Dell Data Guardian

Administrator Guide v1.2

Notes, cautions, and warnings

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

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

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

Dell Data Guardian Administrator Guide

2017 - 05

Rev. A02

Contents

Introduction

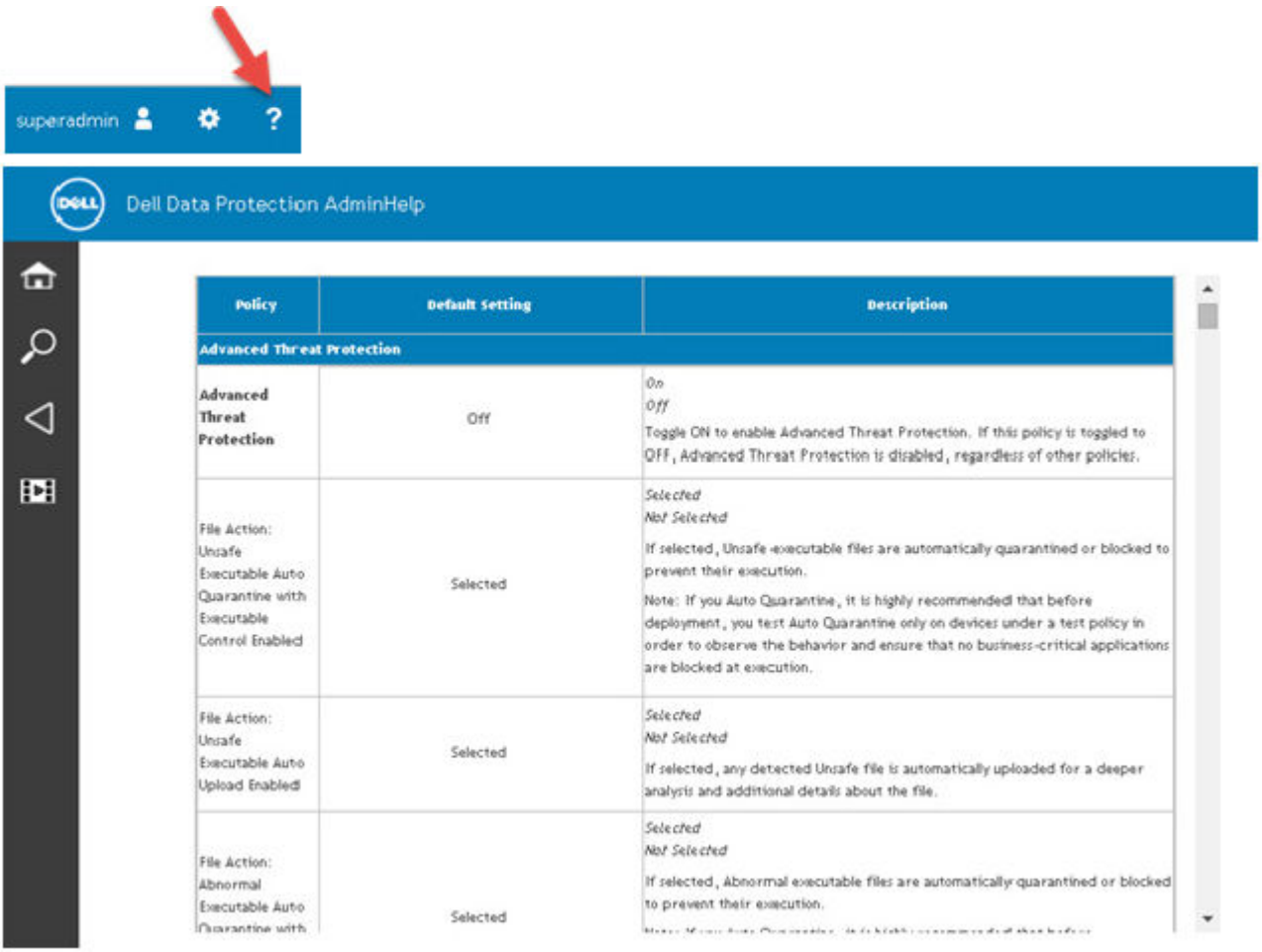
All policy information, and their descriptions are found in the AdminHelp.

Before You Begin

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

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

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



2 Thoroughly read the Requirements chapter of this document.

3 Deploy clients to end users.

Contact Dell ProSupport

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

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

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

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

2

Requirements

Server

Data Guardian requires that the client be connected to a Dell Enterprise Server or Dell Enterprise Server - VE, v9.6 or higher. For the purposes of this document, both Servers are cited as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Dell Enterprise Server - VE).

Data Guardian Client

- IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.
- The user account performing the installation/upgrade/uninstallation must be a local or domain administrator user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or Dell KACE. A non-administrator user that has elevated privileges is not supported.
- Back up all important data before beginning installation/uninstallation.
- Do not make changes to the computer, including inserting or removing external (USB) drives during installation.
- Data Guardian is not supported with Microsoft Office 365.
- For cloud encryption, the computer must have one (letter value) assignable disk drive available.
- Ensure that target devices have connectivity to https://yoursecurityservername.domain.com:8443/cloudweb/register and https://yoursecurityservername.domain.com:8443/cloudweb.
- Before deploying Data Guardian, it is best if the target devices do not yet have cloud storage accounts set up.

