Dell Data Protection | Encryption

Enterprise Edition for Windows Administrator Guide

June 2013

Contents

1

Introduction

Dell Data Protection | Encryption (DDP|E) offers non-disruptive endpoint encryption solutions that help you quickly and easily deploy encryption across your entire organization, enforce policies, and audit encryption state. DDP|E is designed to protect data wherever it goes, including mobile devices, tablets, PCs, public cloud storage, external media, self-encrypting drives and Microsoft® BitLocker™ — enabling your employees to work the way they want, on the devices they want.

As a general rule, we recommend that you install the Dell Enterprise Server first, followed by deployment of the appropriate client to end users. If you have not yet installed the Dell Enterprise Server, locate the *Enterprise Server Installation and Migration Guide*, follow the instructions, then return to this guide for instructions to deploy DDP | Encryption Enterprise Edition for Windows.

All guides are located in the DDP|E installation media and www.dell.com/support > Endpoint Security Solutions.

Continue to Requirements.

2

Requirements

- The user account performing the installation must be an 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 create a Preboot Authentication (PBA) password. Follow the instructions detailed in Pre-Installation Configuration to Enable Hardware Crypto Accelerator prior to DDP|E installation.

Client Prerequisites

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

Prerequisites
• Microsoft Visual C++ 2008 SP1 Redistributable Package (x86 and x64)
• Microsoft SQL Server Compact 3.5 SP2 (x86 and x64)
• .NET Framework Version 4.0

Windows Hardware

The following table details supported hardware.

Windows Hardware
• Intel Pentium-class or AMD processor
• 512 MB-1GB RAM
• +-110 MB of free disk space
Optional Embedded Hardware
• Dell Data Protection | Hardware Crypto Accelerator

NOTE: The legacy Dell Data Protection | Hardware Crypto Accelerator is supported on Windows 7 only, on Dell X4 computers, model numbers:

Latitude 6430u	Latitude E5430	Optiplex 9010, 7010	Precision M4700 and M6700
Precision T1650	Precision T3600	Precision T5600	Precision T7600

• Trusted Platform Module (TPM) chipset

Windows Software

The following table details supported software.

NOTE: DDP|E 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.
Windows XP Mode is not compatible with DDP|E. DDP|E is designed to run Windows 7 and later natively.

Windows Operating Systems (32- and 64-bit)
• Microsoft Windows XP SP3 - Professional Edition
• Microsoft Windows Vista SP0 - SP2 - Enterprise Edition - Ultimate Edition - Business Edition
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional - Ultimate
• Microsoft Windows 8 - Enterprise - Pro
• VMWare Workstation 5.5 and higher
• Windows Embedded Standard 7 in Application Compatibility Mode

Windows Software Supported 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 20MB 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
• Microsoft Windows Vista SP0 - SP2 - Enterprise Edition - Ultimate Edition - Business Edition - Home Premium Edition

Operating Systems Supported to Access EMS-Protected Media (32- and 64-bit)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional - Ultimate - Home Premium
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer)

Language Support

DDP|E 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

Interoperability

Dell Data Protection | Access

Before installing DDP|E or DDP|ST, you must perform the following steps:

1. Go to Dell Data Protection | Access > Advanced > perform a *Reset System*.
2. Uninstall the Dell Data Protection | Access software.
3. Restart the computer.

The *Reset System* guarantees that:

- The USH firmware can be upgraded
- The USH is cleared to a new state
- BIOS PBA is deactivated
- TPM ownership is cleared
- All enrollments are cleared
- The DDPA cred provider is removed

Proceed to Pre-Installation Configuration to Enable Hardware Crypto Accelerator **or** if your computer does not come equipped with a Hardware Crypto Accelerator, proceed to Installation and Configurations Tasks.

3

Pre-Installation Configuration to Enable Hardware Crypto Accelerator

If the computer targeted for encryption is equipped with a Hardware Crypto Accelerator (HCA) and you intend to use Hardware Crypto Accelerator (HCA) policies, you must first set up the TPM and create a PBA password. Follow the instructions detailed in this section to configure HCA **prior** to DDP|E installation.

