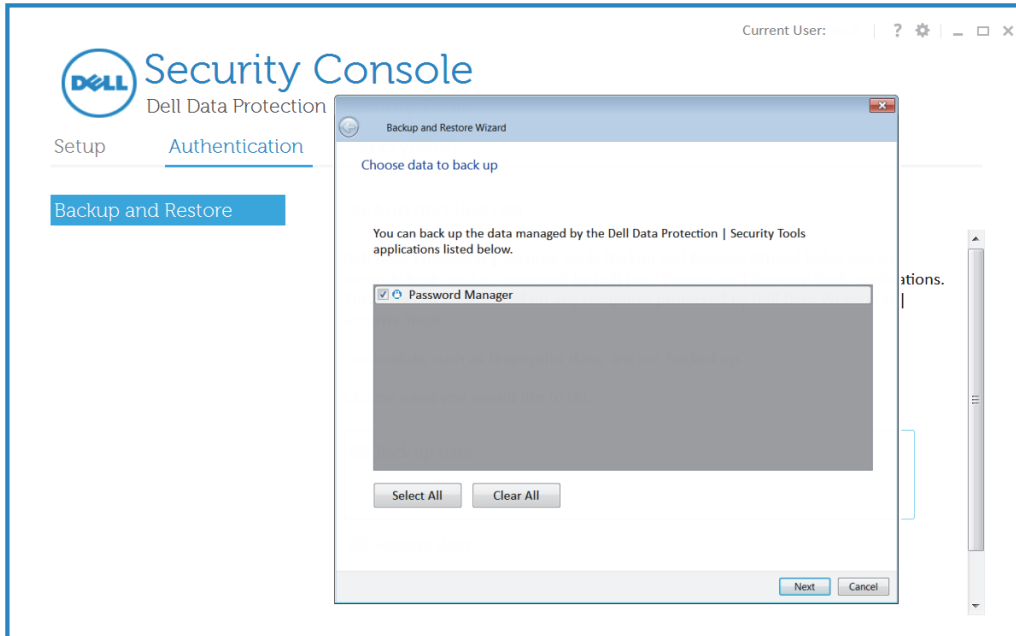


Back up Data

- 1 Click **Back up data** to launch the Backup and Restore Wizard.

The first page of the wizard allows the end user to select the application data to back up. By default, Password Manager is selected.

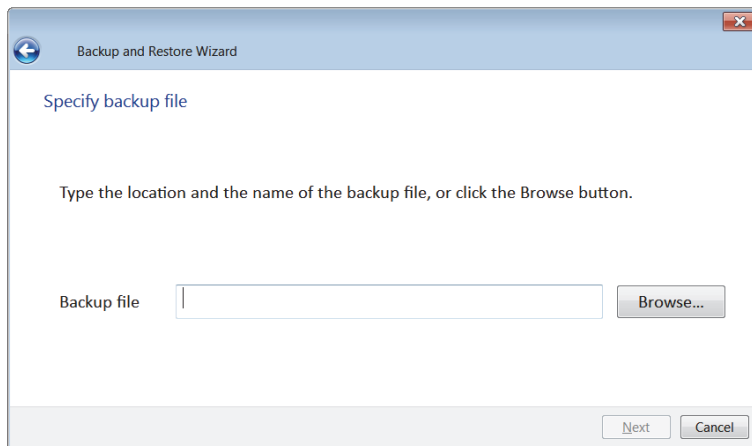
- 2 The end user clicks **Next**.



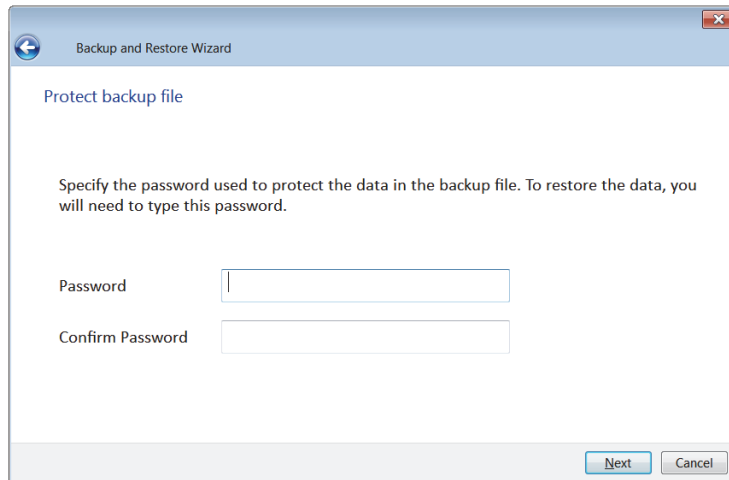
- 3 On the second page of the wizard, the end user types the location and name of the file to be created or navigates to the desired location by clicking **Browse**.

If the end user attempts to back up the data to the same drive as the original data, a warning displays a recommendation to back up the data to portable storage or a network drive.

- 4 The end user clicks **Next**.

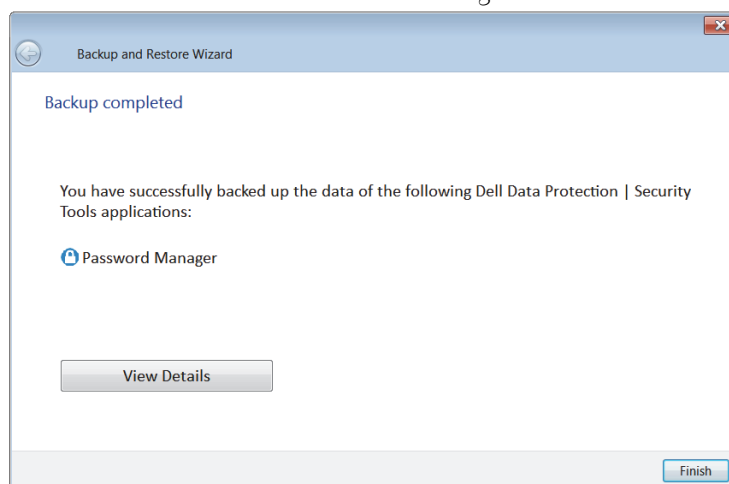


- 5 On the third page of the wizard, the end user must enter and confirm a password to protect the data in the backup file.
- 6 The end user clicks **Next**.



The screenshot shows a window titled "Backup and Restore Wizard" with a back arrow icon. The main heading is "Protect backup file". Below it, a message states: "Specify the password used to protect the data in the backup file. To restore the data, you will need to type this password." There are two text input fields: "Password" and "Confirm Password". At the bottom right, there are "Next" and "Cancel" buttons.

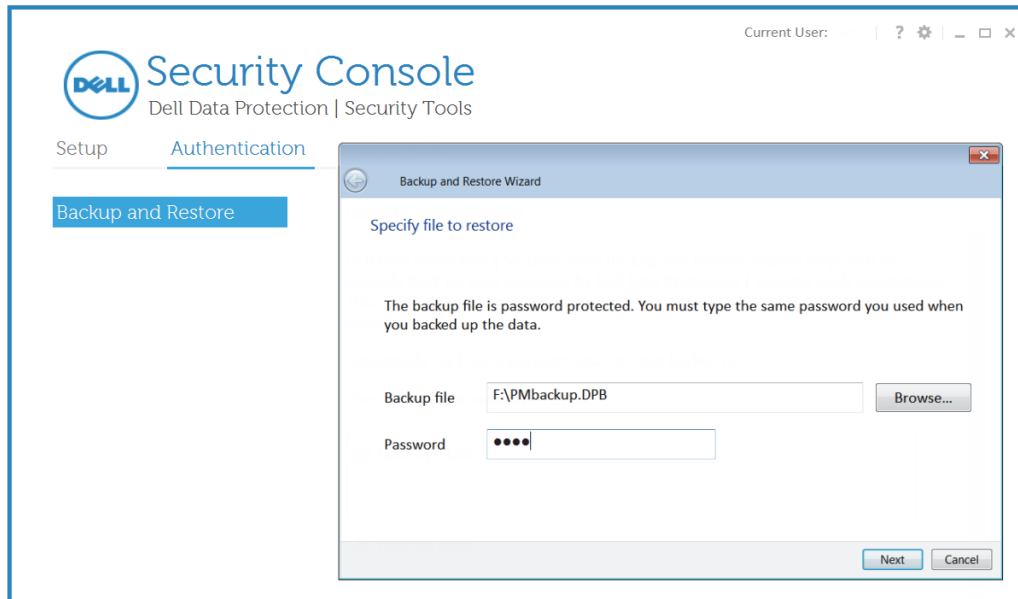
- 7 The final page of the wizard informs the end user that the backup has been completed and lists the applications that have had their data backed up.
The end user clicks **View Details** to view a text log of the backup operations performed.
The end user clicks **Finish** to close the dialog.



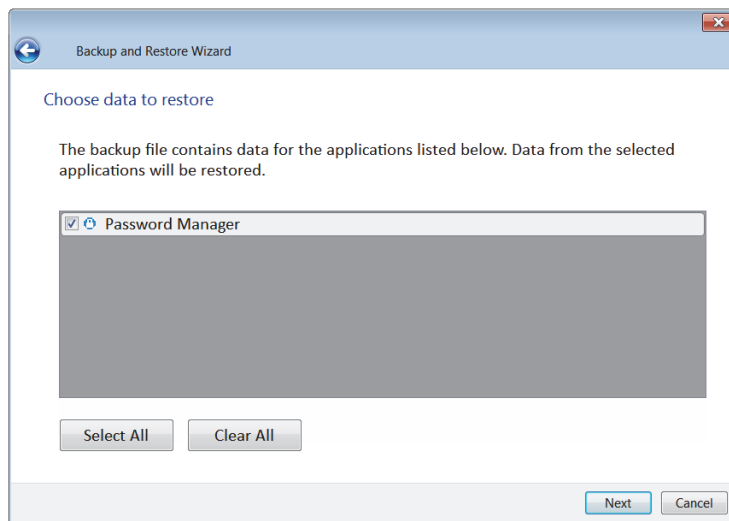
The screenshot shows a window titled "Backup and Restore Wizard" with a back arrow icon. The main heading is "Backup completed". Below it, a message states: "You have successfully backed up the data of the following Dell Data Protection | Security Tools applications:". There is a list item with a blue icon and the text "Password Manager". Below the list, there is a "View Details" button. At the bottom right, there is a "Finish" button.

Restore Data

- 1 Click **Restore data** to launch the Backup and Restore Wizard and to restore the data that was previously backed up using [Back up Data](#).
- 2 The end user enters the name and location of the backup file or clicks **Browse** to navigate to the file and then enters the password for the file. The end user clicks **Next**.

