## Contents

1 **Before You Begin** .......................................................... 5
   - **Pre-encryption Computer Setup** .................................. 5
   - **Computer Requirements** ............................................. 5
     - Windows Hardware .................................................. 5
     - Windows Software .................................................. 5
     - Windows Software Supported for External Media Shield ....... 6
     - Required Components ............................................. 6
   - **Interoperability** ................................................... 6
     - Dell ControlPoint Security Manager ................................ 6

2 **Introduction** .............................................................. 7

3 **Dell Data Protection Encryption Installation and Configurations Tasks** .... 9
   - **Install Dell Data Protection Encryption** .......................... 9
     - Interactive Installation .......................................... 9
     - Command Line Installation ...................................... 11
   - **Apply a Policy Template** ......................................... 13
   - **View Effective Policy** ............................................. 14

4 **Dell Data Protection Encryption Uninstallation and Decryption Tasks** .... 15
   - **Uninstall Dell Data Protection Encryption** ...................... 15
     - Interactive Uninstallation ....................................... 16
     - Command Line Uninstallation .................................... 17

5 **Data Recovery** ............................................................ 21

Appendix A **Configure Features Independently** ................................. 25
   - **Hide Overlay Icons** ............................................... 25
   - **Prevent Temporary File Deletion** ................................ 25
   - **Forced Poll** .......................................................... 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Options</td>
<td>26</td>
</tr>
<tr>
<td>Send Optimized Inventory to Server</td>
<td>26</td>
</tr>
<tr>
<td>Send Full Inventory to Server</td>
<td>26</td>
</tr>
<tr>
<td>Send Full Inventory for All Activated Users</td>
<td>26</td>
</tr>
<tr>
<td>Slotted Activation</td>
<td>26</td>
</tr>
<tr>
<td>Appendix B Retrieved a Recovery Bundle</td>
<td>29</td>
</tr>
<tr>
<td>Appendix C (Optional) Create an Encryption Removal Agent Log File</td>
<td>31</td>
</tr>
<tr>
<td>Appendix D Check Encryption Removal Agent Status</td>
<td>33</td>
</tr>
<tr>
<td>Appendix E Configure Key Server</td>
<td>35</td>
</tr>
<tr>
<td>Appendix F Use CMGAd</td>
<td>37</td>
</tr>
<tr>
<td>Use the Administrative Download Utility in Backup Mode</td>
<td>37</td>
</tr>
<tr>
<td>Use the Administrative Download Utility in Forensics Mode</td>
<td>37</td>
</tr>
<tr>
<td>Use the Administrative Download Utility in Admin Mode</td>
<td>38</td>
</tr>
<tr>
<td>Appendix G Use WSScan</td>
<td>39</td>
</tr>
</tbody>
</table>
Before You Begin

Pre-encryption Computer Setup
If the computer targeted for encryption comes equipped with an Encryption Accelerator, and you intend to use Full Volume Encryption (FVE) policies, you must first set up the Trusted Platform Module (TPM) and create a Pre-Boot Authentication (PBA) password. Follow the appropriate Dell hardware documentation to prepare the endpoint.

Computer Requirements
The user account performing the installation must be an Admin User (Local and/or Domain) which can be temporarily assigned by a deployment tool such as Microsoft SMS or Tivoli. A non-Admin User that has elevated privileges is not supported. To successfully install Dell Data Protection Encryption, the computer must have network connectivity to the Device Server and Policy Proxy.

Windows Hardware

<table>
<thead>
<tr>
<th>Windows Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Pentium-class or AMD processor</td>
</tr>
<tr>
<td>512 MB RAM</td>
</tr>
<tr>
<td>Approximately 110 MB of free disk space (55 +/- MB footprint)</td>
</tr>
</tbody>
</table>

Windows Software

<table>
<thead>
<tr>
<th>Windows Operating Systems (32- and 64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP SP3</td>
</tr>
<tr>
<td>• Professional Edition</td>
</tr>
<tr>
<td>Microsoft Windows Vista SP0 - SP2</td>
</tr>
<tr>
<td>• Enterprise Edition</td>
</tr>
<tr>
<td>• Ultimate Edition</td>
</tr>
<tr>
<td>• Business Edition</td>
</tr>
<tr>
<td>Microsoft Windows 7 SP0-SP1</td>
</tr>
<tr>
<td>• Enterprise</td>
</tr>
<tr>
<td>• Professional</td>
</tr>
<tr>
<td>• Ultimate</td>
</tr>
</tbody>
</table>
Windows Software Supported for External Media Shield

**NOTE:** To host an External Media Shield, removable storage must have approximately 17MB available, plus open space on the removable storage that is equal to the largest file to be encrypted.

### Operating Systems Supported to Access External Media Shield Protected Removable Storage (32- and 64-bit)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Editions</th>
</tr>
</thead>
</table>
| Microsoft Windows XP SP3                               | • Professional Edition  
• Home Edition  
• Media Center Edition |
| Microsoft Windows Vista SP0 - SP2                    | • Enterprise Edition  
• Ultimate Edition  
• Business Edition  
• Home Premium Edition |
| Microsoft Windows 7 SP0-SP1                            | • Enterprise  
• Professional  
• Ultimate  
• Home Premium |

**NOTE:** Microsoft Windows 7 disables autorun functionality to reduce the risk of malware. When EMS-encrypted removable media is inserted into a non-Shielded Windows 7 computer, users will not be automatically prompted by EMS to run EMS Explorer or install the EMS Service. To access encrypted files, users can either manually run AccessEncryptedFiles.exe or click the drive in Windows Explorer, and then choose to run EMS Explorer or install the EMS Service.