  If users decide to keep their existing accounts, they should ensure that any files that are to remain *unencrypted* are moved out of the sync client before installing Data Guardian.
- Users should be prepared to restart their computer after the client is installed.
- Data Guardian does not interfere with the behavior of sync clients. Therefore, administrators and end users should familiarize themselves with how these applications work prior to deploying Data Guardian. For more information, see Box support at https://support.box.com/home, Dropbox support at https://www.dropbox.com/help, or OneDrive support at http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- If running Office 2010: If policies have been set to protect Office documents and macro-enabled documents, users must have Office 2010 Service Pack 1 or higher (v14.0.6029 or higher). See https://support.microsoft.com/en-us/kb/2121559 to determine whether a service pack has been applied to a Microsoft Office 2010 suite. Without this update, protected documents cannot be accessed. New Office documents are unprotected, regardless of policy unless sweep functionality is on. The next sweep converts Office documents to protected files, but users cannot access them without a supported version of Office.
- Although Dell Encryption is not required, if used, the Encryption client should be v8.12 or later.
- Data Guardian does not support the Windows System Restore tool.
- Be sure to periodically check www.dell.com/support for the most current documentation and Technical Advisories.

Client Prerequisites

If not already installed, the installer installs Microsoft Visual C++ 2015 Redistributable Package (x86 and x64).

NOTE:

For Windows 7 and Windows 8.1, the computers should be up-to-date with Windows Updates. For more information, see https://support.microsoft.com/en-us/help/2919355 and https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (or later) is required for Data Guardian. All computers shipped from the Dell factory are pre-installed with .Net 4.5.2. However, if you are not installing on Dell hardware or are upgrading Data Guardian on older Dell hardware, you should verify which version

of .Net is installed and update the version, if needed, prior to installing Dell Data Guardian to prevent installation/upgrade failures. To verify the version of .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. To install Microsoft .Net Framework 4.5.2, go to https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Windows Client Hardware

Minimum hardware requirements must meet the minimum specifications of the operating system. The following table details supported hardware for the Windows client.

Windows Hardware

- 200 MB free disk space, depending on operating system
- 10/100/1000 or Wi-Fi network interface card
- TCP/IP installed and activated

If your enterprise encrypts data for storage in the cloud, your computer must have one alphabetic letter available to assign to a disk drive.

Operating Systems

The following table details supported operating systems.

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

- Windows 7 SP0-SP1
- Windows 8.1
- Windows 10

NOTE:
Windows 7 is not supported with the geolocation policy for Data Guardian audit events.

Android Operating Systems

- 4.4 - 4.4.4 KitKat
- 5.0 -5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow
- 7.0 Nougat

iOS Operating Systems

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

Cloud Sync Clients

The following table details cloud sync clients that work with Data Guardian. Sync client updates are released frequently. Dell recommends testing new sync client versions with Data Guardian before introducing them into the production environment.

Cloud Sync Clients

- Dropbox
- Dropbox for Business (Windows only)

  NOTE:
  Depending on the Dell Server version used by your company, all files and folders in personal Dropbox accounts that are linked to business accounts may be encrypted.

- Box

  NOTE:
  Box Tools and Box Edit are not supported with Data Guardian. Using Box Tools may cause a blue screen condition.

- Google Drive
- OneDrive
- OneDrive for Business
- Unified OneDrive

  NOTE:
  Unified OneDrive is a unified sync client for both OneDrive and OneDrive for Business.

Web Browsers

You can use Data Guardian > Cloud Encryption with Internet Explorer, Mozilla Firefox, and Google Chrome.

NOTE:
Data Guardian > Cloud Encryption does not support Microsoft Edge browser.

Language Support

These clients are Multilingual User Interface (MUI) compliant and support the following languages.

Language Support

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

3

Registry Settings

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

Data Guardian Client Registry Settings

- Logging levels can be increased to aid in troubleshooting. Create or modify the following registry setting.

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

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

  Available values:

  Off=0x0 (0)

  Critical=0x1 (1)

  Error=0x3 (3)

  Warning=0x7 (7)

  Information=0xf (15)

  Debug=0x1f (31)

- After installation of Data Guardian, internal users are automatically activated. If necessary, you can modify a registry setting to override auto-activation.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  DWORD Value: DisableAutomaticActivation=1

  NOTE:
  You can also confirm the aliases for your domain on the Dell Server. See Troubleshoot Auto-Activation Issues.

Configure Server for Data Guardian

Based on policies set by an administrator, Data Guardian protects data, for example:

- Cloud-based file sharing systems - Windows computers or mobile devices capture data intended for cloud storage, encrypt that data, and then upload the encrypted data into the cloud.
- Office documents stored locally, shared with other users in various ways, or stored on removable media. These Office documents can be protected: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

Inform users if your enterprise uses Data Guardian with cloud storage only, Office documents only, or both.