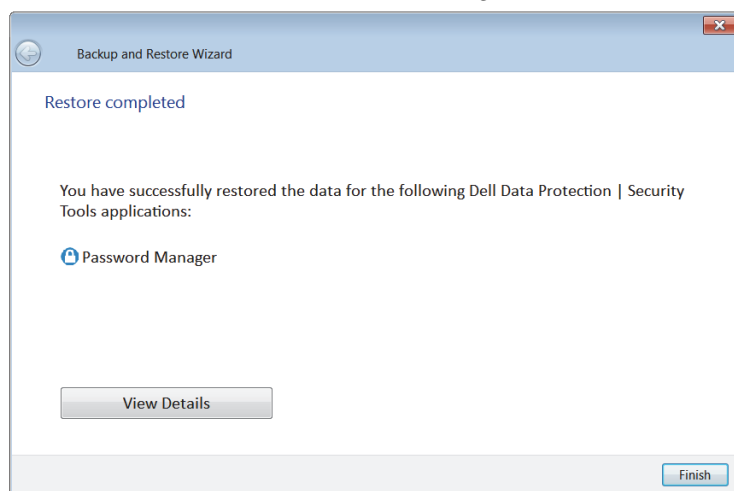


- 3 On the next page of the wizard, the end user is asked to select the data to restore. By default, all data that is managed is restored. The end user can deselect specific applications that they do not want to have restored at this time. The end user clicks **Next**.



- 4 The final page of the wizard informs the end user that the restore has been completed, and lists the applications that have had their data restored.
The end user clicks **View Details** to view a text log of the backup operations performed.

The end user clicks **Finish** to close the dialog.



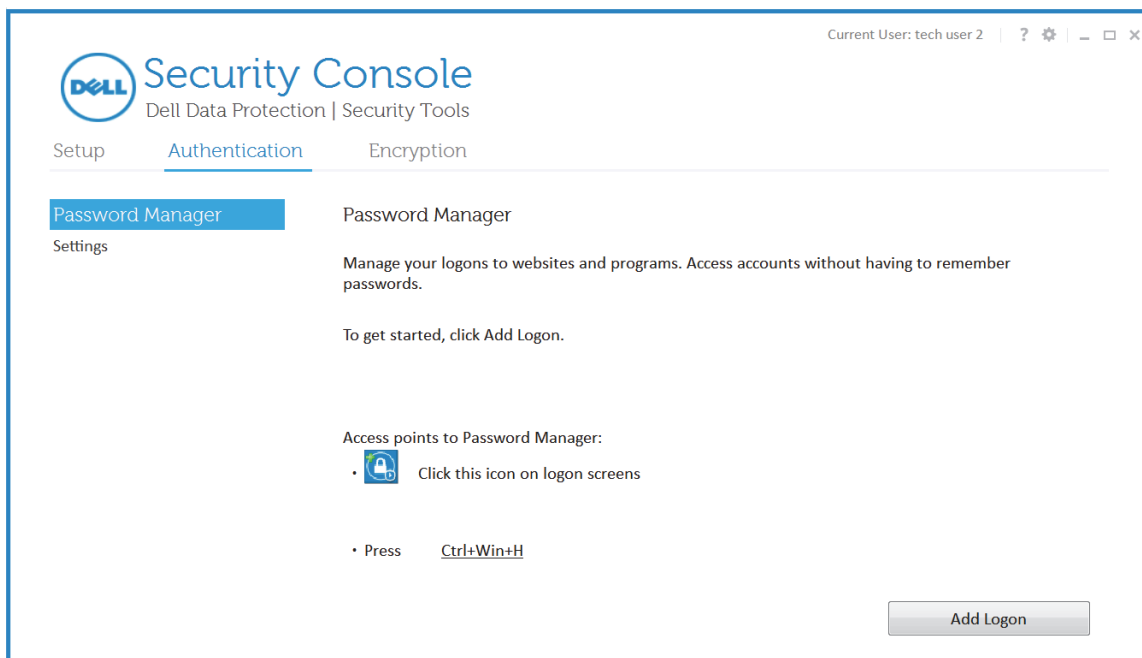
Password Manager

Password Manager allows an end user to automatically fill in and submit data required to log on to websites, Windows applications, and network resources. Password Manager also provides the capability for an end user to change their logon passwords through the application, ensuring that logon passwords maintained by Password Manager are kept in sync with those of the targeted resource.

NOTE: Due to the ever changing structure of web logon screens, the software may not be able to support all websites at all times.

Website and Application Logon Training

- To train new website and application logons, an end user launches the logon screen (a web page or program) to train. An icon displays when the software detects the logon screen. Alternatively, the end user can click **Add Logon** and then navigate to the web page or program logon screen.



- The Password Manager icon in the upper left area of a screen indicates that this screen can be trained with the software.



- To start training a logon screen, an end user can perform any of the following actions:
 - Scan enrolled credentials. An end user with an enrolled fingerprint or contactless smart card can touch the fingerprint reader with an enrolled fingerprint or present an enrolled card to the card reader.
 - Double-click the active area of the Password Manager icon (arrow) or click the active area and select the appropriate item from the context menu.
 - Press the Password Manager hot key combination (user configurable). The default is Ctrl+Win+H).

- After performing one of the above-listed actions, the *Add Logon to Password Manager* dialog displays.

Add Logon

- The end user adds their logon information for the website or program in the Add Logon dialog.
- The end user can add or subtract logon fields or edit the field labels through the *More fields* button.
- For password fields, a password strength indicator is shown below the password field in the dialog. The indicator bar changes from red (weak) to yellow (medium) to green (strong). To accommodate color blindness, the length of the strength bar grows as the password becomes stronger. A message is shown to alert the end user of the password strength. Because this is training an existing logon, the end user can only create a stronger password by going to the change password screen of the website or application.

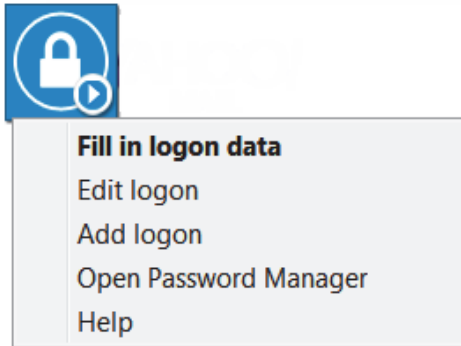
NOTE: If there are several editable fields on the logon screen, the software may not choose the desired editable fields automatically. To specify which fields to include, the end user can click the *More fields* button. The *More Fields* dialog box is displayed and the end user can specify the desired fields. When the end user navigates to a field in the *More Fields* dialog, the corresponding field on the logon screen is highlighted.

The screenshot shows the 'Add Logon to Password Manager' dialog box. The 'Account Name' field contains 'accounts.google.com'. Under 'Account information', the 'Email' field is set to 'name@gmail.com' and the 'Password' field is masked with dots. A tooltip titled 'Password Strength' is displayed over the password field, stating: 'For strong password it is recommended to have a length of atleast 8 characters and mix of 2 characters from each group: Alphabet, Number and Symbol.' The dialog also includes a 'Show password' button, a checked 'Submit account data' checkbox, and 'OK' and 'Cancel' buttons at the bottom.

- An end user can edit field labels by clicking on the item in the *fields* list.

The screenshot shows the 'Add Logon to Password Manager' dialog box with the 'More Fields' sub-dialog open. The 'More Fields' dialog has the title 'More Fields' and the instruction 'Select the fields that are required for logon.' It contains a list of fields with checkboxes: 'Email' (checked), 'Password' (checked), and 'Stay signed in' (unchecked). Below the list are several empty text input fields. An 'OK' button is at the bottom of the 'More Fields' dialog. The main dialog also shows the 'Account Name' field and the 'OK' and 'Cancel' buttons at the bottom.

- For logon to applications, Submit changes. A drop-down list of available options displays.
- When saving the entered logon data, the end user is required to authenticate according to the Session Authentication policy in force (configured in the Remote Management Console).
- The Add logon dialog box can also be launched by clicking the *Password Manager* icon on the white arrow of the blue circle and selecting the first menu item.



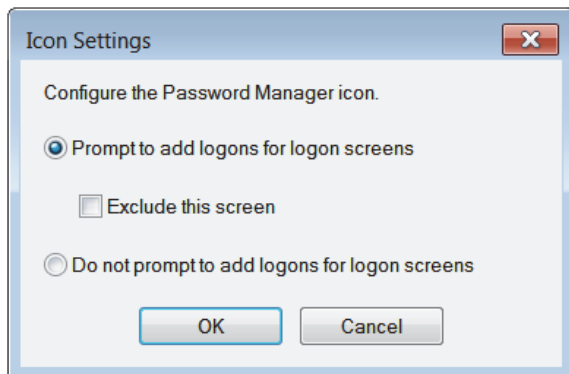
Icon Context Menu

The context menu displays the following options:

- Add <domain> to Password Manager - launches the Add logon dialog.
- Open Password Manager - launches the *Password Manager* page in the Security Console.
- Icon Settings - Allows the end user to configure the display of the Password Manager icon on trainable logon pages.

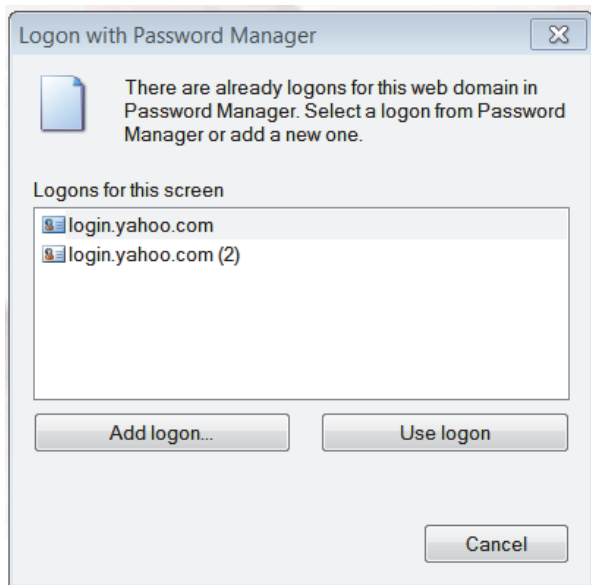
NOTE: The *Exclude this screen* option is not reversible for the specific logon screen for the current user. The *Prompt to add* or *Do not prompt to add* options can be changed on the *Settings* page of the Password Manager application.

- Once trained, the web or application logon displays in Password Manager.