### Required Components

- Microsoft Visual C++ 2005 SP1 Redistributable Package (x86 and x64)
- Microsoft SQL Server Compact 3.5 SP1 (x86 and x64)

**NOTE:** The Dell Data Protection Encryption installer installs the components if not installed.

### Interoperability

**Dell ControlPoint Security Manager**

Although Dell ControlPoint Security Manager can be used with Dell Data Protection Encryption, a few settings must be changed prior to installing Dell Data Protection Encryption.

You cannot use Dell ControlPoint Security Manager to *Initialize and Lock the Drive*, if you also intend to encrypt the Windows Hibernation file (by setting your *Secure Windows Hibernation File* policy to *True*).

If this combination exists, once the computer attempts to come back from hibernation, it will not accept user name and password credentials, rendering the computer permanently inaccessible.

To safely use Dell ControlPoint Security Manager and the encryption policy *Secure Windows Hibernation File*, consult the Dell ControlPoint Security Manager documentation to set the Hard Drive Password using the BIOS Internal HDD Password.
Introduction

Dell Data Protection enables an enterprise to support a mobile workforce with the peace of mind that sensitive information is secure.

- **Shield** - encrypts all data and enforces access control
- **Policy Proxy** - distributes Shield policies
- **Enterprise Server and its components** - supports activations, provides centralized security policy administration, integrates with existing enterprise directories, and creates audit logs and reports

These components interoperate seamlessly to provide a secure mobile environment without detracting from the user experience.

Additional Information

The documentation set provides information about using and administering the Servers, Policy Proxy, Shield, and Manager. All documents are located in the Documentation folder in the installation media.

- The *Enterprise Server Installation and Migration Guide* provides the information needed to install/migrate the Server components.
- The *Administrator Help* provides the information needed to administer Dell Data Protection. The Administrator Help is accessible from the “?” icon in the Remote Management Console.
- The *Configuration Guide* provides the information needed to customize your environment.
- The *Release Notes* provide information about new features and changes in each major release, current supported platforms, resolved issues, key workarounds, and known issues, and any migration considerations.
- The *Dell Encrypt Help* provides information about using encryption in a remotely-managed environment. The Help is accessible from the Dell icon in the status area of the Windows taskbar.
- The *EMS Help* provides information about using EMS for Windows. The EMS Help is accessible from the “?” icon in the application.
- The *Server Configuration Tool Help* provides information about initializing or migrating your Servers, configuring certificates, and controlling Dell Services. The Server Configuration Tool Help is accessible from Start > Programs > Dell > Enterprise Edition > Server Configuration Tool > Server Configuration Tool Help.
- The *Compliance Reporter Help* provides information about using Compliance Reporter. The Help is located from the Help link in the Compliance Reporter interface.
- The *Admin Utilities Guide* provides information about using the admin utilities.
- The *Enterprise Edition for Windows Administrator Guide* provides the information needed to install and deploy Shields.
- The *Manager for BitLocker Administrator Guide* provides the information needed to install and deploy Manager for BitLocker.
Dell Data Protection Encryption Installation and Configurations Tasks

To install Dell Data Protection Encryption, you must be a Local or Domain Admin User.

This section guides you through the installation process, the process of applying a policy template, and how to view effective policies in the Remote Management Console.

You can install Dell Data Protection Encryption interactively, or using scripts/batch files/.msi/or any push technology available to your organization (such as Microsoft SMS, Tivoli, or Marimba), or through scripts using the command line (use this option to implement a silent installation).

We recommend upgrading when no encryption sweep is running. Performing an upgrade during an encryption sweep may prevent the Shield Service from restarting normally after the installation finishes. If this occurs, a computer restart corrects the issue.

It is important to note that some features of Dell Data Protection Encryption can be configured independently using registry settings. Some of these features must be applied prior to encryption to be effective. Before you begin installation, see Appendix A, Configure Features Independently on page 25 for the list of features and how to apply them.

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.

1. Back up any important data.
2. To reduce encryption time, run the Windows Disk Cleanup Wizard to remove temporary files and any other unnecessary data.
3. Turn off sleep mode to prevent an unattended computer from going to sleep. Encryption cannot occur on a sleeping computer.

Install Dell Data Protection Encryption

There are two methods to install/upgrade the Shield, select one of the following:

* Interactive Installation
  
* Command Line Installation

Interactive Installation

To begin installation, install Dell Data Protection Encryption from the setup.exe file included on the installation media.

**NOTE:** If UAC is enabled, pop-ups may display that ask you if you want to allow an action. In the case of Dell Data Protection Encryption, always select Yes. If you select No, Dell Data Protection Encryption will be prevented from installing, activating, modifying policies, or uninstalling the software by the operating system.

1. Locate setup.exe in the installation media. Copy it to the local computer.
Double-click setup.exe to launch the installer.

**NOTE:** The Dell Data Protection Encryption installer requires Microsoft Visual C++ 2005 SP1 (x86 and x64) and Microsoft SQL Server Compact 3.5 SP1 (x86 and x64). Click **Install** if prompted to install these components.

Click **Next** when the introductory screen displays.

Read the license agreement, agree to the terms, and click **Next**.

Click **Next** to install Dell Data Protection Encryption in the default location.

Select **Remotely Managed** on the Data Encryption Management Type screen. If you intend to only install External Media Edition, select the **External Media Edition only** checkbox. Click **Next**.

In the Dell Data Encryption Server Name field, enter the fully qualified host name of the Enterprise Server that will manage the target user, such as department.organization.com.

In the Managed Domain field, enter the domain managed by the Enterprise Server.

Click **Next**.