Configure VE Server for Data Guardian

To configure VE Server to support Data Guardian, in the Remote Management Console, set one or both Data Guardian policies to On:

- *Protected Office Documents* - Enterprise level only
- *Cloud Encryption* - Enterprise, Endpoint Groups, or Endpoints level

Configure EE Server for Data Guardian

To configure EE Server to support Data Guardian, in the Remote Management Console, set one or both Data Guardian policies to On:

- *Protected Office Documents* - Enterprise level only
- *Cloud Encryption* - Enterprise, Endpoint Groups, or Endpoints level

Then Configure the Security Server to Allow Cloud Client Downloads.

Configure the Security Server to Allow Data Guardian Client Downloads

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

1 On the EE Server, navigate to **<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources** and open the **messages.properties file** with a text editor.

2 Ensure that the entries are as follows:

download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe

3 Edit the entries to the following

download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe

4 Save and close the file.

5 Go to <Security Server install dir> and create a new folder under it named Download (Security Server\Download).

6 Within the Download folder, create another new folder and name it cloudweb (Security Server\Download\cloudweb).

7 Add the 64-bit and the 32-bit setup files for Data Guardian to the cloudweb folder and, optionally, rename them, for example, to DataGuardian64.exe and DataGuardian32.exe, respectively.

These are user-defined but must match the filenames in the versions.xml file.

8 Restart the Security Server for the changes to take effect.

Configure the EE Server for Automatic Downloads of the Windows Data Guardian Client (Optional)

For automatic downloads, the versions.xml file and binaries must be in the same location. The location must be accessible by the client, so it could be IIS or you could use the **Security Server\Download\cloudweb** folder you created. If using the cloudweb folder, here is an example of how to configure the Server.

1 Navigate to the **Security Server\Download\cloudweb** folder. (See step 6 in Configure the Security Server to Allow Data Guardian Client Downloads.)

2 Create a folder under named DataGuardianUpdate.

> **NOTE:**
> DataGuardianUpdate is used in this example, but you can choose any name.

3 Place the updated executables in the DataGuardianUpdate folder.

4 Create a *versions.xml* file in the DataGuardianUpdate folder.

5 Open *versions.xml* with a text editor and verify the filename path is correct for your environment.

Sample:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version: File version of the updated executables

setup.exe filename: The setup name of the executables is user-defined but must match the setup name in the messages.properties file. (See step 3 in Configure the Security Server to Allow Data Guardian Client Downloads.)

6 Save and close the file.

7 Add the binaries to this folder.

8 If using IIS, restart IIS.

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

10 In the left pane, click **Populations** > **Enterprise**, and the Security Policies tab displays.

11 Under the Data Guardian technology group, click **Cloud Encryption**.

12 Click **Show advanced settings**.

13 Scroll to the *Software Update Server URL* policy and enter **https://<YOUR HOST URL> /DataGuardianUpdate**.

> **NOTE:**
> DataGuardianUpdate is only an example to match the example above.

14 Click **Save** to store the policy modification in the queue to commit.

15 Click **Management** > **Commit**.

16 Enter a comment and click **Commit Policies**.

Manage Cloud Storage Protection Provider Profiles

Data Guardian encrypts users' files and sends audit events to the EE Server/VE Server. To change the behavior for each supported cloud storage provider, set each provider to one of these values:

Value	Description
Protect	Allow the provider/connection, encrypt the files, and send audit events about file/folder activity.
Block	Block all access to the provider/connection.
Allow	Allow the provider/connection to pass through without encrypting, but audit file/folder activity.
Bypass	Bypass the protection of the provider/connection without encrypting or auditing. When this value is set, the cloud storage provider folder does not display in the Data Guardian virtual drive on the client computer.

For more information, see the *AdminHelp*, which is accessible from the Remote Management Console.

Allow/Deny Users on Full Access List/Blacklist

You can determine which external users can register with the EE Server/VE Server to use Data Guardian. For adequate security, be sure to carefully set up and manage these lists.

- An internal user is within the domain.
- An external user is a non-domain user, either a person from another organization with whom an internal user wants to share business-sensitive documents or an internal user who wants to access their computer from a non-domain device.

To allow a user who is not in the organization's domain to register to use Data Guardian:

1 In the left pane of the Remote Management Console, click **Management > External User Management**.

2 Click **Add**.

3 Select Registration Access Type:

Blacklist - Blocks registration for a user or a domain. User cannot open a protected Office document or .xen file.

Full Access List - Grants registration and all file access for a user or domain. If a user or domain is also on the blacklist, no access is granted.

4 In the Enter Domain/Email field, enter either the user's domain to set access for the entire domain, or email address to set access only for that user.

5 Click **Add**.

For more information on using full access list/blacklist, see *AdminHelp*, which is accessible from the Dell Server Remote Management Console.

Re-image a Computer with Data Guardian

If a remote user's computer needs to be re-imaged and they have Dell Data Guardian, ask if the user has worked offline and created any protected Office documents while offline. If so, offline keys were generated for those documents and those keys have not been escrowed to the Dell Server.

1 For information on recovering Data Guardian offline-generated keys that were not escrowed to the Dell Server, see the *Recovery Guide*.