HCA Pre-Installation BIOS Configuration

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

1. Boot into the BIOS Configuration:
   - Press F2 or F12 continuously during boot until message in upper right screen says something 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 BIOS password has not yet been configured.

2. Define BIOS Administrator Password if not already configured:
   - Under **Settings**, click the + (plus) sign next to **Security**, and then click **Admin Password**. This step must be completed before you can create a preboot/system password.
   - Enter your new Admin password information and click **Apply**.
3. Define 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 **Step 4 and 5**, understand that you should **never** clear TPM or HCA ownership after HCA policies have been implemented. If you ignore the BIOS warning and clear the TPM or HCA after HCA 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 radio button for **Clear** and click **Apply**.
   - Select the radio button for **Activate** 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 will not clear, select **Load Default** and then **Exit**.

6 Enter Preboot (System) Password:
   — After exiting the BIOS configuration you will be prompted for the preboot (system) password defined in Step 3.
   — 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 PBA Password

If you forget your PBA password, log in with the BIOS Admin password and assign a new PBA password as described in 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).

Proceed to Installation and Configurations Tasks.

4

Installation and Configurations Tasks

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

You can install DDP|E along with several other clients using the master installer, or alone by extracting the child installer out of the master installer. Either way, DDP|E can be installed by command line or scripts, and using any push technology available to your organization.

About Backups

When performing backups, it is important to note if the backup is being performed offline or online. In offline mode, all files backed up will be in an encrypted state. In online mode, any User-encrypted files will be blocked unless the user is logged in at the time of backup. SDE-encrypted files are accessible in online backup mode.

It is also worth noting that backups are either done in block mode or file mode. It is recommended that you use the same mode for restore that you did for the backup. The block mode backup can operate while the CEF driver is active and operates underneath it in the same way as a disk defrag. This copies all the files in their encrypted state and the CredDB.CEF file. **It is strongly recommended that you perform a block mode restore while offline to prevent corruption. The file mode requires access to the** encryption keys **and backs up the files in clear text.**

While Dell does not endorse any specific backup solution, many offline and online solutions have been tested.

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.
4. In environments where systems are installed with images, it is **strongly recommended** to install DDP|E after image installation. If it is necessary to incorporate DDP|E in an image, it should be done in an unencrypted state. Should you have questions or concerns, contact support.
5. When upgrading, we recommend 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.

Prerequisites

- You must have a local or domain Admin user account to perform the installation.
- Network connectivity is required.

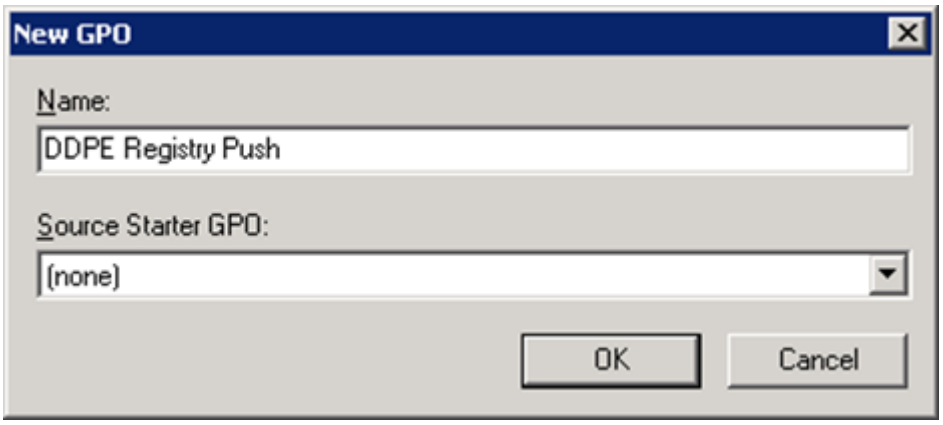
Set GPO on Enterprise Server to Enable Entitlements

- Before beginning the installation process for DDP|E, set the GPO on the Enterprise Server to enable entitlements.
- The workstation must be a member of the OU where the GPO is applied.