In the Dell Policy Proxy Host Name field, enter the fully qualified host name of the Policy Proxy that Dell Data Protection will communicate with. This field will be pre-populated with the same address used in step 7 above. If the Policy Proxy is installed in a non-default location, change this field as needed. If the Policy Proxy is installed on the local computer, ensure that **localhost** is entered in the Dell Policy Proxy Host Name field.

In the Dell Policy Proxy Port field, the default port is pre-populated. Only change the port number if the Policy Proxy is installed on a non-default port.

Click **Next**.

In the Dell Device Server URL field, enter the URL of the Device Server that Dell Data Protection will communicate with, such as https://department.organization.com:8081/xapi.

Click **Next**.

Click **Install** to begin the installation.

A status window displays the installation progress.

Click **Finish** when the Installation Complete screen displays.

Restart and reauthenticate to Windows.

Installation of Dell Data Protection Encryption is complete.
Command Line Installation
The installation is performed using the setup.exe file located in the installation media.

The following table details the command line options to select from.

Command Line Options

<table>
<thead>
<tr>
<th>Component</th>
<th>Log File</th>
<th>Command Line Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>/v* [fullpath]Install.log</td>
<td>SERVERHOSTNAME= &lt;ServerName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>POLICYPROXYHOSTNAME= &lt;RGKName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MANAGEDDOMAIN= &lt;MyDomain&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DEVICESEVERURL= &lt;ServerName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HIDESYSTRAYICON=1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GKPORT= &lt;NewGKPort&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MACHINEID= &lt;MachineName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RECOVERYID= &lt;RecoveryID&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REBOOT=ReallySuppress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HIDEOVERLAYICONS=1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EME=1</td>
</tr>
</tbody>
</table>

The following table details the switches available upon the install.

Command Line Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/v</td>
<td>Pass variables to the .msi inside the setup.exe</td>
</tr>
<tr>
<td>/a</td>
<td>Administrative installation</td>
</tr>
<tr>
<td>/s</td>
<td>Silent mode</td>
</tr>
</tbody>
</table>
The following table details the different display options available upon the install. These can be substituted at the end of the command line to achieve the expected behavior.

### Command Line Display Options

<table>
<thead>
<tr>
<th>Display Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/q</td>
<td>No Progress dialog, restarts itself after process completion</td>
</tr>
<tr>
<td>/qb</td>
<td>Progress dialog with Cancel button, prompts for restart</td>
</tr>
<tr>
<td>/qb-</td>
<td>Progress dialog with Cancel button, restarts itself after process completion</td>
</tr>
<tr>
<td>/qb!</td>
<td>Progress dialog without Cancel button, prompts for restart</td>
</tr>
<tr>
<td>/qn</td>
<td>Progress dialog without Cancel button, restarts itself after process completion</td>
</tr>
<tr>
<td>/qn!</td>
<td>No user interface</td>
</tr>
</tbody>
</table>

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

### Example Command Line Installation

Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks. The Device Server URL is case-sensitive.

- The following example installs the Shield with default parameters (Shield, Encrypt for Sharing, CREDActivate, no dialogue, no progress bar, automatic restart).
  
  ```
  ```

- The following example installs the Shield, Encrypt for Sharing, and CREDActivate, hides the Dell system tray icon, hides the overlay icons, no dialogue, no progress bar, suppresses restart.
  
  ```
  setup.exe /s /v"SERVERHOSTNAME=server.dell.com POLICYPROXYHOSTNAME=rgk.dell.com MANAGEDDOMAIN=DELL DEVICESERVERURL=https://server.dell.com:8081/xapi HIDESYSTRAYICON=1 HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

### Install EME

- The following example installs EME only (no dialogue, no progress bar, automatic restart).
  
  ```
  setup.exe /s /v"SERVERHOSTNAME=server.dell.com POLICYPROXYHOSTNAME=rgk.dell.com MANAGEDDOMAIN=DELL DEVICESERVERURL=https://server.dell.com:8081/xapi EME=1 /qn"
  ```

**NOTE:** Although the About box in the client displays software version number information, it does not display whether a full Shield is installed or EME only. To locate this information, go to C:\ProgramData\CREDANT\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 EME to an full Enterprise Shield

- Run a command line similar to the following:
  
  ```
  setup.exe /s /v"SERVERHOSTNAME=server.dell.com POLICYPROXYHOSTNAME=rgk.dell.com MANAGEDDOMAIN=DELL DEVICESERVERURL=https://server.dell.com:8081/xapi REINSTALL=ALL EME=0 REINSTALLMODE=vemus /qn"
  ```

  *A decrypt operation is not needed when converting EME to a full Enterprise Shield.*
Command Line Upgrade

When upgrading, replace the older setup.exe file with the newer setup.exe file, and re-run the batch file used for installation. If you customized any properties (such as HIDESYSTEMTRAY=1, etc.), use the same parameters that were originally used.

Create Custom Transform File

The setup.exe file provides the ability to create custom transform files. Customer Support is provided for issues relating to the use of the 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. Customer Support is not equipped to provide support for third-party tools and issues related to your environment. Once the transform file is created, issues related to troubleshooting or deployment should be handled by your in-house subject matter expert.

Do not run the extracted MSI. There is a high risk of installing components in the wrong order or missing an installation step. Run setup.exe for installation.

Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks. Follow the steps below to extract the necessary Shield files to create a custom transform file.

1. Enter the following command to create an administrative installation package.
   ```cmd
   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 Shield’s setup.exe installer.
   ```cmd
   setup.exe /v"PROPERTY1="value with spaces" PROPERTY2=ValueWithoutSpaces INSTALLDIR=D:\Program Files\Destination TRANSFORMS=NewTransform1.mst /qn"
   ```

Apply a Policy Template

**NOTE:** Network connectivity is required before encryption can begin, as the Shield must successfully escrow its encryption keys to the Server prior to encryption. For this to occur, network connectivity to the Device Server is needed. This process requires VPN connectivity if the required components are not deployed to a DMZ. You should consider deploying a Device Server to a DMZ if encryption will be enabled on computers outside of the organization and you do not want to rely on VPN connectivity.