2 Check for an offline keys folder before you re-image the user's computer.

When the first escrow keys are created a Data Guardian folder is added to **C:\Program Files\Dell\Dell Data Protection**. Navigate to the **Data Guardian > OfflineKeys** folder. If no OfflineKeys folder exists, check the user's **My Documents** folder.

5

Install Data Guardian

There are two methods to install Data Guardian:

- Install Data Guardian Interactively
- Install Data Guardian with Command Line

Data Guardian users must perform the following tasks in order for files and folders in their cloud sync clients to be protected. After installation of the Data Guardian client, users must download a cloud storage provider:

- The administrator should specify which cloud sync provider to be used.

  or

- Provide users with a link for downloading and installing Dropbox for Business or OneDrive for Business/Unified OneDrive if your enterprise uses one of these providers. Remember that Dropbox for Business users must connect to Dropbox for Business through Data Guardian.

Pre-existing Folders with Unencrypted Files

When deploying Data Guardian, it is best if the target devices do not yet have a cloud storage provider account set up.

If a cloud storage provider account is set up with folders that are synced to the local computer before Data Guardian installation:

- Pre-existing files and folders that sync up to the cloud remain in cleartext
- Files you add to those pre-existing folders remain in cleartext
- Files that sync down from the cloud are encrypted

  If you want pre-existing files to be encrypted, navigate to the DDG VDisk virtual drive (created when Data Guardian is installed), create a new subfolder within the cloud sync client and move the pre-existing files into that folder.

Install Data Guardian

You must be a local administrator on the computer to install Data Guardian.

The computer must have one alphabetic letter available to assign to a disk drive.

Be prepared to restart the computer after Data Guardian is installed.

1. To download the Data Guardian installer, go to the location specified by your administrator.
2. Based on your operating system, select either the 32-bit or 64-bit installer, typically **setup32.exe** or **setup64.exe**, and copy it to the local computer.
3. Double-click the file to launch the installer.
4. If you get a Security Warning, click **Run**.
5. Select a language and click **OK**.
6. If prompted to install Microsoft Visual C++ 2015 Redistributable Package or Microsoft .NET Framework 4.0 Client Profile, click **OK**.
7. At the Welcome screen, click **Next**.
8. Read the license agreement, accept the terms, and click **Next**.

9 At the Destination Folder screen, click **Next** to install in the default location of **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\.**

On **C:**, do not install Data Guardian in the Users or Windows folders or at the root of any drive. You will get an error.

10 In the *Server Name:* field, enter the Server Name that this computer will communicate with, such as server.domain.com. You do not need to include www or http(s). This information is supplied by your administrator.

Do not clear the *Enable SSL Trust Verification* check box unless your administrator instructs you to do so.

11 Click **Next**.

12 In the Confirm Activation Server Information screen, confirm that the Server URL address is correct. The installer adds www or http(s) and the port. Click **Next**.

13 In the Management Type window, select this option:

- Internal Use - A user with an email address within the company's domain.

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

A status window displays the installation progress.

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

16 Click **Yes** to restart.

Installation of Data Guardian is complete.

17 The Data Guardian system tray icon shows a green check mark  after activation. Depending on the way Data Guardian is deployed within the enterprise, activation may not be immediate.

Install Data Guardian with Command Line

- Command line switches and parameters are case-sensitive.
- Be sure to enclose a value that contains one or more special characters, such as a blank space in the command line, in escaped quotation marks.
- The following table details the switches available for the installation.

Switch	Meaning
/V	Pass variables to the .msi inside the setup.exe. The content must always be enclosed in plain-text quotes.
/S	Silent mode

Option	Meaning
/QB	Progress dialog with **Cancel** button, prompts for restart
/QB!	Progress dialog without **Cancel** button, prompts for restart
/QN	No user interface

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

Parameters
SERVER=<ServerName> (FQDN of the Dell Server for activation)
ENTERPRISE=1 (Internal User)
ENABLESSLTRUST=0 (Disable SSL trust validation)
REBOOT=SUPPRESS (Null allows for automatic reboots, SUPPRESS disables reboot)

Example Command Line

- The following example installs Data Guardian silently, for an internal user, with no SSL trust validation, logs stored to C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

Set GPO on Domain Controller to Enable Entitlements

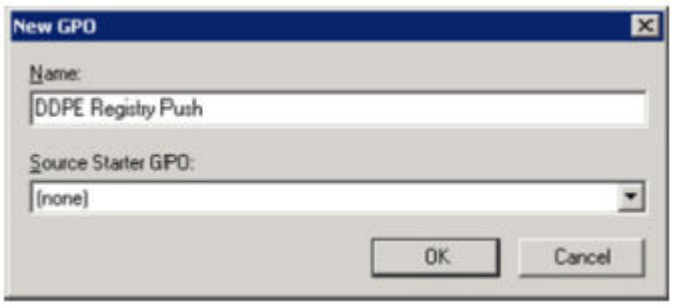
- If your clients will be entitled from Dell Digital Delivery (DDD), follow these instructions to set the GPO on the domain controller to enable entitlements (this may not be the same server running the EE Server/VE Server).
- The workstation must be a member of the OU where the GPO is applied.