Web Domain Support

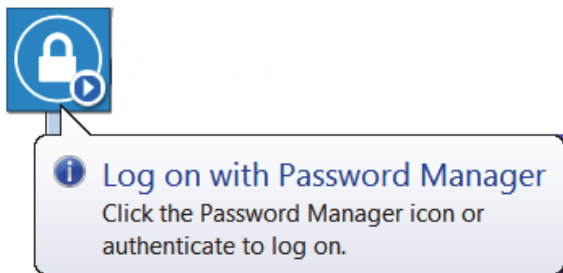
- If an end user has trained a logon screen for a specific web domain but then wants to access his account on that web domain from a different logon screen, the end user can navigate to the new logon screen. The end user is then prompted to use an existing logon or to add a new one to Password Manager.



- If the end user clicks *Use logon*, they are logged on to the previously created account. The next time the end user tries to access that account from the new logon screen, they can access without the prompt.
- If the end user clicks *Add logon*, the Add logon dialog is shown.

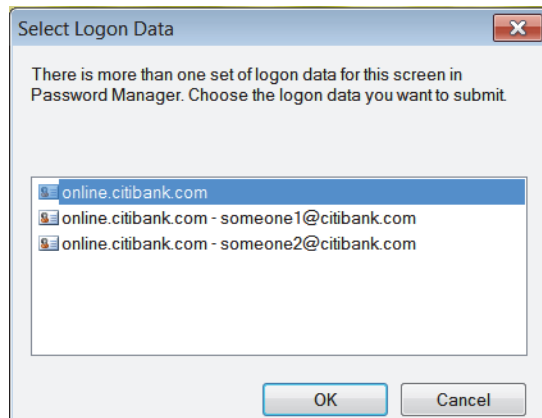
Logging on to Trained Logon Screens

- If the end user directly navigates to a web or application logon, the application detects whether this screen was trained and shows the Password Manager icon in the upper left corner of the screen.
- The first three times the end user accesses a trained logon, an information balloon is shown to guide the end user.



- To start the logon process, an end user can perform any of the following actions:
 - a Scan enrolled credentials. An end user with an enrolled fingerprint or contactless smart card can touch the fingerprint reader with an enrolled fingerprint or present an enrolled card to the card reader.
 - b Double-click the active area of the Password Manager icon (arrow), or click the active area and select the appropriate item from the context menu.
 - c Press the Password Manager hot key combination (user configurable, the default is Ctrl+Win+H).

- The end user must authenticate according to the Session Logon authentication policy in force, which is configurable in the Remote Management Console. Upon a successful authentication, the logon data is filled in on the logon screen. The end user is prompted to choose the account to use if more than one logon for the logon screen exists.



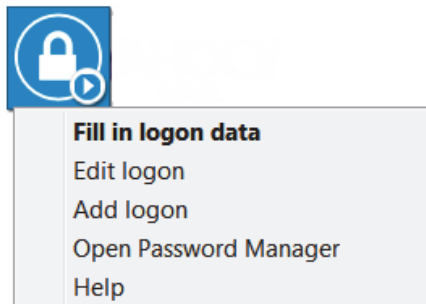
- Additional options are available through the context menu upon successful authentication.

Fill in logon data - If the end user selects *Fill in logon data* or double-clicks the active area of the icon, the logon data populates the logon screen. Using the context menu or pressing the Password Manager hot key combination (default is Ctrl+Win+H) are the only actions available to fill in logon data if password is the only authentication credential available (no Fingerprint, no Contactless or Smart card).

Edit logon - Clicking the *Edit Logon* menu item opens the Edit Logon dialog. The caption is *Edit Logon*. The text is the same as in the *Add Logon* dialog.

Add logon - opens the *Add logon* dialog.

Open Password Manager - The Security Console is opened to the *Password Manager* page.



Filling in with Windows Credentials

- The application allows the end user to use their Windows credentials for web and application logon.

Instead of typing the username and password, the end user can choose their Windows credentials from the drop-down menus available in the *Add Logon* and *Edit Logon* dialogs.

For the username, the end user can choose between the following types:

- Windows User Name
- Windows User Principal Name
- Windows Domain\User Name
- Windows Domain

For the password, the end user can use their Windows password.

All options above are hard-coded and cannot be modified.

Add Logon to Password Manager

Account Name:
login.yahoo.com (2)

Account information
The following logon fields for this website or program have been detected. Type the information that you want Dell Data Protection | Security Tools to fill in automatically.

User name
Password

[Windows User Name]
[Windows User Principal Name]
[Windows Domain\User Name]
[Windows Domain]

Show password More fields...

☒ Submit account data

Use Old Password

- It is possible that an end user may modify a password in Password Manager and then have the password rejected by the application. In this case, the application allows the end user to use a previous password (a password previously entered for this logon page) instead of the most recent one.

User name
Password

[Windows User Password]
[Use previous password...]

Show password More fields...

- If the end user selects *Use previous password*, then after authentication, the end user is prompted to choose an old password from the Password Manager list. The list includes seven passwords and can be deleted permanently by clicking *Clear list*.

Choose Password

To use a previous password instead of your current one, select the password and click OK.

Old passwords

password1

Clear list OK Cancel

Password Change

- Password Manager provides a change password functionality that helps the end user create stronger passwords. When the application detects a password change screen, a dedicated Password Manager icon is shown on the password screen.



- Upon authentication, the end user can change their password from a dedicated change password dialog. Generate password functionality is supported. The end user can also choose the complexity criteria to be used in generating a password.

The image shows two overlapping windows from a software application. The background window is titled "Change password" and contains the following text: "A strong password helps prevent unauthorized access to your account. Type your new password or click Create to generate it automatically." Below this is a text input field labeled "New password" containing eight asterisks. To the right of the input field is a "Create" button with a dropdown arrow. Below the input field is a yellow progress bar and the text "Password strength: Medium". At the bottom left is a "Show password" button, and at the bottom right is a "Save and Fill in" button. The foreground window is a sub-dialog titled "Specify the complexity requirements for the new password if it is generated automatically." It contains two spinners: "Minimum password length:" set to 6 and "Maximum password length:" set to 12. Below these is a label "Password must contain:" followed by a dropdown menu currently showing "Letters and numbers with at least one number".

Password Manager Page




- The *Password Manager* page allows an end user to launch their trained logons and to add, remove, and edit logon data. Until the end user has created a logon, instructional text is shown on the user interface to help the end user understand the password management functionality offered by the program.



After the end user has created a logon, the regular user interface displays.



- Logons are grouped by domain. If an end user has multiple logons for the same web domain, the logons will be listed, indented, under their domain.

	accounts.google.com
	nobody@gmail.comm
	login.yahoo.com
	[Windows User Name]
	online.citibank.com
	someone@citibank.com
	someone2@citibank.com
	someone1@citibank.com

- If the end user clicks the *Manage* command next to a logon, a drop-down menu shows a subset of the following commands, depending on whether a domain or a logon is selected.

Open (default - also triggered if the end user double-clicks the logon)

Edit

Add




Delete

- The logons show a password strength indicator bar for each account added. The indicator bar changes from red (weak) to yellow (medium) to green (strong). To accommodate color blindness, the length of the strength bar grows as the password is stronger.

Categories

All	✕
E-mail	
Banking	
News	



Your Logons

	accounts.google.com	Manage ▼
	nobody@gmail.comm	Add
		Delete
	login.yahoo.com	Manage ▼
	[Windows User Name]	Manage ▼
	online.citibank.com	Manage ▼
	someone@citibank.com	Manage ▼
	someone2@citibank.com	Manage ▼
	someone1@citibank.com	Manage ▼

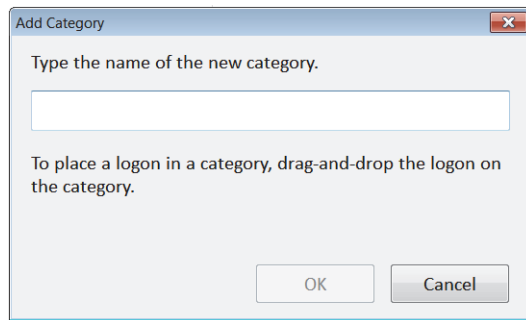
Categories

All	✕
E-mail	
Banking	
News	

Your Logons

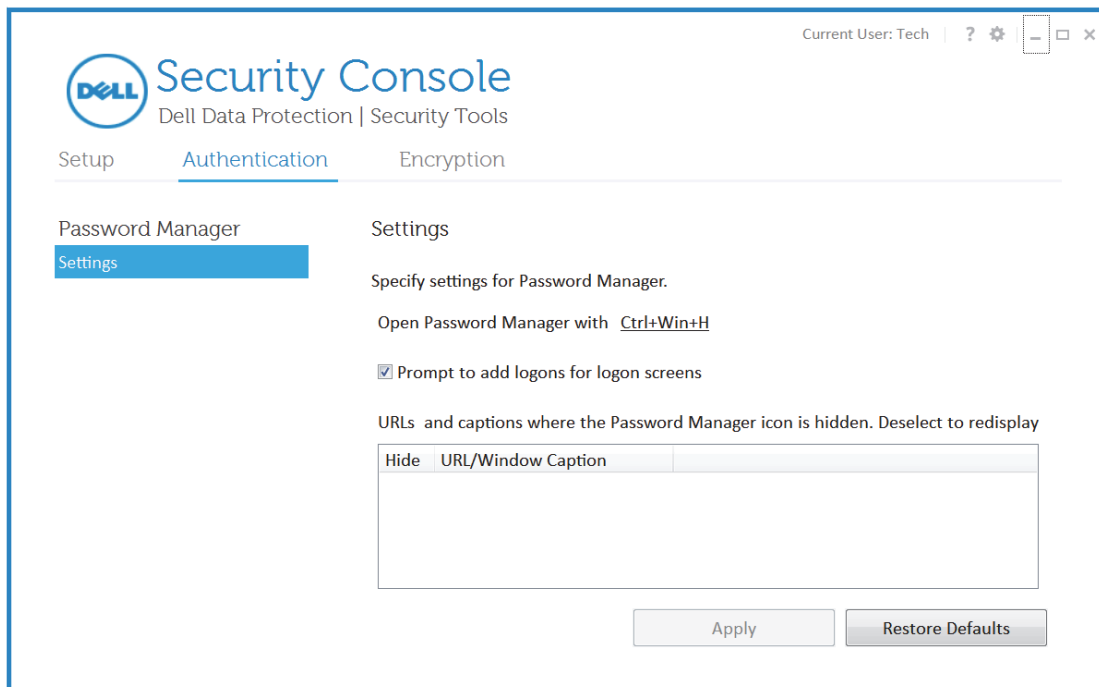
	accounts.google.com	Manage ▼
	nobody@gmail.comm	Manage ▼
	login.yahoo.com	Open
	[Windows User Name]	Edit
		Delete
	online.citibank.com	Manage ▼
	someone@citibank.com	Manage ▼
	someone2@citibank.com	Manage ▼
	someone1@citibank.com	Manage ▼

- If the end user clicks the *Add* category, the Add Category dialog displays.