You can apply a policy template at the Enterprise, Domain, Group, or User level to allow activations against the Server. The default configuration of Dell Data Protection Servers disables all activations and encryption policies at the Enterprise level to prevent overloading the Servers with activations after initial Shield deployment.

The Policy Administrator and Superadmin are the only roles which can work with Policy Templates.

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

2. In the left pane, click Protect & Manage > Enterprise (or Domains, Groups, or Users).
   
   For Enterprise, click Security Policies on the top menu. Highlight the policy template to apply, and click Save. Applying a policy template at the Enterprise level turns the Allow Activations policy from False to True for all Domains, Groups, Users, and Endpoints in the enterprise. The Enterprise level is the only level that disallows activations and encryption policies by default after Server installation.
   
   or

   For Domains, click the Policies icon for the appropriate Domain. Highlight the policy template to apply, and click Save. Policy templates at the Domain level allow activations and encryption policies for all Groups and Users in the specified Domain.
   
   or
For Groups, click the **Policies** icon for the appropriate Group. Highlight the policy template to apply, and click **Save**. Policy templates at the Group level allow activations and encryption policies for all Users in the specified Group.

*or*

For Users, click the **Policies** icon for the appropriate User. Highlight the policy template to apply, and click **Save**. Policy templates at the User level allow activations and encryption policies for the specified User.

3  When satisfied with how the Policy Template is applied, in the left pane, click **Actions > Commit Policies**.

4  Click **Commit Now**.

Your Policy Template is now applied as specified. The specified policies will now propagate from the Server to the Policy Proxy, and then to the Enterprise level, Domain level, Group level, or User level targeted for encryption.

To learn more about policy templates, see the Admin Help, **Manage Policies > Policy Template Editor** or **Manage Policies > Work with Policy Templates**.

**View Effective Policy**

Effective policies equal the policy template applied, plus any policy template overrides made. Effective policies are policies that are currently implemented policies for a specific endpoint.

1  As an 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 full Hostname of the device, enter it in the Hostname field (wildcarding is not supported). However, you may leave the field blank to display all Endpoints.

   Click **Search**.

   If you do not know the full Hostname, in the Endpoints area, scroll through the list available endpoints to locate the device.

   An endpoint or list of endpoints displays, based on your search filter.

6  To view the Endpoint Detail for the selected Endpoint, click the **Details** icon.

7  Click **Details & Actions** on the top menu.

8  In the Actions area, click **View Effective Policies**.
Dell Data Protection Encryption Uninstallation and Decryption Tasks

When using SDE, User, or Common encryption, file decryption optionally occurs at uninstallation if you choose to install the Encryption Removal Agent, enabling you to decide whether or not to decrypt files.

When using FVE encryption, all FVE-encrypted drives must be decrypted prior to uninstallation. The Encryption Removal Agent will not decrypt FVE encrypted drives. To decrypt FVE encrypted drives, publish the policy Full Volume Encryption (FVE) = False, and then initiate the uninstall process.

Best Practices

1. Back up all data.
2. To reduce decryption time, run the Windows Disk Cleanup Wizard to remove temporary files and any other unnecessary data.
3. Disable UAC. UAC may prevent uninstallation of Dell Data Protection Encryption.
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 setup.exe file. Use the same version to uninstall as was used to install.
7. Ensure that you have the correct version of WSScan. Use the same version as the setup.exe file.
8. Shut down all processes and applications to minimize decryption failures because of locked files.
9. Follow your existing process for decrypting data, such as issuing a policy update.
10. Before performing a restart, run WSScan to ensure that all data is decrypted. See Appendix G, Use WSScan on page 39 for instructions.
11. Disable all network connectivity, otherwise new policies may be acquired that would re-enable encryption.
12. Restart and re-authenticate to Windows.
13. Uninstall using the process in the following section.
14. Periodically check the Encryption Removal Agent Service (see Appendix D, Check Encryption Removal Agent Status on page 33 for information). If the Encryption Removal Agent Service exists, then data decryption is still in process.

Uninstall Dell Data Protection Encryption

There are two methods available to uninstall Dell Data Protection Encryption. Select either:

- Interactive Uninstallation
- Command Line Uninstallation
Interactive Uninstallation

Before you begin, ensure the following items are complete:

- The Encryption Removal Agent Service must be used by a domain member. See Windows Service Instructions on page 35 for instructions.
- When using the option Encryption Removal Agent - Download Keys from Server, Forensic Administrator credentials are required and the Key Server must first be configured. See Appendix E, Configure Key Server on page 35 for instructions.
- When using the option Encryption Removal Agent - Import Keys from a File, the CMGAd utility must be used prior to launching the Encryption Removal Agent, to obtain the encryption key bundle. See Appendix F, Use CMGAd on page 37 for instructions.
- See Appendix D, Check Encryption Removal Agent Status on page 33 for information on how to check decryption status following uninstallation.

1. Locate the original setup.exe file used to install Dell Data Protection Encryption. You must use the same setup.exe file to uninstall that was used to install.
2. Double-click setup.exe to launch the Encryption Removal Agent.
3. Read the Welcome screen and click Next.
4. At the Encryption Removal Agent Installation screen, select one of the following options:
   - Encryption Removal Agent - Download Keys from Server
     For SDE, User, or Common encryption, this option decrypts encrypted files and uninstalls Dell Data Protection Encryption.
     For FVE, this option uninstalls Dell Data Protection Encryption.