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

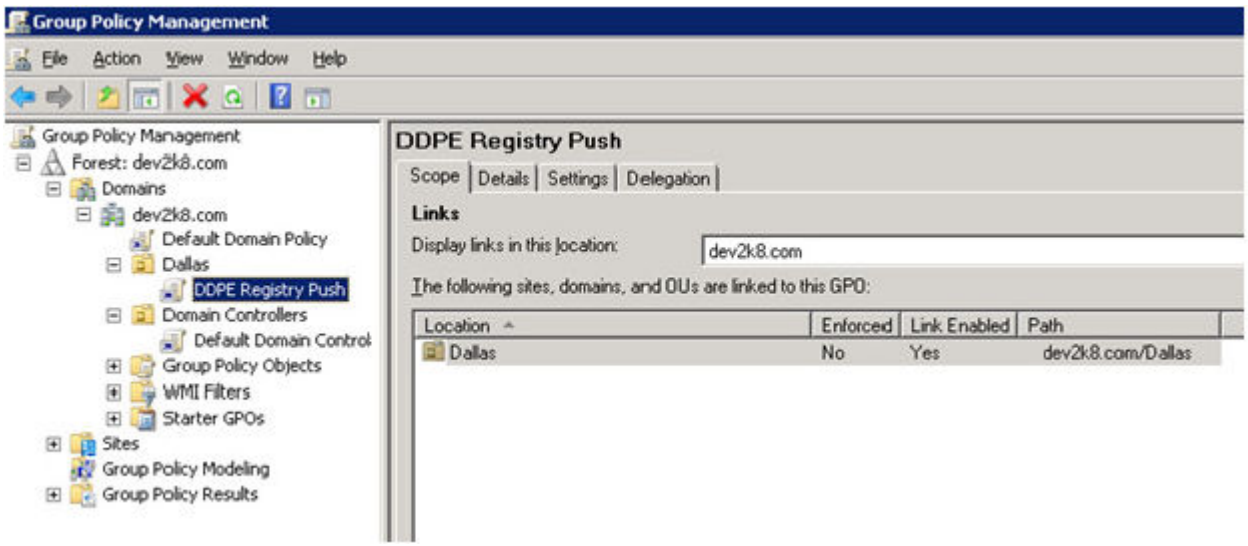
1 On the Domain Controller to manage the clients, click **Start** > **Administrative Tools** > **Group Policy Management**.

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

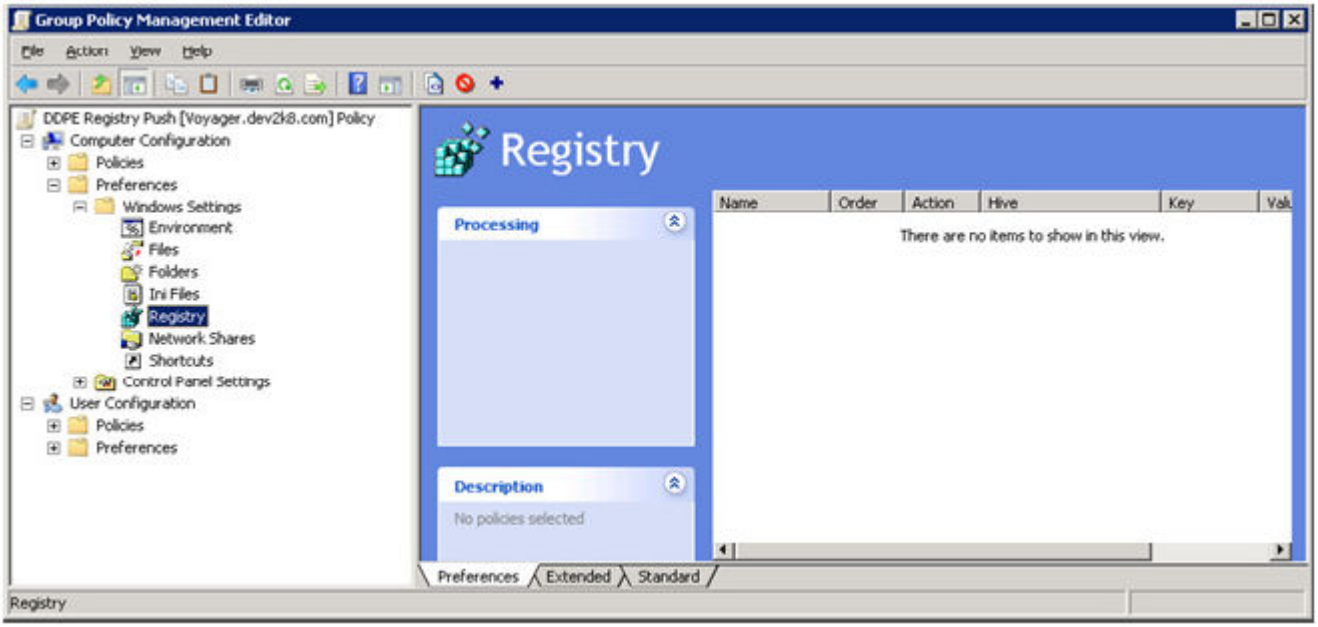
3 Enter a name for the new GPO, select (none) for Source Starter GPO, and click **OK**.