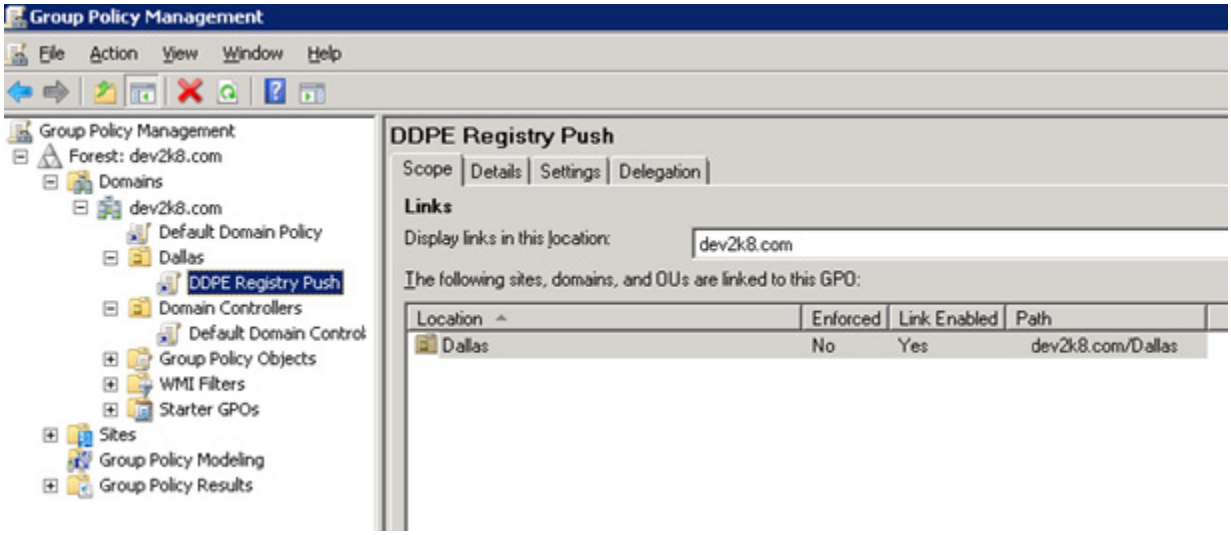
1 On the Enterprise Server to manage DDP|E, click **Start > Administrative Tools > Group Policy Management**.

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

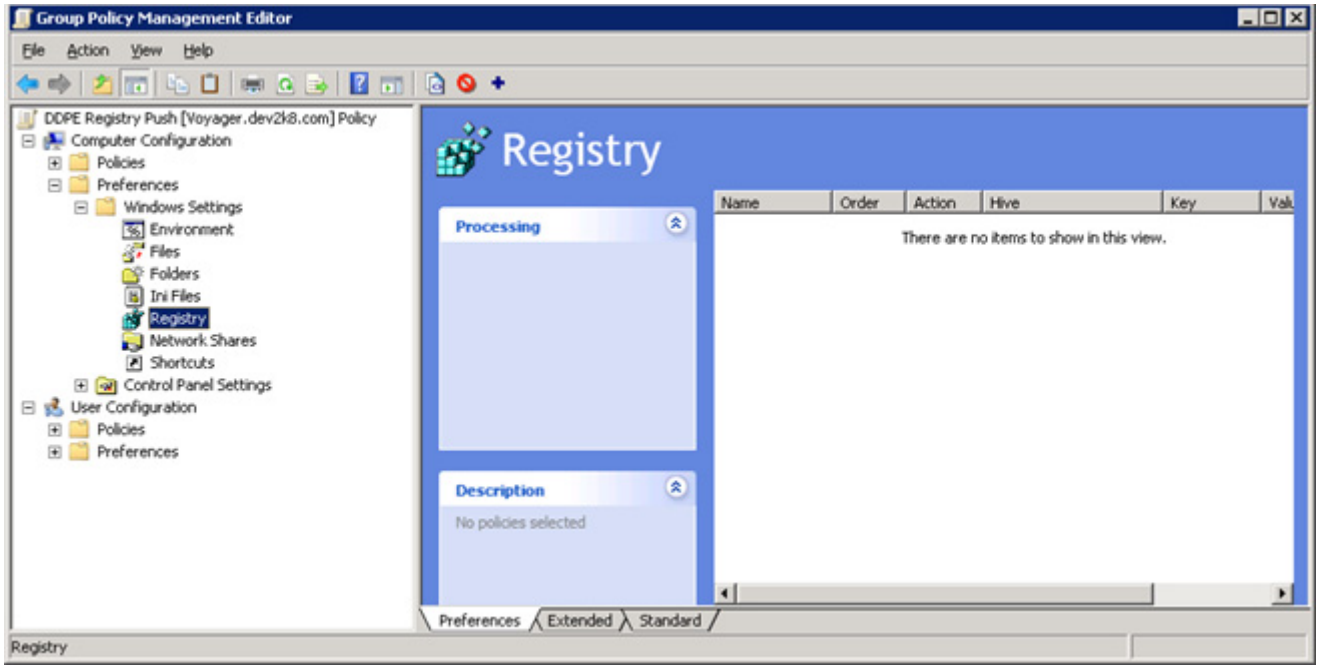
3 Enter a name for the new GPO, select (none) for Source Starter GPO, and click **OK**.