     Select this option to download the encryption keys from the Server. This option requires Forensic Administrator credentials and the Key Server must be configured prior to using this option. See Appendix E, Configure Key Server on page 35 for instructions on how to do both.
   1. At the Encryption Removal Agent Setup window, enter the following information (some fields may be pre-populated):
      - Fully qualified Device Server URL (for example, https:\test.dell.com:8081\xapi
      - Forensic Admin name (you must have Forensic Admin privileges set in the Remote Management Console)
      - Forensic Admin password
      - MCID (Machine ID)

     Click Next.
   2. Your encryption keys begin downloading. When the download is complete, click Next.
   3. At the Encryption Removal Agent Service Logon As window, select one of the following options:
      - Local System Account
• This Account
  This Account - Enter the Domain member name in the format of dell\jdoe
  Password - Enter the Domain member password
  Confirm password - Re-enter the Domain member password

  Click Finish.

  4 To complete the uninstall process, click Remove. Proceed to step 5.

• Encryption Removal Agent- Import Keys from a File
  For SDE, User, or Common encryption, this option decrypts encrypted files and uninstalls Dell Data Protection Encryption.

  For FVE, this option uninstalls Dell Data Protection Encryption.

  Select this option to import the encryption keys from a file. This option requires the use of CMGAd before uninstallation to obtain the encryption key bundle. Once CMGAd obtains the encryption key bundle, the file is then imported using this process. See Appendix F, Use CMGAd on page 37 for instructions.

  1 Browse to the location of the previously downloaded file.
  2 In the Passphrase: field, enter the passphrase associated with this file.
  3 Click Next.
     A message displays, indicating that key material is being downloaded.
  4 Once complete, click Finish.

  Proceed to step 5.

• Do not install Encryption Removal Agent
  Select this option to not decrypt files. All components of the Shield will be left on your computer to allow the encrypted files to remain accessible.

  1 To complete the uninstall process, click Remove. Proceed to step 5.

  5 Click Next.

  For SDE, User, or Common encryption, Dell Data Protection Encryption is uninstalled and decryption is in progress (if you chose to decrypt). See Appendix D, Check Encryption Removal Agent Status on page 33 for information on how to check decryption status.

  For FVE, Dell Data Protection is uninstalled.

Command Line Uninstallation

Before you begin, ensure the following items are complete:

• The Encryption Removal Agent Service must be used by a domain member. See Windows Service Instructions on page 35 for instructions.

• When using the option Encryption Removal Agent - Download Keys from Server, Forensic Administrator credentials are required and the Key Server must first be configured. See Appendix E, Configure Key Server on page 35 for instructions.

• When using the option Encryption Removal Agent- Import Keys from a File, the CMGAd utility must be used prior to launching the Encryption Removal Agent, to obtain the encryption key bundle. See Appendix F, Use CMGAd on page 37 for instructions.
• See Appendix C, (Optional) Create an Encryption Removal Agent Log File on page 31 for instructions on how to create an Encryption Removal Agent log file.
• See Appendix D, Check Encryption Removal Agent Status on page 33 for information on how to check decryption status following uninstallation.

## Command Line Parameters

<table>
<thead>
<tr>
<th>Command Line Parameters</th>
<th>Meaning</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMG_DECRYPT</td>
<td>Property for selecting the type of Encryption Removal Agent installation</td>
<td>1=Download keys from Server 2=Import keys from a file 0=Do not install Encryption Removal Agent</td>
</tr>
<tr>
<td>CMGSILENTMODE</td>
<td>Property for silent uninstallation</td>
<td>1=Silent 0=Not Silent</td>
</tr>
<tr>
<td>DA_SERVER &lt;Server Name&gt;</td>
<td>FQHN for the Server hosting the negotiate session.</td>
<td></td>
</tr>
<tr>
<td>DA_PORT=&lt;PortNumber&gt;</td>
<td>Port on the Server for request (default is 8050)</td>
<td></td>
</tr>
<tr>
<td>DA_KM_PATH=&lt;C:\keyfilename&gt;</td>
<td>The full path to the key file.</td>
<td></td>
</tr>
<tr>
<td>DA_KM_PW=&lt;keypassphrase&gt;</td>
<td>The password for the key file.</td>
<td></td>
</tr>
<tr>
<td>SVCPN=<a href="mailto:administrator@dell.com">administrator@dell.com</a></td>
<td>Username in UPN format that the Key Server Service is logged on as on the server.</td>
<td></td>
</tr>
<tr>
<td>DA_RUNAS=&lt;DELL\Administrator&gt;</td>
<td>Username in SAM compatible format under whose context the key fetch request will be made.</td>
<td></td>
</tr>
<tr>
<td>DA_RUNASPWD=&lt;password associated with DA_RUNAS name&gt;</td>
<td>Password for the runas user.</td>
<td></td>
</tr>
</tbody>
</table>

The following table details the switches available upon the uninstall.

### Command Line Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/v</td>
<td>Pass variables to the .msi inside the setup.exe</td>
</tr>
<tr>
<td>/a</td>
<td>Administrative uninstallation</td>
</tr>
<tr>
<td>/x</td>
<td>Uninstall mode</td>
</tr>
<tr>
<td>/s</td>
<td>Silent mode</td>
</tr>
</tbody>
</table>

The following table details the different display options available upon the uninstall. These can be substituted at the end of the command line to achieve the expected behavior.

### Command Line Display Options

<table>
<thead>
<tr>
<th>Display Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/q</td>
<td>No Progress dialog, restarts itself after process completion</td>
</tr>
</tbody>
</table>
Example Command Line Uninstallation

Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks. The DA_Server URL is case-sensitive.