Settings Page

- On the *Settings* page, the end user can configure the following:
 - The display of the Password Manager icon on the logon screens that can be trained for automatic data fill in. Clearing the **Prompt to add logons for logon screens** check box disables the Password Manager.
 - The key combination that can be pressed to display the Logons menu. The default key combination is “Ctl+Alt+H”.



Section VI. BitLocker Manager

BitLocker Manager Installation Tasks

- You can install BitLocker Manager by itself by extracting the child installer out of the master installer. If you have not extracted the individual installer yet, follow the procedure in [Extract the Child Installers from the Master Installer](#). BitLocker Manager can be installed by command line using any push technology available to your organization.

Best Practices

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.

Install BitLocker Manager

BitLocker Manager Client - locate the installer at C:\extracted\Security Tools

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

Command Line Installation

For a command line installation, 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.

Switches

The following table details the switches available for the installation.

Switch	Meaning
/v	Pass variables to the .msi inside the EMAgent_XXbit_setup.exe (required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the installation.

Log File	Parameters
/l*v [fullpath][filename].log	CM_EDITION=1 <remote management>
	INSTALLDIR= <change the installation destination>
	SERVERHOST= <coreserver.organization.com>
	SERVERPORT=8888
	SECURITYSERVERHOST= <securityserver.organization.com>
	SECURITYSERVERPORT=8443
	ADDLOCAL=DELL_Security_Tools
	ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Options

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

Options	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

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

Example Command Line Installation

- The installation is performed using the **EMAgent_XXbit_setup.exe** file located in the C:\extracted\Security Tools folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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" will create install logs in a "C:\Logs" folder.

- The following example installs BitLocker Manager (silent installation, no reboot, log file at the specified location, 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=securityserver.organization.com  
SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 ADDLOCAL=  
DELL_Security_Tools,BITLOCKER FEATURE=BLM /l*v Bitlockerinstall.log /norestart  
/qn"
```

BitLocker Manager Uninstallation Tasks

These instructions detail the process of uninstalling BitLocker Manager client software.

Prerequisites

- You must have a local or domain Administrator account to uninstall BitLocker Manager.
- Use the same EMAgent_XXbit_setup.exe file to uninstall that was used to install.

Uninstall BitLocker Manager

Command Line Uninstallation

For a command line uninstallation, 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.

Switches

The following table details the switches available for the uninstallation.

Switch	Meaning
/v	Pass variables to the .msi inside the EMAgent_XXbit_setup.exe (required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the uninstallation.

Log File	Parameters
/l [fullpath][filename].log	CM_EDITION=1 <remote management>
	INSTALLDIR= <change the installation destination>
	SERVERHOST= <coreserver.organization.com>
	SERVERPORT=8888
	SECURITYSERVERHOST= <securityserver.organization.com>
	SECURITYSERVERPORT=8443
	ADDLOCAL=DELL_Security_Tools
	ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Options

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

Options	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

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

Example Command Line Uninstallation

- The uninstallation is performed using the **EMAgent_XXbit_setup.exe** file located in the C:\extracted\Security Tools folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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

```
EMAgent_XXbit_setup.exe /x /s /v"/I Uninstall.log /qn"
```

Reboot the computer when prompted.

BitLocker Manager is uninstalled.

BitLocker Manager Recovery

To recover data, you obtain a recovery password or key package from the Remote Management Console, which then allows you to unlock data on the computer.

Recover Data

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

2 In the left pane, click **Actions > Recover Data**.

3 Click the *Manager* tab.

4 For *BitLocker*:

Enter the **Recovery ID** received from BitLocker.

Click **Get Recovery Password** or **Create Key Package**.

Depending on how you want to recover, you will use this recovery password or key package to recover data.

For *TPM*:

Enter the **Recovery ID** received from BitLocker.

Click **Get Recovery Password** or **Create Key Package**.

Depending on how you want to recover, you will use this recovery password or key package to recover data.

5 To complete the recovery, see [Microsoft's Instructions for Recovery](#).

NOTE: If BitLocker Manager does not “own” the TPM, the TPM password and key package are not available in the Dell database. You will receive an error message stating that Dell cannot find the key, which is the expected behavior.

To recover a TPM that is “owned” by an entity other than BitLocker Manager, you should follow the process to recover the TPM from that specific owner or follow your existing process for TPM recovery.

How to Turn Off Manager SSL Trust Validation

When using SED or BitLocker Manager and you want to turn off Manager SSL trust validation, follow the steps below.

Dell Enterprise Server

NOTE: The Server Configuration Tool and the Remote Management Console cannot run simultaneously. Close the Remote Management Console before opening the Server Configuration Tool.

- 1 In the Server Configuration Tool on the *Settings* tab, check the box for **Disable Trust Chain Check**.
- 2 Save your changes and close the Server Configuration Tool.
- 3 On the client computer, add the following registry entry:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

NOTE: Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. Dell does not recommend the use of self-signed certificates for a production environment.

Manager SSL trust validation is now turned off.

DDP Enterprise Server - VE

If a self-signed certificate is used on VE for SED or Bitlocker Manager, SSL trust validation must be disabled on the client computer. On the VE Server, SSL trust validation is disabled by default.

On the client computer, add the following registry entry:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

NOTE: Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. Dell does not recommend the use of self-signed certificates for a production environment.

Manager SSL trust validation is now turned off.

Section VII. Cloud Edition

Cloud Edition Installation Tasks

Before you begin installing Cloud Edition, you must first complete a few tasks on the DDP Server.

DDP Server Tasks

Configure DDP Enterprise Server - VE for Cloud Edition

To configure VE to support Cloud Edition, in the VE Remote Management Console, set the Cloud Storage Protection Enabled protection policy to True.

Configure Dell Enterprise Server for Cloud Edition

To configure Dell Enterprise Server to support Cloud Edition, in the Remote Management Console, set the Cloud Storage Protection Enabled protection policy to True, then [Set Up the Dell Security Server to Allow Cloud Client Downloads](#).

Set Up the Dell Security Server to Allow Cloud Client Downloads

This section details the steps needed to allow end users to download the Windows Cloud client from your Dell Security Server.

- 1 On the Dell Enterprise Server, go to <Security Server install dir>\webapps\cloudweb\brand\dell\resources and open the messages.properties file with a text editor.
- 2 Ensure that the entries are as follows:
download.deviceWin.mode=remote
download.deviceWin.local.filename.32=cloud32.exe
download.deviceWin.local.filename.64=cloud64.exe
download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/cloud32.exe
download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/cloud64.exe
- 3 Save and close the file.
- 4 Go to <Security Server install dir> and create a new folder under it named Download (Security Server\Download).
- 5 Within the Download folder, create another new folder and name it Cloudweb (Security Server\Download\Cloudweb).
- 6 Add the 64-bit and the 32-bit setup files for Cloud Edition to the Cloudweb folder and rename them to cloud64.exe and cloud32.exe, respectively.

Set Up the Server for Automatic Downloads of the Windows Cloud Client (Optional)

- 1 On the server hosting your Dell Enterprise Server, go to C:\inetpub\wwwroot\.

NOTE: This web server must have a trusted certificate.

- 2 Create a folder under wwwroot named CloudUpdate (C:\inetpub\wwwroot\CloudUpdate).

NOTE: CloudUpdate is used in this example, but you can choose any name.


- 3 Place the updated executables in the CloudUpdate folder.
- 4 Place the updated *versions.xml* file in the CloudUpdate folder.
- 5 Open *versions.xml* with a text editor and verify the filename path is correct for your environment.

Sample:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION channel="release" brand="1" arch="x86" version="1.0.0.1814" filename="/Cloud32.exe"/>
<VERSION channel="release" brand="1" arch="x64" version="1.0.0.1814" filename="/Cloud64.exe"/>
</VERSIONS>
```

Version: File version of the updated executables

Filename: Path from the end of the URL above (/CloudUpdate) to the actual executables.

- 6 Save and close the file.
- 7 Restart IIS.
- 8 As a Dell administrator, login to the Dell Remote Management Console.
- 9 In the left pane, click **Protect & Manage > Enterprise**.
- 10 Click **Security Policies** on the top menu.
- 11 Select the Policy Category: **Cloud Storage** from the drop-down list.
- 12 Expand the Policy grouping  to show *Cloud Storage Settings*.
- 13 Scroll to the *Software Update Server URL* policy and enter **https://<YOUR HOST URL>/CloudUpdate**.

NOTE: CloudUpdate is only an example to match the example above.

- 14 Click **Save** to store the policy modification in the queue to commit.
- 15 Click **Actions > Commit Policies**.
- 16 Click **Apply Changes**.

Allow/Deny Users on Whitelist /Blacklist

The whitelist and blacklist entries determine which users can register with the DDP Server to use Cloud Edition. For adequate security, be sure to carefully set up and manage these lists.

Whitelist

The whitelist allows specific users or groups of users to register with the DDP Server and to use Cloud Edition. To allow [external users](#), they must be placed on the whitelist to allow registration. However, in order for the blacklist to be used, if you have used a wildcard in the whitelist, it must be removed. See the following examples:

`<Allow>*@organization.com</Allow>` Allows all organization.com email addresses to register with the DDP Server.

`<Allow>*</Allow>` All users are allowed to register DDP Server.

`<Allow>jdoe@organization.com</Allow>` Allows this specific user to register with the DDP Server.

`<Allow>*@gmail.com</Allow>` Allows all Gmail[®] users to register with the with the DDP Server.

Blacklist

The blacklist prevents specific users or groups of users from registering with the DDP Server and using Cloud Edition.

This list does not prevent users who are already registered from using Cloud Edition. Users whose email addresses are entered in the blacklist receive a message stating that they cannot register for Cloud Edition.

You can use the blacklist to exclude specific users who are members of approved groups on the whitelist. Additionally, using the wildcard (*), entire domains can be placed on the blacklist, which will prevent anyone with an email address in that domain from registering. See the following examples:

`<deny>*@organization.com</deny>` Prevents all organization.com email addresses from registering with the DDP Server.

`<deny>jdoe@organization.com</deny>` Prevents this specific user from registering this email address with the DDP Server.

`<deny>*@gmail.com</deny>` Prevents all Gmail users from registering with the DDP Server.