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



5 The Group Policy Management Editor loads. Drill into **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

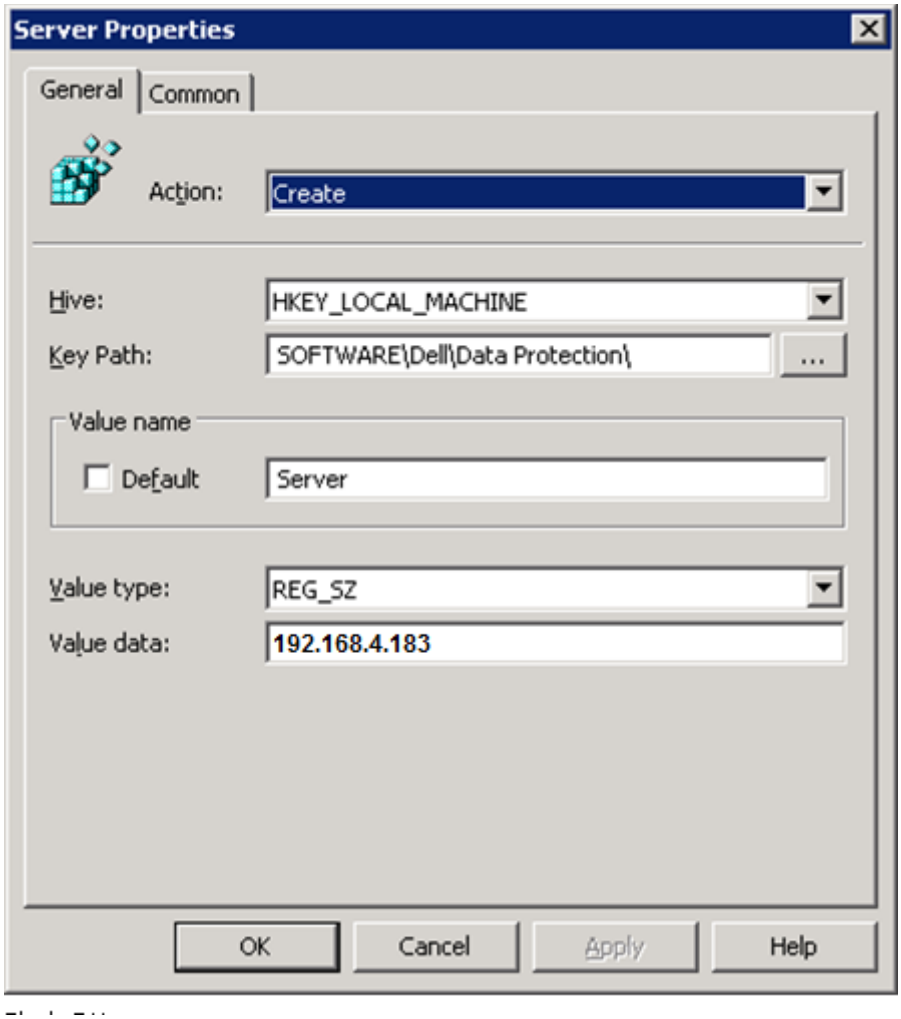
Key Path: SOFTWARE\Dell\Dell Protection

Value name: Server

Value type: REG_SZ

Value data: <IP address of Enterprise Server>

Click **OK**.



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

Install DDP|E

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

- Install DDP|E Using the Master Installer
- Install DDP|E Individually Using the Child Installer

Install DDP|E Using the Master Installer

Command Line Installation

- The master installer does not support upgrades from pre-v8.0 components. For upgrade needs, extract the child installer from the master installer. See Install DDP|E Individually Using the Child Installer for extraction instructions.
- If your Dell Device Server uses a port other than 8443 or 8081, install using the user interface instead of the command line installation so that you can change the port number.

Example Command Line Installation

The installation is performed using the **setup.exe** file located in the DDP|E installation media.

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

Supported features:

CE = Cloud Edition

PE = Personal Edition (locally managed - DDP|E, SED, Authentication). Requires PE Entitlement.

DE = Drive Encryption (DDP|E remotely managed)