- The following example imports keys from a file (CMGAd must be used before launching this command line).

  ```
  setup.exe /s /x /v"CMG_DECRYPT="2" CMGSILENTMODE="0" DA_SERVER="server.dell.com" DA_PORT="8050" SVCPN="administratorname@dell.com" DA_RUNAS="DELL\RunAsName" DA_RUNASPWD="RunAsPassword" DA_KM_PATH="C:\recoveryfilename" DA_KM_PW="KeyMaterialPassword" /qn"
  ```

- The following example downloads the keys from the Server.

  ```
  setup.exe /s /x /v"CMG_DECRYPT="1" CMGSILENTMODE="0" DA_SERVER="server.dell.com" DA_PORT="8050" SVCPN="administrator@dell.com" DA_RUNAS="DELL\RunAsName" DA_RUNASPWD="RunAsPassword" /qn"
  ```

Allow the Encryption Removal Agent to run and check its status as needed (Appendix D, Check Encryption Removal Agent Status on page 33 for information).

Uninstall EME

- Run a command line similar to the following:

  ```
  ```

Allow the Encryption Removal Agent to run and check its status as needed (Appendix D, Check Encryption Removal Agent Status on page 33 for information).

### Table: Display Option Meaning

<table>
<thead>
<tr>
<th>Display Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qb</td>
<td>Progress dialog with <strong>Cancel</strong> button, prompts for restart</td>
</tr>
<tr>
<td>/qb-</td>
<td>Progress dialog with <strong>Cancel</strong> button, restarts itself after process completion</td>
</tr>
<tr>
<td>/qb!</td>
<td>Progress dialog without <strong>Cancel</strong> button, prompts for restart</td>
</tr>
<tr>
<td>/qb!-</td>
<td>Progress dialog without <strong>Cancel</strong> button, restarts itself after process completion</td>
</tr>
<tr>
<td>/qn</td>
<td>No user interface</td>
</tr>
</tbody>
</table>

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

Display Option 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
Data Recovery

If you have not already retrieved the recovery bundle, see Appendix B, Retrieve a Recovery Bundle on page 29 for instructions.

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 Dell Data Protection Encryption.

The recovery program must be run with Administrative rights on the drive that it is recovering. In Windows XP, the user account that recovery program is run under must at least be a member of the Administrator Group. In Windows Vista and Windows 7, recovery program must be “Run as Administrator” to have access to perform the recovery operation.

There are two data recovery methods:

• Data Recovery using Current Computer - If the target computer is still bootable, data recovery can be accomplished in-place.
• Data Recovery using Slaved Drive or Pre-installed Environment - If the target computer is not bootable, data recovery must be accomplished on a slaved drive or a computer booted into a pre-installed environment.

Data Recovery using Current Computer

1. Locate the recovery program downloaded from the Remote Management Console.
2. Copy the recovery program to the target computer (the computer to recover data) and double-click the file to launch it.
3. A dialog displays asking 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 FVE encrypted drive.
   • I want to restore access to my FVE encrypted drive.
   Select the second option and click Next.
4. Click Next at the Backup\Recovery Information screen.
5. Select the volume to recover and click Next.

NOTE: If you have more than one volume to recover, repeat these steps for each volume.
6. Enter the recovery password associated with this file. This is the Recovery Password defined when the recovery program was retrieved from the Remote Management Console.
7. A dialog displays notifying you which volume is being recovered. Click Recover.
8. A dialog displays notifying you that recovery was completed successfully. Click Finish.
9. Restart the computer when prompted and re-authenticate to Windows.

Data recovery is complete and you may use your computer as usual.
Data Recovery using Slaved Drive or Pre-installed Environment

**NOTE:** See www.microsoft.com for Windows PE instructions.

1. Locate the recovery program downloaded from the Remote Management Console.
2. For **SDE recovery** (first option below), copy the recovery program to a slaved drive or a computer booted into a pre-installed environment.

   For **FVE decryption** (third option below), copy the recovery program to a computer booted into an 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 a Win PE environment, or by booting from another drive or helper partition that has another version of Windows installed (**but not FVE encrypted**). Note that this can be done on any computer running a compatible operating system, as long as the drive to be decrypted is attached and accessible.

   For **FVE recovery** (fourth option below), copy the recovery program to the computer to recover, and with an FVE encrypted drive attached, and while booted to the Dell Data Protection v7.2 Win PE environment. You **must** boot into this specific environment, as there are external environmental dependencies that are configured in this PE. If you do not have access to this specific environment, contact customer support for drivers and instructions. Note that FVE recovery outside of this environment will not work.

   Note that connectivity to the Device Server is required for FVE recovery. The Shield escrows the new Encryption Accelerator Critical Data back to the Device Server. The Server can either be specified in the command line or by creating the servletURL registry entry that the Shield uses. Also note that DNS may not work. If not, set the IP address of the Device Server instead of the FQDN.

   If the Encryption Accelerator is already owned, no escrow step is performed. If the Encryption Accelerator is unowned and the recovery has to own the Encryption Accelerator, it has to escrow the new Encryption Accelerator Critical Data. On reboot/login to Windows, the Shield knows that it needs updated encryption Accelerator Critical Data, and will communicate with the Server to download the new data and complete the recovery. It will attempt this on every login until it succeeds in obtaining the new critical data.

   Double-click the file to launch it.

3. A dialog displays asking 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 FVE encrypted drive.**
   - **I want to restore access to my FVE encrypted drive.**

   Select the **first, third or fourth** option as appropriate and click **Next**.

4. Click **Next** when the Backup/Recovery Information screen displays.

5. Select the volume to decrypt/recover and click **Next**.

   **NOTE:** If you have more than one volume to recover, repeat these steps for each volume.

6. Enter the recovery password. This is the Recovery Password defined when the recovery program was retrieved from the Remote Management Console.