To modify the whitelist/blacklist, follow the instructions below:

- 1 Go to `<Security Server install dir>\conf\`.
- 2 Open `registration-access.xml` with a text editor.
- 3 Allow or deny users based on the above information and the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<access>
  <whitelist>
    <allow>user1@organization.com</allow>
    <allow>*@organization.com</allow>
    -->
    <allow>*</allow>
  </whitelist>
  <blacklist>
    <!--All addresses not specifically allowed are denied.
    <deny> </deny>
    -->
  </blacklist>
</access>
```

- 4 Save and close the file.

An email is automatically sent (as configured in the Server Configuration Tool's SMTP tab) to the users added to the whitelist directing them to `https://yoursecurityservername.domain.com:8443/cloudweb/register`.

Use Dropbox for Business

Cloud Edition with Dropbox for Business offers additional functionality:

- [Remote Wipe a Team Member Account](#)
- With a DDP Enterprise Server - Virtual Edition v8.4 or later, you can set policies to control how business and personal Dropbox folders are protected. If your enterprise allows both business and personal accounts, end users should understand encryption of each type of account. See [Policy for Business and Personal Accounts](#).

Policy for Business and Personal Accounts

Your enterprise may have guidelines on whether team members can use business and personal accounts. Also, the enterprise may allow only certain users to have both business and personal accounts.

NOTE: If your enterprise allows both business and personal accounts, and an end user chooses to use both, the user must understand folder management of both account types.

The following table describes encryption based on your DDP Server and policy.

Encryption	DDP Server and Policy	Deployment Considerations
Encrypt all business and personal files and folders.	DDP Enterprise Server - VE (pre-v8.4) or Dell Enterprise Server or DDP Enterprise Server - VE: v8.4 or later with Policy > <i>Dropbox Encrypt Personal Folders</i> > set to True (True is the default.)	Before Cloud Edition is deployed, users should back up pre-existing business files that are in cloud storage sync folders to locations outside the sync folders. Users with personal files that should remain unencrypted must move the files out of sync folders or unlink personal accounts from business sync clients. After Cloud Edition is deployed, cloud files and folders can be viewed only on computers or devices running Cloud Edition. If a personal folder becomes unintentionally encrypted, see Decrypting Folders in a Personal Account .
Encrypt all business account files and folders. Allow personal account files and folders to remain unencrypted.	DDP Enterprise Server - VE v8.4 or later with Policy > <i>Dropbox Encrypt Personal Folders</i> > set to False	You can use the optional <i>Dropbox Encrypt Personal Folders Message</i> policy to display a customized message to remind users not to store business files in personal accounts, since those files won't be protected. The message is displayed at these times: <ul style="list-style-type: none">• Each time the user logs in• When the user creates or adds a new file or folder to a personal Dropbox account If you set the <i>Dropbox Encrypt Personal Folders</i> policy to False for an Endpoint or Endpoint Group, personal accounts of all users on those endpoints will remain unencrypted.

Business and Personal Folders

If your enterprise has Dropbox for Business and you allow end users to have both business and personal folders, you may want to run reports to ensure that all business files have the .xen file extension, in case an end user copies a sensitive unprotected file into a business folder. See [Run Reports](#).

Remote Wipe a Team Member Account

If your enterprise has Dropbox for Business, you can remotely remove a team member from the corporate Dropbox for Business team account if, for example, a user leaves the company. Files and folders associated with the team member's account will be removed from all devices used by the account. This revokes that user's access to those files.

Prerequisites

NOTE: Before you perform this procedure, you must back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.

Only a Dropbox for Business Administrator can remote wipe a Dropbox for Business account.

The end user must have activated Cloud Edition and connected to Dropbox for Business.

Register in Remote Management Console

Only one Dropbox for Business Administrator needs to register.

- 1 In the Remote Management Console, select **Settings** in the left pane.
- 2 Click the **Cloud** tab.
- 3 Click **Register**.

The browser opens to the Dropbox for Business site.

- 4 If prompted, log in to Dropbox with your Dropbox for Business Administrator account.
- 5 To allow access to Cloud Edition, click **Allow**.

A confirmation page displays to indicate Dropbox authorization is granted to the DDP Enterprise Server - VE.

- 6 In the Remote Management Console, return to **Settings > Cloud** and refresh the page.

The Administrator name displays.

NOTE: Generally, the best practice is not to de-register. However, to withdraw the privileges of the Dropbox for Business Administrator for removing team members from the Dropbox for Business team, click **De-register**.

Remote Wipe a Team Member Account

NOTE: The Remote Wipe option is available only for enrolled Dropbox for Business team member accounts. If the Remote Wipe option does not display for a user account, the user has not enrolled a Dropbox for Business account.

- 1 In the Remote Management Console, select **Users** in the left pane.
- 2 Access the **User Detail** page.
- 3 In the Command column, click **Remote Wipe**.

The remote wipe is performed.

NOTE: Before you select Remote Wipe, you must back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.

- 4 At the confirmation for Remote Wipe, click **Yes**.

The User Detail page lists the date the remote wipe is performed.

- 5 In your Dropbox for Business Administrator Console Members page, refresh the list of Team Members.

The user is removed from the list. You can select the **Removed Members** tab to view which users have been removed.

Run Reports

Reports about your Cloud Edition environment are available through Dell Compliance Reporter, a component of the Dell Enterprise Server and DDP Enterprise Server - VE. For example, you can run reports that detail the following:

- User activations
- Applied policy on a device
- Actions performed on encrypted files
- Dropbox for Business file encryption status

For more information on running reports, see *Compliance Reporter Help*.

Essential Steps

You can run reports to confirm that all internal users have completed some essential steps. For example:

- End users must activate Cloud Edition.
- If your enterprise uses Dropbox for Business, the end user must connect to it through Cloud Edition. Otherwise, you won't have the ability to use Dropbox for Business' Remote Wipe option.

Provide Temporary Folder Management Rights

If users uploaded files before you installed Cloud Edition, you can provide temporary Folder Management rights to some users.

- 1 Set the *Folder Management Enabled* policy for specific end points to **True**.
- 2 Instruct the user to manually turn on encryption for the pre-existing folder. The files will be encrypted when the files sync to the cloud.
- 3 After the folders are encrypted, set the *Folder Management Enabled* policy for those end points to **False**.

Update Cloud Edition Policy

The *Server Polling Period* policy determines how often the client checks for policy updates. If you modify a policy that internal end users need to implement before that time interval, be sure to inform end users to check for the update.

Client Tasks

You can install the Cloud Edition client by itself by extracting the child installer out of the master installer. If you have not extracted the individual installer yet, follow the procedure in [Extract the Child Installers from the Master Installer](#). The Cloud Edition client can be installed using the user interface or by command line using any push technology available to your organization. Activation by the end user is still required.

Before Installing

- As a best practice, deploy Cloud Edition before users set up cloud storage accounts and store files in them.
If end users decide to keep existing cloud storage accounts on computers where Cloud Edition will be installed, they must use the settings in the cloud storage application to deselect any folders that are to remain *unencrypted* before you install Cloud Edition. Otherwise, their existing personal data might be encrypted. For more information, see [Remove Protected Files](#).
- Be prepared to restart the computer after Cloud Edition client is installed. If applicable, notify users of the timeframe during which their computers will be rebooted.

Best Practices

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.

Install Cloud Edition

Cloud Edition Client - locate the installer at C:\extracted\Cloud

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

Command Line Installation

For a command line installation, 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.

Switches

The following table details the switches available for the installation.

Switch	Meaning
/v	Pass variables to the .msi inside the Cloud_XXbit_setup.exe (required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the installation.

Log File	Parameters
/l*v [fullpath][filename].log	SERVER= <securityserver.organization.com>

Options

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

Options	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

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

Example Command Line Installation

- The installation is performed using the **Cloud_XXbit_setup.exe** file located in the C:\extracted\Cloud folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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" will create install logs in a "C:\Logs" folder.

- The following example installs Cloud Edition (silent installation, no reboot, log file at the specified location, installed in the default location of C:\Program Files\Dell\Dell Data Protection)

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /l*v Cloudinstall.log /qn"
```

Reboot the computer and authenticate to Windows.

Installation of Cloud Edition is complete.

Notify End Users

Cloud Edition users must perform the following tasks in order for files and folders in their cloud sync clients to be protected:

- Activate Cloud Edition.
- Download a cloud storage provider.

If your enterprise has a provider preference, specify that.

If your enterprise uses Dropbox for Business, provide users with a link for downloading and installing it.

NOTE: Dropbox for Business users must connect to Dropbox for Business through Cloud Edition.

Also, if your enterprise has previously blocked access to cloud storage, you will need to change that setting.

Activate Cloud Edition and Install a Cloud Sync Client

For information about Cloud Edition user tasks, see [Cloud Edition Activation and User Experience](#).

Cloud Edition Uninstallation Tasks

If an end user has a local Administrator account, they can uninstall Cloud Edition themselves. See *Cloud Edition User Guide*. This section describes the *Administrator* process for uninstalling Cloud Edition.

These instructions detail the process of:

- Removing protected files
- Uninstalling Cloud Edition client software.

Prerequisites

- You must have a local or domain Administrator account to perform the uninstallation.
- Use the same Cloud_XXbit_setup.exe file to uninstall that was used to install.

Remove Protected Files

All encrypted documents on the device **must** be removed locally. Choose one of the following methods to remove protected files:

- **Recommended method:** Turn off syncing from the sync folders. All folders and files will remain in the cloud but will be removed from the local device.
- Delete the files directly from the cloud and allow syncing to occur. The cloud service will show there are no files on the device, and when syncing occurs the local device will remove all data from the shared folder.
- Delete the files directly from the local sync folder. The sync client will observe the change and remove all files from the cloud service.
- The installer offers the option to override its protection check for synchronized files. For more information, see [Override Protection Check for Synchronized Files](#).

Dropbox

- 1 In the system tray, select the **Dropbox icon**, and click the Settings icon.
- 2 In **Preferences**, click the **Account** tab, and then **Selective Sync**.
- 3 Deselect folders to remove syncing.
- 4 Click **Update**.
- 5 At the confirmation dialog, click **OK**. (The folders will be removed from Dropbox on the computer but are still available on the web and other devices.)
- 6 At the Dropbox Preferences window, click **OK**.
- 7 The system tray icon indicates settings are being applied. This may take several minutes.
- 8 When the Dropbox icon indicates that remove syncing is complete, navigate to **Windows Explorer > Dropbox**. If any files or folders were not removed, manually delete them.

Box

- 1 In the system tray, right-click the Box icon and select **Open Box web site**.
- 2 In the Box web site, right-click a file or folder and select **Synced > Unsync**.
- 3 In the Disable Sync window, click **Unsync Folder**.
- 4 The system tray icon indicates settings are being applied. This may take several minutes.
- 5 When complete, navigate to **Windows Explorer > Box**. If any files or folders were not removed, manually delete them.