EME = Drive Encryption - External Media Edition Only (DDP|E EME remotely managed)

BLM = BitLocker Manager

SED = Self-Encrypting Drive management - remotely managed

- The following example installs with Entitlement server setting. Assumes Entitlement in registry:
  `setup.exe /z"\"SERVER=qatest.organization.com\""`
- The following example installs with manually specifying Entitlement. Assumes no Entitlement in registry. Installs DDP|E, BitLocker Manager and Cloud Edition remotely managed.
  `setup.exe /z"\"FEATURES=DE-BLM-CE\""`
- The following example installs DDP|E, SED, Authentication locally managed Requires PE Entitlement.:
  `setup.exe /z"\"FEATURES=PE\""`
- The following example installs DDP|E, Authentication, SED remotely managed:
  `setup.exe /z"\"SERVER=qatest.organization.com\""`
- The following example installs with updated installation directory:
  `setup.exe /z"\"InstallPath=C:\<newpath>\""`
- The following example is a silent install example. Assumes Entitlement in registry:
  `setup.exe /S /z"\"InstallPath=C:\<newpath>, SERVER=qatest.organization.com\""`
- The following example extracts all installers:
  `setup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""`
- The following example suppresses reboot:
  `setup.exe /S /z"\"SUPPRESSREBOOT=1\""`
- The following example installs BitLocker Manager and SED remotely managed.
  `setup.exe /z"\"FEATURES=SED-BLM\""`

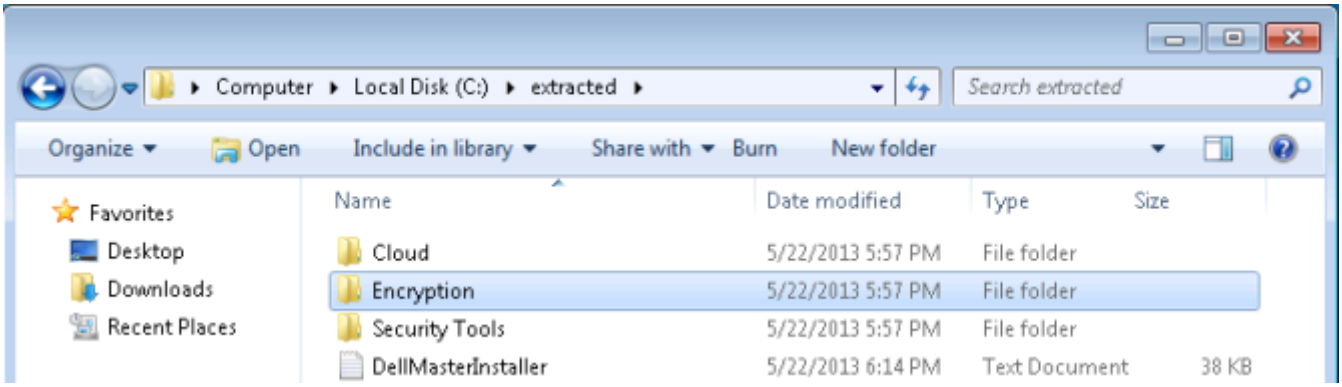
Install DDP|E Individually Using the Child Installer