7. A dialog displays notifying you which volume is being decrypted/recovered. Click **Recover**.

   **NOTE:** When restoring access to FVE encrypted files (performing recovery), several conditions could occur that require an action to be taken, as follows. Once the appropriate action is taken, restart the computer and re-initiate the recovery procedure.

   If you are swapping in a new Encryption Accelerator card, you will need to clear Encryption Accelerator ownership in order to establish new ownership. Since the new Encryption Accelerator card from the other computer was previously owned, recovery cannot succeed until the Encryption Accelerator owner is cleared in the BIOS.
No system password is set. Recovery 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.

An FVE key already exists in the BIOS. You will be notified that an FVE key was detected and instructed to clear the key in the BIOS.

The Encryption Accelerator is already owned. An attempt will be made to use the Encryption Accelerator Critical Data and password it has backed up, to establish and maintain the Encryption Accelerator ownership of an already owned Encryption Accelerator card. If that attempt fails, then the recovery operation fails. Go into the BIOS and clear the Encryption Accelerator ownership.

8 A dialog displays notifying you that recovery was completed successfully. Click Finish.

9 Restart the computer when prompted and re-authenticate to Windows.

10 Optional - For SDE recovery - To fully decrypt data, copy it from the slaved drive to a network location or other location that does not have encryption targeted.

OR

Optional - For SDE recovery - To fully decrypt data, copy it from the slaved drive to another local drive. All data is re-encrypted with encryption key of new computer.
Configure Features Independently

This section explains how to independently control Shield features. Some features in this section need to be applied prior to encryption to be effective.

Depending on the permission set of an Admin user, a change in permissions may be needed to create registry settings. If problems arise when attempting to create a new DWORD, follow the steps below to make the permissions change.

1. In the Windows registry, go to HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Right-click Notify > Permissions.
3. When the Permission for Notify window opens, select the checkbox for Full Control.
4. Click OK.

You may now create your new registry setting.

Hide Overlay Icons

By default, during installation, all encryption overlay icons are set to be shown. Use the following registry setting to hide the encryption overlay icons for all managed users on a computer after the original installation.

Create or modify the registry setting as follows:

HKLM\Software\CREDANT\CMGShield
HideOverlayIcons (DWORD value) = 1

If a user (with the appropriate privileges) chooses to show the encryption overlay icons, that setting will override this registry value.

Note that an installation command line parameter is available for use when the Shield is first installed. See Command Line Options on page 11.

Prevent Temporary File Deletion

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

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

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

HKLM\SOFTWARE\CREDANT\CMGShield
DeleteTempFiles (REG_DWORD) = 0
Forced Poll

Use the following registry setting to have the Shield poll the Server for a forced policy update.
Create or modify the registry setting as follows:
HKLM\SOFTWARE\Credant\CMGShield\Notify
PingProxy (DWORD value) = 1
Depending on Shield version, the registry setting will automatically disappear or change from 1 to 0 after the poll is complete.

Inventory Options

Use the following registry settings to either allow the Shield to send an optimized inventory to the Server, send a full inventory to the Server, or to send a full inventory for all activated users to the Server.

Send Optimized Inventory to Server
Create or modify the registry setting as follows:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield
OnlySendInvChanges (REG_DWORD) = 1
If no entry is present, optimized inventory is sent to the Server.

Send Full Inventory to Server
Create or modify the registry setting as follows:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield
OnlySendInvChanges (REG_DWORD) = 0
If no entry is present, optimized inventory is sent to the Server.

Send Full Inventory for All Activated Users
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield
RefreshInventory (REG_DWORD) = 1
This entry is deleted from the registry as soon as it is processed. The value is saved in the vault, so even if the computer is rebooted before the inventory upload takes place, the Shield still honors this request the next successful inventory upload. This entry supersedes the OnlySendInvChanges registry value.

Slotted Activation

Important: Configure Slotted Activation only with the assistance of Customer Support. Improper time slot configuration could result in large numbers of clients attempting to activate against a Device Server at once, creating potentially severe performance issues.
Slotted Activation is a feature that allows you to spread activations of clients over a set time period in order to ease Server load during a mass deployment. Activations are delayed based on algorithmically generated time slots to provide a smooth distribution of activation times.
For users requiring activation through VPN, a slotted activation configuration for the client may be required, to delay initial activation for long enough to allow time for the VPN client to establish a network connection.
The following registry keys are used to configure Slotted Activation. Changes to these registry keys require a restart of the computer for the updates to take effect.
• HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\SlottedActivation
  Enables or disables Slotted Activation
  Disabled=0 (default)
  Enabled=1

• HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat
  The time period in seconds that your activation slot interval occurs. Use this setting to override the time period in seconds that the activation slot interval occurs. 25200 seconds are available for slotted activations during a seven-hour period. The default setting is 86400 seconds, which represents a daily repeat.

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

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

• HKCU\Software\CREDANT\ActivationSlot (per-user data)
  Deferred time to attempt the slotted activation, which is set when the user logs onto the network for the first time after Slotted Activation is enabled. The activation slot is recalculated for each activation attempt.

• HKCU\Software\CREDANT\SlotAttemptCount (per-user data)
  Number of failed or missed attempts, when the time slot arrives and activation is attempted but fails. When this number reaches the value set in ACTIVATION_SLOT_MISSTHRESHOLD, the device attempts one immediate activation upon connecting to the network.