OneDrive

- 1 In the system tray, right-click the **OneDrive icon**, and click **Settings**.
- 2 Select the **Choose Folders** tab and then click **Choose Folders**.
- 3 Then, select **Choose folders to sync**.
- 4 When the list of folders displays, clear the check boxes to remove syncing and click **OK**.
- 5 Click **OK**.
- 6 The system tray icon indicates settings are being applied. This may take several minutes.
- 7 When complete, navigate to **Windows Explorer > OneDrive**. If any files or folders were not removed, manually delete them.

Uninstall Cloud Edition

Command Line Uninstallation

For a command line uninstallation, 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.

Switches

The following table details the switches available for the uninstallation.

Switch	Meaning
/v	Pass variables to the .msi inside the Cloud_XXbit_setup.exe (required)
/a	Administrative installation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the uninstallation.

Log File	Parameters
/l [fullpath][filename].log	SERVER= <securityserver.organization.com>

Options

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

Options	Meaning
/q	No Progress dialog, restarts itself after process completion

Options	Meaning
/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

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

Example Command Line Uninstallation

- The uninstallation is performed using the **Cloud_XXbit_setup.exe** file located in the C:\extracted\Cloud folder.

NOTE: Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

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

```
Cloud_XXbit_setup.exe /x /s /v"/I Uninstall.log /qn"
```

Reboot the computer when prompted.

Cloud Edition is uninstalled.

OR

Override Protection Check for Synchronized Files

You can uninstall files without stopping synchronization. However, if you use this option, and protected files are currently synchronizing, these files could enter the cloud **unencrypted**. **Use this option with caution.**

To override the check for synchronized files and perform a silent uninstall, enter the following command:

```
Cloud_XXbit_setup.exe /x /s /v"PROTECTIONCHECK=0 /qn"
```

Reboot the computer when prompted.

Cloud Edition is uninstalled.

Section VIII. User Experience - Cloud Edition

Cloud Edition Activation and User Experience

Activate Cloud Edition

After Dell Data Protection | Cloud Edition is installed and the computer reboots, follow these steps:

- 1 Log in to Windows.
- 2 From the Cloud Edition system tray icon, select **User Activation**.
- 3 Enter your domain email address and domain password, and click **Activate**.
After activation finishes, a green check displays on the Cloud Edition system tray icon.
- 4 Confirm your user mode status. Click the Cloud Edition system tray icon and select **Details**.
- 5 At the top, confirm User Mode:
 - **Internal:** A user with an email address within the company's domain.
 - **External:** A user with a non-domain email address.

Install a Cloud Sync Client

NOTE: The installation steps will prompt you for the Server Name that this computer will communicate with, such as server.domain.com. This information is supplied by your Administrator.

The best practice is to select and install just one sync client to work with Cloud Edition. If applicable, use your company's preferred cloud sync client.

- 1 Click one of the following to install a sync client:
 - **Dropbox** (if your company allows business and personal accounts, this is the personal account) - see <https://www.dropbox.com/install>
 - **Dropbox for Business** - If your company has Dropbox for Business, your Administrator will provide you with a link for downloading and installing it. Your enterprise will determine if internal users can have a business account only or if they can use both business and personal folders. If you install Dropbox for Business, see [Authenticate Dropbox for Business](#).
 - **Box** - see <https://www.box.com/platform/>
 - **OneDrive** - see <https://onedrive.live.com/about/en-us/download/>
- 2 In the sync client, create a shared folder or accept an existing one from another person or group in your company.
If you are running one of the following, you can access a sync client folder from the system tray:
 - **Dropbox/Dropbox for Business** - Click the Dropbox icon and select **Dropbox Folder**.
 - **Box** - Right-click the Box icon and select **Open Box Sync folder**.
 - **OneDrive** - Click the OneDrive icon and select **Open your OneDrive folder**.
- 3 In Windows Explorer, you can use the sync client to create folders and upload files.

NOTE: You can upload files using the browser. However, the best practice is to upload files through the sync client in Windows Explorer. For more information, see [Sync Folders](#).

Authenticate Dropbox for Business

If you install Dropbox for Business, Cloud Edition prompts for authentication.

- 1 After you install Cloud Edition, an Authentication window may open, or click the Cloud Edition icon and then select **Dropbox > Connect**.
The Authentication window notifies you that Cloud Edition must have access to your Dropbox account and may give instructions about business and personal accounts.
- 2 At the Authentication window, click **Next**.
- 3 If a Network Threat Protection window opens, click **Yes**.
- 4 In the Authentication window, enter your domain email and Dropbox password.
- 5 If you have linked your Dropbox business and personal accounts, you will be prompted to select one now. You must select your business account.
- 6 At the next window, click **Allow**.
- 7 Click **Finish** or wait for the window to close.

Sync Folders

Select the instructions for one sync client.

Dropbox for Business

To sync folders:

- 1 In the system tray, click the **Dropbox for Business** icon.
- 2 Click the **Settings** icon, and select **Preferences**.
- 3 Click the **Account** tab, then click **Selective Sync**.
- 4 Select only folders or subfolders that you will share.
- 5 Click **Update**.
- 6 On the Update confirmation dialog, click **OK**.
- 7 On the Dropbox Preferences window, click **OK**.
- 8 A pop-up displays in the system tray that folders are being synced.

Box

To sync folders:

- 1 In the system tray, right-click the Box icon and select **Open Box web site**.
- 2 In the cloud, right-click a folder and select **Sync Folder to Computer**.
- 3 In the Sync folder window, click **Sync Folder**.
- 4 The system tray icon indicates settings are being applied. This may take several minutes.
- 5 When complete, navigate to **Windows Explorer > Box Sync**. The synced folders display with a check mark.

OneDrive

To sync folders:

- 1 In the system tray, right-click the **OneDrive icon**, and click **Settings**.
- 2 Select the **Choose Folders** tab and then click **Choose Folders**.
- 3 Next, select **Choose folders to sync**.
- 4 A list of folders display. Select or clear check boxes to sync those folders. Click **OK**.
- 5 Click **OK**.
- 6 The system tray icon indicates settings are being applied. This may take several minutes.
- 7 When complete, navigate to **Windows Explorer > OneDrive**. The synced folders display with a check mark.

Work with Folders and Files

You can continue to use Dropbox, Box, or OneDrive to sync and continue working on files as you normally would. Depending on policy settings, when files are synced into the cloud, they are encrypted.

Cloud Storage Provider Help

Cloud Edition works transparently with your cloud sync client. Before using Cloud Edition, be sure to learn about the cloud storage provider:

- Dropbox support at <https://www.dropbox.com/help>
- Box support at <https://support.box.com/home>
- OneDrive support at <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>

Pre-existing Folders with Unencrypted Files

When you install DDP|CE and have pre-existing folders that are now being synced by a sync client, DDP|CE will not encrypt them.

Using Windows Explorer, one person within the group that shares that folder must move the files out of the sync client's folder to a temporary location outside of the sync client's folder. When the sync client folder indicates that it has completed syncing the changes, move the files back into the original folder.

or

For large content, request permission to have the Manage Folders option. Select that folder.

Access a Cloud Storage Provider

Dropbox

In the system tray, click the Dropbox icon and select **Dropbox.com**.

NOTE: If you use Chrome or Firefox to open Dropbox.com, be sure to close it after you finish working with files and folders. Even if you open another tab in the browser, the content will be encrypted. This could include email, an attachment, or uploads using the browser.

Box

In the system tray, right-click the Box icon and select **Open Box web site**.

OneDrive

In the system tray, right-click the OneDrive icon and select **Go to OneDrive.com**.

Dropbox for Business

Dropbox for Business has specific requirements. See [Cloud Sync Clients](#).

Connect Cloud Edition and Dropbox

If your company uses Dropbox for Business, you must allow Cloud Edition to stay connected. To connect:

- 1 In the system tray, click the Cloud Edition icon and then select **Dropbox > Connect**.
- 2 At the Dropbox Authentication window, read the information and then click **Next**.
- 3 If you have linked your Dropbox business and personal accounts, you will be prompted to select one now. You must select your business account.
- 4 At the prompt to allow Cloud Edition to access your Dropbox files and folders, click **Allow**.
- 5 Click **Finish**.

Use Dropbox for Business Context Menu

In Windows Explorer when Cloud Edition is installed, Dropbox for Business has an additional context menu.

NOTE: You must connect Cloud Edition to Dropbox.

To access the context menu, in Windows Explorer, open a Dropbox folder and right-click a file. The cloud icon has these options:

- Share Secure Dropbox link
- View on Dropbox.com
- View previous versions

Use Business and Personal Dropbox Accounts

If your company has Dropbox for Business and also allows you to link a personal Dropbox account with your business account, be sure to understand the policies set by your administrator for those accounts. For example, a company can set the following policies:

- Both business and personal files are encrypted.
or
- Only business files and folders are encrypted. Personal files remain unencrypted.
For security, your enterprise may have an auditing policy. File names in the personal folder are logged and sent to the Dell Data Protection Server.

If you use business and personal Dropbox accounts, do not store business files in your personal Dropbox folder.

Decrypting Folders in a Personal Account

If a personal folder is accidentally encrypted, navigate to the Cloud Edition system tray icon > **Manage Folders** and deselect folders that should be unencrypted. Also, you can remove folders from syncing by unlinking the account or unsyncing personal folders that should remain unencrypted.

Understand the Cloud Edition System Tray Menu Items

Details Screen

You can use the Details screen for troubleshooting or support issues. For example:

- If a user creates a folder but it's not encrypting, select **Details > Files > Folder State**.
- Check [Cloud Edition Policy Settings](#).
- View logs for troubleshooting.

The Details screen has a basic view and an enhanced view with additional details.

Basic Details Screen

Click the Cloud Edition system tray icon, and then click **Details...**

The upper-left corner of the Details screen displays the following information:

Service Status:	Status of the Cloud Edition Service. Values are: Stopped, Start Pending, Stop Pending, Running, Continue Pending, Pause Pending, Paused
Run State:	The device activation state. Values are: Active, Reactivating, Suspended, Suspending
User Mode:	Internal user - a user within this domain address External user - a user outside of this domain address
Registration Email:	For Internal users, this is the domain email address. For External users, this is the email they registered under.
Server URL:	DDP Server that communicates with this client.
Policy Last Modified:	Date and timestamp of when the policy was last modified and consumed by the client.
Policy Version:	Policy version generated by the DDP Server.