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



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



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

Action: Create

Hive: HKEY_LOCAL_MACHINE

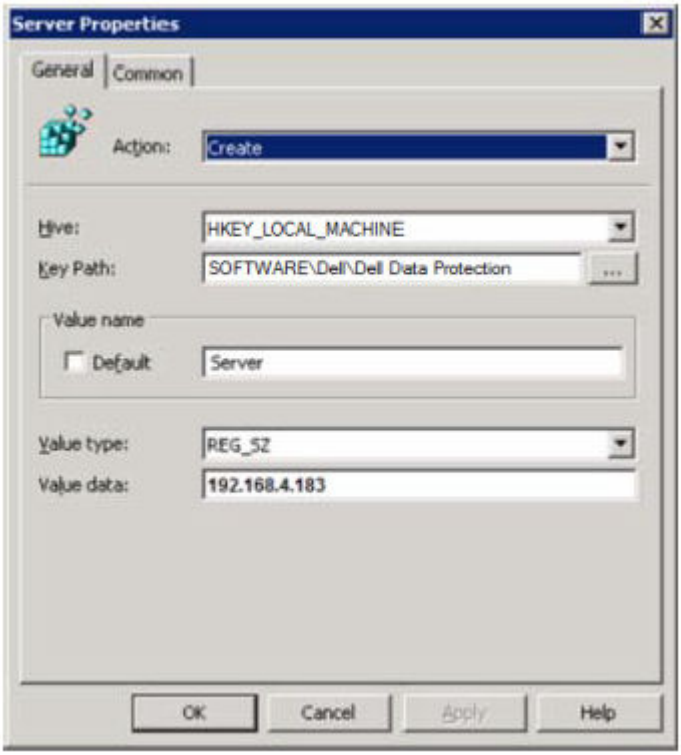
Key Path: SOFTWARE\Dell\Dell Data Protection

Value name: Server

Value type: REG_SZ

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

7 Click **OK**.



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

Use Data Guardian with Dropbox for Business

Data Guardian with Dropbox for Business offers additional functionality over basic Dropbox.

- Remote Wipe a Team Member Account
- You can set policies to control how business and personal Dropbox folders are protected. If your enterprise allows both business and personal accounts, end users should understand encryption of each type of account. See Policy for Business and Personal Accounts.

Policy for Business and Personal Accounts

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

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

The following table describes encryption based on the *Dropbox Encrypt Personal Folders* policy setting.

Encryption	Policy Setting	Deployment Considerations
Encrypt all business and personal files and folders.	Policy > Dropbox Encrypt Personal Folders > set to **Selected** (default)	Before Data Guardian is deployed, users should back up pre-existing business files that are in cloud storage sync folders to locations outside the sync folders. Users with personal files that should stay unencrypted must move the files out of business sync folders or unlink personal accounts from business sync clients. After Data Guardian is deployed, cloud files and folders can be viewed only on computers or devices running Data Guardian. If a personal folder becomes unintentionally encrypted, see "Decrypting Folders in a Personal Account" in the Dell Data Guardian User Guide.
Encrypt all business account files and folders. Allow personal account files and folders to remain unencrypted.	Policy > Dropbox Encrypt Personal Folders > set to **Not Selected**	You can use the optional Dropbox Encrypt Personal Folders Message policy to display a customized message to remind users **not** to store business files in personal accounts, since those files will not be protected. The message is displayed at these times. • Each time the user logs in • When the user creates or adds a new file or folder to a personal Dropbox account If you set the Dropbox Encrypt Personal Folders policy to **False** for an Endpoint

Encryption	Policy Setting	Deployment Considerations
		or Endpoint Group, personal accounts of all users on those endpoints will remain unencrypted.

Business and Personal Folders

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

Remote Wipe a Team Member Account

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

Prerequisites

- Before performing a remote wipe, back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.
- Only a Dropbox for Business administrator can remote wipe a Dropbox for Business account.
- Data Guardian must have been activated, and the end user must have connected to Dropbox for Business.

Register in the Remote Management Console

Only one Dropbox for Business administrator needs to register.

1 In the Remote Management Console, select **Dropbox Management** in the left pane.
2 Click **Register**. The browser opens to the Dropbox for Business site.
3 If prompted, log in to Dropbox with your Dropbox for Business administrator account.
4 Click **Allow** to allow access to Data Guardian. A confirmation page displays to indicate Dropbox authorization is granted to the VE Server.
5 In the Remote Management Console, return to **Dropbox Management** and refresh the page. The administrator name displays.

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

Remote Wipe a Team Member Account

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

1 In the Remote Management Console, select **Populations** > **Users** in the left pane.
2 Search for the specified user.
3 Click the **Details & Actions** tab.
4 In the Command column, click **Remote Wipe**.

NOTE:

You should perform a back up of any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members before you Remote Wipe the account.

5 Click **Yes** at the confirmation for Remote Wipe. The User Detail page lists the date the remote wipe is performed.

6 Refresh the list of Team Members in the Dropbox for Business Administrator Console Members page. The user is removed from the list. You can select the **Removed Members** tab to view users which have been removed.