To install DDP|E individually, without the other clients that are included in the master installer, the child executable file must first be extracted from the master installer.

1. From the DDP|E installation media, copy the master installer's setup.exe file to the local computer.
2. Open a command prompt in the same location as the setup.exe file and enter:

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

3. The extracted child installer is located at C:\extracted\Encryption. Use **DDPE_*XX*bit_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 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	/lv* [fullpath]Install.log **NOTE:** /lv* should be inside /v", such as **DDPE_XXbit_setup.exe /v"/lv*c:\Logfile.log"**.	SERVERHOSTNAME=<ServerName>
		POLICYPROXYHOSTNAME=<RGKName>
		MANAGEDDOMAIN=<MyDomain>
		DEVICESERVERURL=<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.

Display 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_*XX*bit_setup.exe file located in the extracted installers folder.

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

  If your Dell Enterprise Server is pre-v7.7:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8081/xapi /qn"
  ```

  If your Dell Enterprise Server is v7.7 or later:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /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.

  If your Dell Enterprise Server is pre-v7.7:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8081/xapi HIDESYSTRAYICON=1
  HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

  If your Dell Enterprise Server is v7.7 or later:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
  HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

Install Dell Data Protection | External Media Edition (EME)

- The following example installs EME only (no dialogue, no progress bar, automatic restart).

  If your Dell Enterprise Server is pre-v7.7:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8081/xapi EME=1 /qn"
  ```

  If your Dell Enterprise Server is v7.7 or later:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /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\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 Dell Data Protection | External Media Edition to Dell Data Protection | Enterprise Edition

- Run a command line similar to the following:

  If your Dell Enterprise Server is pre-v7.7:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8081/xapi REINSTALL=ALL EME=0
  REINSTALLMODE=vemus /qn"
  ```

  If your Dell Enterprise Server is v7.7 or later:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
  REINSTALLMODE=vemus /qn"
  ```