• To enable Slotted Activation through the command line, use a command similar to the following. Be sure to enclose a value that contains one or more special characters, such as a blank space, in escaped quotation marks.

  setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0,25200 <other parameters>"
Retrieve a Recovery Bundle

To access data on an encrypted disk (meaning, to perform data recovery), a recovery program containing the disk's encryption keys must first be retrieved from the Remote Management Console. There are two methods to retrieve encryption keys. Choose one of the following:

**Method 1**

1. As an 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 endpoint and click **Save**.
7. When prompted, save the file to a convenient and accessible location.

You may now use this recovery bundle to perform **Data Recovery**.

**Method 2**

1. As an 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 full Recovery ID or Host Name of the device, enter it in the appropriate field (wildcarding is not supported).
   - You can find the Host Name on the Endpoint Detail page in the Endpoint Detail section. It is listed as the Unique ID.
   - You can find the Recovery ID on the Endpoint Detail page in the Shield Detail section.
   - You may also leave the field blank to display all Endpoints.
6. Click **Search**.
   - If you do not know the full Hostname, in the Endpoints area, scroll through the list available endpoints to locate the device.
   - An endpoint or list of endpoints displays, based on your search filter.
7 Select the Details icon of the appropriate endpoint.
8 Under the Shield Detail section, click Actions: > Device Recovery Keys.
9 When prompted, create a Recovery Password for this endpoint and click Save.
10 When prompted, save the file to a convenient and accessible location.

You may now use this recovery bundle to perform Data Recovery.
(Optional) Create an Encryption Removal Agent Log File

Before beginning the uninstall process, you can optionally create an Encryption Removal Agent log file. This log file is useful for troubleshooting an uninstall/decryption operation. If you do not intend to decrypt files during the uninstall process, you do not need to create 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\CREDANT.
For Windows Vista and Windows 7, the log file path is C:\ProgramData\CREDANT.
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 computer is successfully uninstalled and 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 – Dell Data Protection Encryption is still installed, is still configured, or both. Decryption does not start until Dell Data Protection Encryption 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 Appendix C, (Optional) Create an Encryption Removal Agent Log File on page 31 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.
Configure Key Server

This section explains how to configure components for use with Kerberos Authentication/Authorization.

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

The Key Server then checks with the 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 Key Server component will need to be part of the affected domain.

### 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 Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the 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 will fail because the 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 Server restarts.
   
   If using “superadmin” in Step 3, and the superadmin password is not “changeit”, it must be changed here. Save your changes and close the file.
Sample Configuration File

```xml
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" />  <!-- Which TCP port the Server will listen to. Default is 8050, change if needed.]
        <add key="maxConnections" value="2000" />  <!-- how many active socket connections the Server will allow
        <add key="url" value="https://keyserver.domain.com:8081/xapi" />  <!-- your Device Server URL
        <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 Device Server. Note that this user must have the Forensic Administrator type selected in the Remote Management Console. The “superadmin” format can be any method that can authenticate to the Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the 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 will fail because the 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 (in seconds) it gets a new list. When a user connects, the Key Server needs to download authorized users from the 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 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 which 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 Forensic Admin. Click Update.
The components are now configured for Kerberos Authentication/Authorization.
Use CMGAd

This utility allows the download of a key material bundle for use on a computer that is not connected to a Server. The Admin Utilities can use this offline bundle.

This utility uses one of the following three methods to download a key material bundle, depending on the command line parameter passed to the application:

- **Backup Mode** - Used if `-b` is passed on the command line. Extracts a key material bundle from an LSARecovery_[hostname].exe file.
- **Forensics Mode** - Used if `-f` is passed on the command line. This is the default mode when no command line parameter is used.
- **Admin Mode** - Used if `-a` is passed on the command line.

Log files can be located at:
- Windows XP - `C:\Documents and Settings\All Users\Application Data\CmgAdmin.log`
- Windows Vista and Windows 7 - `C:\ProgramData\CmgAdmin.log`

Use the Administrative Download Utility in Backup Mode

1. In the location where the Administrative Download Utility is located, open a command prompt.
2. Enter `cmgad.exe -b`.
3. When the utility launches, browse to the location of LSARecovery_[hostname].exe file. When prompted, enter the password associated with this file.

Use the Administrative Download Utility in Forensics Mode

1. Double-click `cmgad.exe` to start the utility.
2. Enter the following information (some fields may be pre-populated).
   - **Device Server URL**: Fully Qualified Device Server URL, such as `https://deviceserver.dell.com:8081/xapi`
   - **Dell Admin**: Name of the Administrator with Forensic Admin credentials (enabled in the Remote Management Console), such as jdoe
   - **Password**: Forensic Admin password
   - **MCID**: Machine ID, such as `machineID.dell.com`
   - **DCID**: First eight digits of the 16-digit Shield ID
3. Click **Next**.
   A message displays, indicating that the key material was successfully unlocked. Files are now accessible.
4. Once complete, click **Finish**.
Use the Administrative Download Utility in Admin Mode

1 In the location where the Administrative Download Utility is located, open a command prompt.
2 Enter `cmgad.exe -a`.
3 Enter the following information (some fields may be pre-populated).
   - **Server**: Fully Qualified Hostname of the Key Server, such as keyserver.dell.com
   - **Port Number**: The default port is 8050
   - **Server Account**: The domain user the Key Server is running as. The format is domain\username. The domain user running the utility must be authorized to perform the download from the Key Server
   - **MCID**: Machine ID, such as machineID.dell.com
   - **DCID**: First eight digits of the 16-digit Shield ID

   Click **Next**.
   A message displays, indicating that the key material was successfully unlocked. Files are now accessible.
4 Once complete, click **Finish**.
Use WSScan

When uninstalling Dell Data Protection Encryption, 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 installation media, copy WSScan.exe to the desktop (or another location) of the Windows device to scan.
2. Launch a command line at the location above.
3. At the command prompt, enter `wsscan.exe -i`.
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

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