The **Files** and **Folders** areas of the Details screen display the following information:

Name:	Name of the file or folder
Key:	Key ID assigned to that folder (new files use that key for encryption)
Sync Client:	The last sync client to sync that folder (Dropbox, Box, or OneDrive)
FolderOwnership:	This value indicates who the folder is owned by. Value is determined by the Key ID.
FolderState:	The folder state is typically <i>Idle</i> unless a sync client is working on a folder, in which case it would be Enumerating.
Obfuscation Type:	A set on each folder indicating what type of .xen files will be created in the cloud. This is a policy set by your Administrator. If your Administrator selects <i>Extension only</i> , the actual filename with the “.xen” extension will be displayed. If your Administrator selects <i>Guid</i> , a scrambled filename with the “.xen” extension will display. This is a policy setting that takes effect on new folders only.

Enhanced Details Screen

While pressing <Ctrl> <Shift>, click the **Dell Data Protection | Cloud Edition** system tray icon, and then select **Details**.

In addition to Files and Folders, the following display:

Security:	Lists the key, key type, and state.
-----------	-------------------------------------

Audit: Lists modules, user ID, and event type. Information is in queue in this audit log and then sent to the server at specified intervals. The Administrator can use Compliance Reporter to create reports for auditing. See *Compliance Reporter Help*.

Policy: Lists the policy names and values for your enterprise.

To view log files, from the bottom-left corner of the Details screen, click **View Log**.

NOTE: Log files can be also be found at C:\ProgramData\Dell\Dell Data Protection\Cloud Edition.

If needed, Administrators can increase logging levels to aid in troubleshooting, as follows:

Create or modify the registry setting:

HKLM\SOFTWARE\Dell\Dell Data Protection\Cloud Edition\
LogVerbosity (DWORD value)=0x1f (31)

By default, the logging level is set to 0xf (15).

Available values:

Off = 0x0 (0)

Critical = 0x1 (1)

Error = 0x3 (3)

Warning = 0x7 (7)

Information = 0xf (15)

Debug = 0x1f (31)

Cloud Edition Policy Settings

To view the policy setting for your enterprise:

- 1 Press <Ctrl> <Shift>.
- 2 In the system tray, click the Cloud Edition icon and then select **Details**.
- 3 Click the **Policy** tab.
- 4 Look at the Value column for the *Cloud Storage Protection Enabled* policy.
 - **True** - the client encrypts and protects all files and folders.
 - **False** - the client encrypts and protects all files and folders in the business account, but the user can create a personal folder in which the contents are not encrypted. When set to False, the system displays a message each time the user logs in or reboots, reminding them not to add business files to a personal folder, since those files won't be protected.

Cloud Edition Manage Folders Menu

Based on policy, your Administrator grants access to this screen

This feature is allowed or denied by policy and enables the management of encryption on a folder-by-folder basis within the sync client folders. To access the Manage Folders screen, click the Cloud Edition system tray icon and select **Manage Folders**.

If this feature is not enabled by policy, Manage Folders does not display in the menu. Additionally, when the policy is enabled, the menu item does not display until the end user has created a folder, added files, and those files are encrypted up to the cloud.

A hierarchical view of cloud synchronized folders on the computer displays for each sync client. All folders are selected by default, although the end user can clear folders they do not want to encrypt.

Using Cloud Edition with iOS or Android

This section describes basic information on installing Cloud Edition on iOS or Android devices as well as a few tips.

When using Cloud Edition on an iOS or Android client, if you open files directly through Dropbox, Box, or OneDrive, the file names and file contents are encrypted and unreadable.

NOTE: Be aware that Windows has more options for sync clients than some other devices. For example, on some mobile devices, you can open and view Dropbox, Box, and OneDrive files, but you cannot upload a change.

Prerequisite

Before you install DDP|CE, you need the name of your enterprise's Dell Data Protection Server, such as server.domain.com.

Cloud Edition on an iOS device

Install on an iOS device

- 1 On your device, tap **App Store** and search for **Dell Data** or **Cloud Edition**.
- 2 Select and install the **Dell Data Protection | Cloud Edition** app.
- 3 For the Server field at the login screen, enter the name of your company's Dell Data Protection Server, such as server.domain.com.
- 4 Select a cloud storage provider: Dropbox, Box, or OneDrive.

Cloud Edition on an Android device

Install on an Android device

- 1 On your device, access **Google Play** and search for **DDP**.
- 2 Select and install the **DDP Cloud Edition** app.
- 3 For the Server field at the login screen, enter the name of your company's Dell Data Protection Server, such as server.domain.com.
- 4 Enter your user name and password and click **Login**.
- 5 Select a cloud storage provider: Dropbox, Box, or OneDrive.

Share Files With External Users

An external user is one with a non-domain email address. If an internal user wants to work on or share files protected by Cloud Edition with an external user, they must coordinate this with the Administrator.

Administrator Tasks

The enterprise determines the extent to which internal users can share business-sensitive files and folders with external users. For example:

- An internal user can send a request to any external user to register with and install Cloud Edition.
or
- Best practice: The enterprise blacklists any user not within the enterprise email domain. Internal users must first request that the Administrator add an external user to the whitelist.

The Administrator can control this through policies and the whitelist/blacklist. See [Allow/Deny Users on Whitelist/Blacklist](#).

External User Tasks

The external user must have Administrator rights on their computer in order to install Dell Data Protection | Cloud Edition (DDP|CE).

Register Cloud Edition

The external user must do the following:

- 1 When you receive a registration email, click the link.
- 2 At the Registration web page, enter your email address and password. Confirm your password, and click **Register**.
- 3 A confirmation email will be sent to you. Follow the link in the email.
- 4 Log in using the same email address and password you used to register.
Registration is complete. A Cloud Edition download page opens.

Download Cloud Edition

- 1 Select Windows or a device on which to install Cloud Edition.
- 2 When prompted for the server name, use the name at the top of the Download page.

Cloud Edition Frequently Asked Questions (FAQs)

Administrator FAQs

Question

I changed the *Obfuscate Filenames* cloud policy from GUID to **Extension only**. However, the folders I had previously been syncing are still encrypting those files to the other format with GUID filenames.

Answer

When a policy is changed on the DDP Server, DDP|CE maintains the previous policy for that folder. Any new folders created will have the new policy applied and will encrypt to the *Extension only* format.

Solution

To reapply the *Extension only* format to the old files, cut and paste them to a new folder that has the new policy applied.

Question

I installed and activated DDP|CE, but a new domain was stood up. I disjoined the old domain and joined it to the new domain. DDP|CE is still showing as active, but it is not getting any policy updates and no encryption occurs.

Answer

Currently, the DDP Server only recognizes the endpoint against which you originally activated. If you change the endpoint name, the DDP Server will not recognize that endpoint in order to send policy and DDP|CE will not perform as expected.

Solution

- 1 Uninstall DDP|CE and then reinstall.
- 2 Activate the same user again.

NOTE: Ensure that you stop syncing files to the local computer before you do this, or valuable data may become unprotected in the cloud or possibly deleted.

Question

Is there a reason that DDP|CE does not download unobfuscated files in a managed session?

Answer

DDP|CE transforms everything that the browser sees into .xen files. This includes the clear text downloads after the file has been created. You should encourage end users to protect **all** files in a managed cloud website.

Folder Management FAQs

NOTE: To use the Manage Folders option, you may need to request permission from your Administrator.

Question

I have a folder with files that I have shared with another user. In the system tray, I used the **Cloud Edition > Manage Folders** utility to unprotect that folder's contents. Recently, my files have become encrypted in the cloud again. That folder no longer displays in the Manage Folders utility, so I can no longer get those files to become unprotected in the cloud.

Answer

An encryption key ID is associated with a folder based on the first user who adds a file to that folder. If one user creates a folder and does not add any files, their key is not associated with that folder. The user whose encryption key ID has been set on the folder is the only one who can view the folder in the Manage Folders utility. If the user who sees the folder deselects the folder in the Manage Folders utility and they share that folder with another DDP|CE user, the second user's DDP|CE will re-encrypt the contents.

Solution

- 1 Create a new folder.
- 2 Move all the files to be protected to the new folder.
- 3 In the system tray, use the **Cloud Edition > Manage Folders** utility again to decrypt those files.

NOTE: If you unprotect the contents of a folder that are shared with other users who have DDP|CE, the other user's DDP|CE will enforce the policy to encrypt them. You can use the Manage Folders utility to unprotect files that are unshared with other DDP|CE users. The best practice is to unprotect only unshared folders.

Question

I am syncing to a decrypted folder that I had deselected using the Manage Folders utility. However, when I try to upload it through the web browser, I can only upload encrypted files.

Answer

DDP|CE is not designed to actively search for folders in the cloud. With unencrypted folders, DDP|CE can sync through the sync client because it is controlling that environment. Files going through the web browser are required to be protected.

Solution

Add files to the sync folder.

Question

I recently uninstalled my cloud-based file sharing system (Dropbox, Box, or OneDrive) from my computer, but when I opened the Manage Folders utility, Dropbox was still listed as an option.

Answer

DDP|CE does not monitor installation or uninstallation of third-party software. Those options are still listed because, by design, when these clients are uninstalled, they do not remove your existing files. Those files are still being protected by DDP|CE even though that sync client is no longer there.

Solution

To remove the old sync client option from the Manage Folders utility, delete the folder that houses those protected files. The best practice is to move any wanted folders/files out of the default Sync folder prior to deleting it. After you remove it, that file or folder is no longer listed in the Folder Management utility.

Dropbox FAQs

Question

My Dropbox account has many conflicted files. When I delete them from the cloud, they keep being created.

Answer

Sometimes, when a folder has already been shared and then multiple Cloud Edition accounts are activated at the same time, these files are seen as being created at the same time. In an effort to preserve the original, Dropbox will create multiple files of the same name and type and place them into the cloud. Therefore, Cloud Edition will allow all the files to be created without interfering.

Solution

- 1 Everyone who is sharing that file must collaborate on deselecting that folder for sync from the Dropbox application. See [Dropbox for Business](#).
- 2 After all the files and the folder have been removed from each local machine, one person must access the cloud and delete the duplicate files.

Then, each person can use the selective sync to re-add the folder to be synced.

Box Sync Client FAQs

Question

I am using the Box sync client. I created a new folder locally and added some files. The sync client appears to be working, but nothing has been created in the cloud.

Answer

The Box sync client may require some time to collect information about new folders and files. The process can take several minutes compared to other sync clients. Be sure to wait for several minutes for the sync client to complete before creating new folders and files.

Question

I am using the Box sync client. I ran out of room on my primary partition, so I moved it to another drive. Now, the My Box Files folder has one or more folders created and named **New Folder**.

Answer

Currently, when files are being synced between two machines to the same file share, if one person moves that folder to another location, then any new folders that other people create in that file share will create an empty folder named **New Folder**.

Solution

Delete the New Folder directly from the cloud. It will be removed from all systems that are sharing that folder.