View Reports

Information about your Data Guardian environment is available in Dell Server's Remote Management Console. Select **Reporting > Audit Events** for audit events related to cloud sync client folders and protected Office documents.

For more information, see *AdminHelp*, which is accessible through the Remote Management Console.

8

Data Guardian Troubleshooting

Use the Details Screen

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

- If a user creates a folder but it's not encrypting, select **Details** > **Files** > **Folder State** to check the state.
- If an end user requests support, you can instruct them to set up the Enhanced Details screen and select the **Details** > **Policy** tab. This tab lists which policies are being enforced.
- View logs for troubleshooting.

Use the Enhanced Details Screen

- While pressing **<Ctrl><Shift>**, click the Data Guardian system tray icon, and then select **Details**.
- In addition to Files and Folders, the following display:

  Security: Lists the key, key type, and state. This pane temporarily lists some protected Office files until they are sent to the Server - the length of time depends on the polling interval.

  Audit: Lists modules, user ID, and event type. Information is in queue in this audit log and then sent to the EE Server/VE Server at specified intervals. The administrator can view **Audit Events** from the left pane of the Remote Management Console for auditing.

  Policy: Lists the policy names and values.

View Log Files

- Click **View Log** from the bottom-left corner of the Details screen.

  Log files can be also be found at C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.

  Protected Office document logs files are located in the Custom.xml folder.

Troubleshoot Auto-Activation Issues

If Data Guardian does not auto-activate for several users, you can change the Data Guardian Client Registry Settings. You should also check the aliases on the Dell Server:

1. In the Remote Management Console, navigate to **Populations > Domains** and select a domain and any sub-domains.
2. On the Domain Detail page, select the **Settings** tab.
3. In the *Alias* field, confirm that all aliases are correct.

Provide Temporary Folder Management Rights

You can grant an administrator or user temporary rights to manage folders. For example, if users uploaded files to the cloud before Data Guardian was installed, you can provide temporary Folder Management rights to some users to manage encryption on a folder-by-folder basis within the sync client folders.

To provide folder management rights:

1 In the Remote Management Console, click **Populations** > **Endpoints**.

2 Search for or click an endpoint and then click the **Security Policies** tab.

3 Select **Cloud Encryption**, and then click **Show advanced settings**.

4 Click the check box next to *Folder Management Enabled* to select the policy.

5 Click **Save**.

6 In the left pane, click **Management** > **Commit**.

7 Enter a comment and click **Commit Policies**.

NOTE:
Dell recommends that after the folders are encrypted or troubleshooting is completed, clear the *Folder Management Enabled* policy check box to disable the policy for that endpoint.

To manage folders on the endpoint:

1 Create a folder within the sync client folder and add files, so that the files are encrypted in the cloud.

2 Click the Data Guardian system tray icon and select **Manage Folders**.

A hierarchical view of cloud sync folders displays for each sync client. All folders are selected by default. Deselect folders you do not wish to encrypt. If you deselect a folder in Manage Folders, a decryption sweep decrypts existing files in that folder. New files in that folder are not encrypted on the local drive or in the cloud.

NOTE:
If you drag an encrypted file into a folder that is deselected in Manage Folders either in the cloud or on the DDP|SL virtual drive, the file will remain encrypted and you cannot view the contents. Also, if you share the folder with another Data Guardian user who does not have the Manage Folders policy enabled, the files remain encrypted for them, and they cannot view the contents.

3 To encrypt a pre-existing folder, manually turn on encryption for that folder. The files will be encrypted when the files sync to the cloud.

Frequently Asked Questions

Folder Management FAQs

Question

I have a folder with files that I have shared with another user. In the system tray, I used the **Data Guardian > Manage Folders** utility to decrypt that folder's contents. Recently, my files have become encrypted in the cloud again. That folder no longer displays in the Manage Folders utility, so I can no longer decrypt those files in the cloud.

Answer

An encryption key ID is associated with a folder based on the first user who adds a file to that folder. If a user creates a folder and does not add any files, their key is not associated with that folder. The user whose encryption key ID has been set on the folder is the only one who can view the folder in the Manage Folders utility. If the user whose encryption key ID is set on the folder deselects the folder in the Manage Folders utility and they share that folder with another Data Guardian user, the second user's Data Guardian will re-encrypt the contents.

Solution

1 Create a new folder.

2 Move all the files that should be encrypted to the new folder.

3 In the system tray, use the **Dell Data Guardian** > **Manage Folders** utility again to decrypt those files.

NOTE:

If you decrypt the contents of a folder that are shared with another Data Guardian user, the other user's Data Guardian client will enforce the policy to encrypt them. The best practice is to use the Manage Folders utility to decrypt only files that are not shared with other Data Guardian users.

Question

I am syncing to a decrypted folder that I deselected using the Manage Folders utility. However, when I try to upload it through the web browser, I can only upload encrypted files.

Answer

Data Guardian is not designed to actively search for folders in the cloud. With unencrypted folders, Data Guardian can sync through the sync client because it is controlling that environment. Files going through the web browser are required to be encrypted.

Solution

Add files to the sync folder.