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. Customer 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. 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 DDPE_XXbit_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 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_64bit_setup.exe /v"PROPERTY1=\"value with spaces\" PROPERTY2=
   ValueWithoutSpaces INSTALLDIR=D:\Program Files\Destination TRANSFORMS=
   NewTransform1.mst /qn"
   ```

   Continue to Apply Policies.

Apply Policies

NOTE: Network connectivity is required before encryption can begin, as the client must successfully escrow its encryption keys to the Dell Enterprise Server prior to encryption.

You can apply a policy template at the Enterprise level to allow activations against the Dell Enterprise Server. The default configuration of the Dell Enterprise Server disables all activations and encryption policies at the Enterprise level to prevent overloading the Dell Enterprise Server with activations after initial the client deployment.

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

1. As a Dell Administrator, log in to the Remote Management Console.
2. In the left pane, click **Protect & Manage > Enterprise** (or Domains, User Groups, Users, Endpoint Groups, or Endpoints).

NOTE: If an endpoint computer comes equipped with an HCA and you choose to enable HCA policies, all SDE policies are ignored. Likewise, if you enable SDE policies and later decide to enable HCA policies, SDE issues a decryption policy before HCA policies are implemented. HCA and SDE cannot coexist on the same computer.

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, User Groups, Users, endpoint Groups, and Endpoints in the enterprise. The Enterprise level is the only level that disallows activations and encryption policies by default after Dell Enterprise Server installation.

or

For Enterprise, click **Security Policies** on the top menu. Click **Override** on the far right. Change policies as desired. Click **Save** when satisfied with the changes.

or

For Domains, click the **Policies** icon for the appropriate Domain. Change policies as desired. Click **Save** when satisfied with the changes.

or

For User Groups, click the **Policies** icon for the appropriate User Group. Change policies as desired. Click **Save** when satisfied with the changes.

or

For Users, If you know the User name, or part of the User name (use the wild card character * to display partial matches), enter it in the *User Name*: field. Click *Search*. (You can leave all the fields at the default value and click Search to display all Users in the enterprise). Click the **Policies** icon for the appropriate User. Change policies as desired. Click **Save** when satisfied with the changes.

or

For Endpoint Groups, click the **Policies** icon for the appropriate Endpoint Group. Change policies as desired. Click **Save** when satisfied with the changes.

or

For Endpoints, search for a specific endpoint computer or click **Search** to display all endpoint computers in the enterprise. From the Device Type: drop-down, select *Workstation*. From the Show: drop-down, select *All*, *Visible*, or *Hidden*. Disregard the Recovery ID: field. If you know the hostname, or part of the hostname (use the wild card character * to display partial matches), enter it in the *Hostname*: field. Click *Search*. (You can leave all the fields at the default value and click Search to display all endpoints in the enterprise). Once the appropriate endpoint computer is located, click the **Details** icon for the endpoint computer.

3. When satisfied with how policies are applied, in the left pane, click **Actions > Commit Policies**. Click **Apply Changes.**

The policies will now propagate from the Dell Enterprise Server to the Dell Policy Proxy, and then to the levels targeted for encryption.

View Effective Policy

Effective polices are policies that are currently implemented policies for a specific endpoint.

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 full Hostname of the device, enter it in the Hostname field (wildcarding is supported). 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**.

Continue to Uninstallation and Decryption Tasks.

5

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, enabling 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 **will not decrypt HCA encrypted drives**. To decrypt HCA encrypted drives, publish the policy Hardware Crypto Accelerator (HCA) = False, 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 any other unnecessary data.
3. Disable UAC. UAC may prevent uninstallation of DDP|E.
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. Restart and re-authenticate to Windows.
12. Uninstall using the process in the following section.
13. **IMPORTANT** - Periodically check the Encryption Removal Agent Service (see Check Encryption Removal Agent Status for information). If the Encryption Removal Agent Service exists, then data decryption is still in process.

Prerequisites

- Optionally create an Encryption Removal Agent log file to aid in troubleshooting, should the need arise. 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.

Uninstall DDP|E

1. **If you installed using the master installer**, extract the child installers by running the extract command:

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

2. Go to C:\extracted\ to obtain each client installed on the computer.
3. Uninstall the clients in this order:

   DDP|E

   Client Security Framework

   DDP|Authentication

   If the following applications are installed, they can be uninstalled independently without uninstalling the clients listed above: DDP|Cloud Edition
4. Once all clients are uninstalled, run the master installer's setup.exe to uninstall the master installer.

Command Line Uninstallation

- 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.

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 DDPE_*XX*bit_setup.exe
/a	Administrative uninstallation
/x	Uninstall mode
/s	Silent mode

Parameters

The following table details the parameters available for the uninstallation.

Parameters	
Required	CMG_DECRYPT - Property for selecting the type of Encryption Removal Agent installation 1 - Download keys from Dell Enterprise Server 0 - Do not install Encryption Removal Agent
	CMGSILENTMODE - Property for silent uninstallation. 1 - Silent 0 - Not Silent
Required	DA_SERVER - FQHN for the Dell Key Server hosting the negotiate session
Required	DA_PORT - Port on the Dell Key Server for request (default is 8050)

Parameters	
Required	SVCPN - User name in UPN format that the Dell Key Server service is logged on as on the Dell Enterprise Server **NOTE:** Ensure that a domain account is configured for the "Log On As" in the Dell Key Server service.
Required	DA_RUNAS - User name in SAM Compatible format under whose context the key fetch request will be made. **NOTE:** Ensure that the DA_RUNAS user is in the Key Server list in the Dell Remote Management Console.
Required	DA_RUNASPWD - Password for the RunAs user
	SVCLOGONUN - User name in UPN format for Encryption Removal Agent service Log On As parameter
	SVCLOGONPWD - Password for Log On As user

Display Options

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

Display 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

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 downloads the keys from the Dell Enterprise Server.