Miscellaneous FAQs

Question

I moved the cloud provider's sync folder to Program Files, and now I cannot decrypt the files that are being downloaded to my sync folder from the cloud.

Answer

By design, the Program Files folder or other excluded folders are unprotected, based on policy. DDP|CE will not decrypt any files downloaded to this folder or its subfolders.

Solution

Unlink or uninstall the sync client and move the sync folder back to its default location or to an alternate managed location.

NOTE: For a list of managed and unmanaged locations, contact your Administrator.

Question

I had some archived .xen files, and I copied them to my desktop. Some of them decrypted, but others did not.

Answer

During a sync, DDP|CE is designed to decrypt directly to the Sync folder or decrypt when downloading through a web browser. For files that have been copied from another location, use Windows Explorer and move the .xen file into the sync client folder to be decrypted. In the system tray, click the **Cloud Edition** icon and then select **Details**. Locate the .xen file and its key to determine if that provides any information.

Solution

Move the .xen files into the Sync folder to have them uploaded into the cloud. Then, they will be decrypted locally.

Question

I renamed my computer. Now, I am not getting any policy updates, and I am not encrypting into the cloud.

Answer

Currently, the Server only recognizes the endpoint against which you originally activated. If you change the endpoint name, the Server will not recognize the location for sending the policy and DDP|CE will not perform as expected.

Solution

- 1 Uninstall DDP|CE and then reinstall. You must have Administrator rights to uninstall.
- 2 Activate the same user again.

NOTE: Ensure that you stop syncing files to the local computer before you do this, or you will run the risk of having valuable data become unprotected in the cloud or possibly deleted.

Question

On suspended Windows devices, when I try to upload files into the cloud, nothing happens. When I close the windows that were already opened, an error message states, Access Denied.

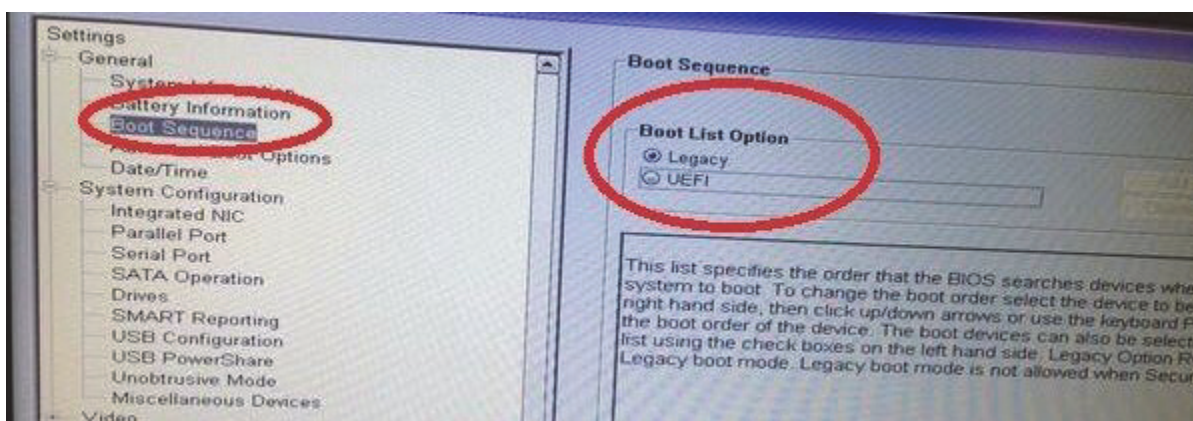
Answer

The error message is not from DDP|CE. You can access the files locally but will not get future updates to the files.

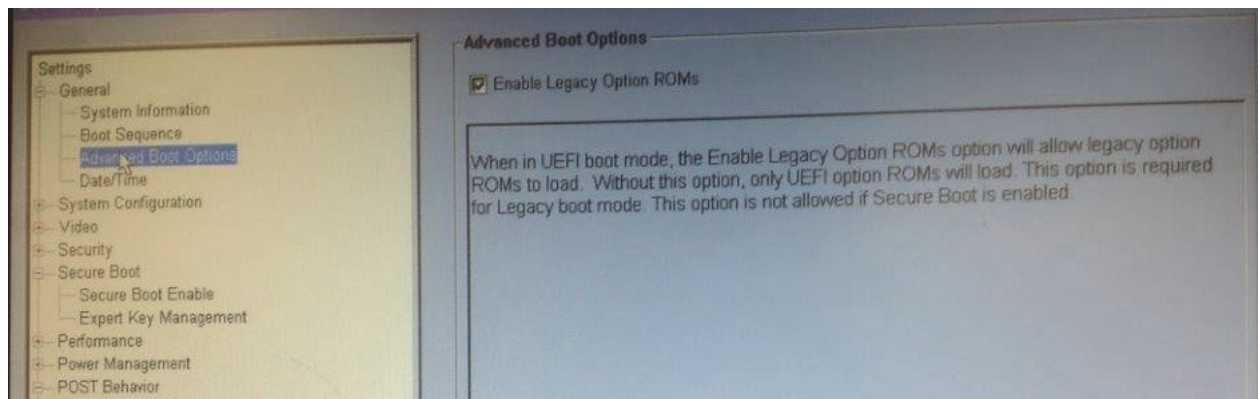
Change Secure Boot/UEFI to Legacy Boot Mode in BIOS

The features available as of v8.3 with HCA are supported on legacy BIOS non-UEFI systems. If running **Windows 8** or **Windows 8.1**, follow these instructions **prior** to client installation.

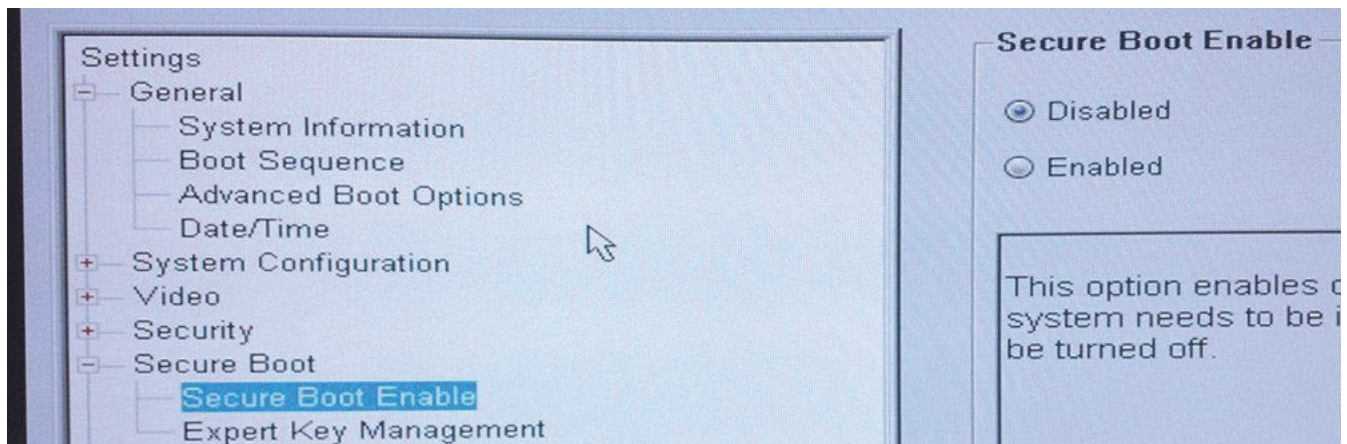
- 1 Turn on the power to your Dell computer. If the computer is already running, reboot it.
- 2 Press F2 or F12 continuously during boot until a message in the upper right screen says something similar to “preparing to enter setup” (F2) or “preparing one-time boot menu” (F12). This launches the system BIOS.
- 3 In **Settings > General > Boot Sequence**, ensure that the **Legacy** Boot List Option is selected.



- 4 In **Settings > General > Advanced Boot Options**, ensure that the **Enable Legacy Option ROMs** check box is selected.



- 5 In **Settings > Secure Boot > Secure Boot Enable**, ensure that the **Secure Boot Enable** selection is **Disabled**.



- 6 Apply the changes.
- 7 Now that the computer BIOS has been changed to a legacy boot mode, the computer must be re-imaged.

Glossary

Activate(d) - Activation occurs when the computer has been registered with the Server and has received at least an initial set of policies.

Active Directory (AD) - A directory service created by Microsoft for Windows domain networks.

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 files accessible to all managed users on the device where they were created.

Deactivate(d) - Deactivation occurs when SED management is turned to FALSE in the Server. Once the computer is deactivated, the PBA database is deleted and there is no longer any record of cached users.

External Users - Users outside the organization's domain address. Likewise, **Internal Users** are users inside the organization's domain address.

Hardware Crypto Accelerator (HCA) – HCA cards enable hardware-based encryption and provide advanced security. During setup, the HCA card is locked to the motherboard, and a unique key is created, encrypted, signed, and stored. Thereafter, access to your encrypted data is allowed only on that specific computer and only with the correct user authentication.

The newest release of DDP|E offers enhanced Preboot Authentication (PBA) for the Dell HCA. The enhanced PBA uses a separate preboot partition to provide encryption of the full windows volume and optional secondary partitions. Enhanced PBA provides features equivalent to PBA for self-encrypting drives, such as network authentication, multi-user support, and network unlock. When HCA policies are in play, System Data Encryption (SDE) policies are ignored.

Legacy Hardware Crypto Accelerator (HCA) – Computers equipped with legacy HCA use a BIOS password to emulate preboot authentication. The BIOS of most of these computers can be upgraded to take advantage of the newest HCA features used by DDP|E v8.3 and later. If the BIOS cannot be upgraded, DDP|E can be installed and run, but the computer will not have access to the newest features of HCA.

See Also Hardware Crypto Accelerator (HCA).

Preboot Authentication (PBA)– Preboot Authentication (PBA) 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.

Protected - For SED, a computer is protected once it has been activated and the PBA is deployed.

System Data Encryption (SDE) – SDE policies encrypt the System Drive, the Fixed Drives, or both - depending on the policy template chosen. 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 starts, the encrypted files are available before user login (to enable patch management, SMS, backup and recovery tools). SDE is designed to encrypt the operating system and program files. In order to accomplish this purpose, SDE must be able to open its key while the operating system is booting, without intervention of a password by the user. 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.

Trusted Platform Module (TPM) – TPM is a security chip with three major functions: secure storage, measurement, and attestation. DDP|E uses TPM for its secure storage function. The TPM can also provide encrypted containers for the DDP|E software vault and to protect the DDP|E HCA encryption key. Dell recommends provisioning the TPM. The TPM is required for use with DDP|E HCA.

User Encryption – The User key makes files accessible only to the user who created them, only on the device where they were created.



0XXXXXA0X