Question

I recently uninstalled my cloud-based file sharing system from my computer, but when I opened the Manage Folders utility, one of the sync clients was still listed as an option.

Answer

Data Guardian does not monitor installation or uninstallation of third-party software. Those options are still listed because, by design, when these clients are uninstalled, they do not remove your existing files. Those files are still being protected by Data Guardian even though that sync client is no longer installed.

Solution

To remove the uninstalled sync client option from the Manage Folders utility, move any folders/files that you want to keep out of the sync folder, and then delete the folder. After you delete the folder, it is no longer listed in the Folder Management utility.

Miscellaneous Frequently Asked Questions

Question

A user has Data Guardian with Protected Office Documents and cannot copy or paste.

Answer

For Data Guardian, some functionality is handled through the systray. Check whether the user has modified the systray.

Solution

Default systray settings must be used. The user must retain the default systray settings.

Question

I changed the **Obfuscate Filenames** policy from Guid to Extension only. However, the folders I had previously been syncing are still encrypting those files to the other format with Guid filenames. Why?

Answer

When a policy is changed on the EE Server/VE Server, Data Guardian maintains the previous policy for that folder. Any new folders created will have the new policy applied and will encrypt to the **Extension Only** format.

Solution

To reapply the **Extension Only** format to the old files, cut and paste them to a new folder that has the new policy applied.

9

Glossary

Advanced Authentication - The Advanced Authentication product provides fully-integrated fingerprint, smart card, and contactless smart card reader options. Advanced Authentication helps manage these multiple hardware authentication methods, supports login with self-encrypting drives, SSO, and manages user credentials and passwords. In addition, Advanced Authentication can be used to access not only PCs, but any website, SaaS, or application. Once users enroll their credentials, Advanced Authentication allows use of those credentials to logon to the device and perform password replacement.

BitLocker Manager - Windows BitLocker is designed to help protect Windows computers by encrypting both data and operating system files. To improve the security of BitLocker deployments and to simplify and reduce the cost of ownership, Dell provides a single, central management console that addresses many security concerns and offers an integrated approach to managing encryption across other non-BitLocker platforms, whether physical, virtual, or cloud-based. BitLocker Manager supports BitLocker encryption for operating systems, fixed drives, and BitLocker To Go. BitLocker Manager enables you to seamlessly integrate BitLocker into your existing encryption needs and to manage BitLocker with the minimum effort while streamlining security and compliance. BitLocker Manager provides integrated management for key recovery, policy management and enforcement, automated TPM management, FIPS compliance, and compliance reporting.

Deactivate - Deactivation occurs when SED management is turned OFF in the Remote Management Console. Once the computer is deactivated, the PBA database is deleted and there is no longer any record of cached users.

EMS - External Media Shield - This service within the Dell Encryption client applies policies to removable media and external storage devices.

EMS Access Code - This service within the Dell Enterprise Server/VE allows for recovery of External Media Shield protected devices where the user forgets their password and can no longer login. Completing this process allows the user to reset the password set on the removable media or external storage device.

Encryption Client - The Encryption client is the on-device component that enforces security policies, whether an endpoint is connected to the network, disconnected from the network, lost, or stolen. Creating a trusted computing environment for endpoints, the Encryption client operates as a layer on top of the device operating system, and provides consistently-enforced authentication, encryption, and authorization to maximize the protection of sensitive information.

Endpoint - a computer or mobile hardware device that is managed by Dell Enterprise Server/VE.

Encryption Sweep - An encryption sweep is the process of scanning the folders to be encrypted on a managed endpoint to ensure the contained files are in the proper encryption state. Ordinary file creation and rename operations do not trigger an encryption sweep. It is important to understand when an encryption sweep may happen and what may affect the resulting sweep times, as follows: - An encryption sweep will occur upon initial receipt of a policy that has encryption enabled. This can occur immediately after activation if your policy has encryption enabled. - If the Scan Workstation on Logon policy is enabled, folders specified for encryption will be swept on each user logon. - A sweep can be re-triggered under certain subsequent policy changes. Any policy change related to the definition of the encryption folders, encryption algorithms, encryption key usage (common versus user), will trigger a sweep. In addition, toggling between encryption enabled and disabled will trigger an encryption sweep.

One-Time Password (OTP) - A one-time password is a password that can be used only once and is valid for a limited length of time. OTP requires that the TPM is present, enabled, and owned. To enable OTP, a mobile device is paired with the computer using the Security Console and the Security Tools Mobile app. The Security Tools Mobile app generates the password on the mobile device that is used to log onto the computer at the Windows logon screen. Based on policy, the OTP feature may be used to recover access to the computer if a password is expired or forgotten, if OTP has not been used to log on to the computer. The OTP feature can be used either for authentication or for recovery, but not both. OTP security exceeds that of some other authentication methods since the generated password can be used only once and expires in a short time.

SED Management - SED Management provides a platform for securely managing self-encrypting drives. Although SEDs provide their own encryption, they lack a platform to manage their encryption and available policies. SED Management is a central, scalable management component, which allows you to more effectively protect and manage your data. SED Management ensures that you will be able to administer your enterprise more quickly and easily.