  ```
  DDPE_64bit_setup.exe /s /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
  \"server.organization.com\" DA_PORT=\"8050\" SVCPN=
  \"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).

Uninstall External Media Edition

- Run a command line similar to the following:

  If your Dell Enterprise Server is pre-v7.7:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8081/xapi REINSTALL=ALL
  REINSTALLMODE=vemus /qn"
  ```

  If your Dell Enterprise Server is v7.7 or later:

  ```
  DDPE_64bit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL
  REINSTALLMODE=vemus /qn"
  ```

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

Windows and EME Shields update the Dell Enterprise 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 Dell Enterprise 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.

Continue to Data Recovery.

6

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.

Prerequisites

- A recovery bundle is needed to recover data. Retrieve the recovery bundle as shown in Retrieve the Recovery Bundle.
- The recovery program must be run with Administrative rights on the drive that it is recovering. In Windows XP, the user account that the recovery program is run under must at least be a member of the Administrator Group. In Windows Vista, Windows 7, and Windows 8, the recovery program must be "Run as Administrator" to have access to perform the recovery operation.
- If the target computer is **not** bootable, call Dell ProSupport for assistance with data recovery (refer to your Welcome Letter for contact information).

Retrieve the Recovery Bundle

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

Method 1

1. As a Dell Administrator, log in to the Dell 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.
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 Recover Data.

Method 2

1. As a Dell Administrator, log in to the Dell 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.

   You can find the Host Name on the Endpoint Detail page in the Endpoint Detail section.

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 Recover Data.

Recover Data

1 Locate the recovery program downloaded from the Dell 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 HCA encrypted drive.
- I want to restore access to my HCA encrypted drive.

Select the **second** option and click **Next**.

NOTE: If you need to recover data due to options 1, 3, or 4, contact Dell ProSupport (refer to your Welcome Letter for contact information).

4 Click **Next** at the Backup\Recovery Information screen.

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

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 volumes are 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.

A

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\CREDANT.

For Windows Vista and Windows 7/8, 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.

B

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.

C

Configure Dell Key Server

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

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.

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 Dell Enterprise Server. The SAM account name, UPN, or domain\username is acceptable. Any method that can authenticate to the Dell 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 will fail because the Dell 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 Dell Enterprise 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 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" /> [how many 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 Dell 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. 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 Dell Enterprise Server. The SAM account
     name, UPN, or domain\username is acceptable. Any method that can authenticate to the Dell 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 will fail
     because the Dell 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 (in
     seconds) 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 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.

D

Use WSScan

When uninstalling DDP|E, 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 DDP|E 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

E

Glossary

Common Encryption – The Common key makes files accessible to all managed users on the device where they were created.

Encryption Keys – The “Common” key makes files accessible to all managed users on the device where they were created. The “User” key makes files accessible only to the user who created them, only on the device where they were created. The “User Roaming” key makes files accessible only to the user who created them, on any Shielded Windows device.

Hardware Crypto Accelerator (HCA) – HCA policies encrypt the files needed by the operating system to start the boot process (including the Master Boot Record), therefore, HCA policies require preboot authentication. HCA policies encrypt all fixed volumes or the system volume only, depending on the template chosen. When HCA policies are in play, System Data Encryption (SDE) policies are ignored.

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.

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) – This Trusted Computing Group specification deals with the storage of encryption keys, platform integrity, authentication of hardware devices and other security functions. It is also used as the general name of implementations of that specification, as in “TPM chip” or “TPM Security Device”.

User Encryption – The User key makes files accessible only to the user who created them, only on the device where they were created.


0 XXXXXA0 X