Dell Data Guardian

Windows, Mac, Mobile, and Web User Guide v2.9

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.

2019 - 08

Rev. A01

Contents

1

Introduction

The *Dell Data Guardian User Guide* provides the information needed to install and use Data Guardian on Windows, Mac, Mobile, or a web portal.

Topics:

Overview

Data Guardian can protect data in a large number of file types whether stored locally, shared with other users in various ways, or stored on removable media. Your administrator can enable policies that protect data, for example:

- **Basic File Protection** - Your administrator defines non-Office file extensions to protect (like .txt or .png) and the applications that can open the file type. A sweep encrypts those file types.
- **Office documents** (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) - Policies determine the level of security:
  - **Opt-in** protection - The user chooses which Office documents to protect.
  - **Forced** protection - A sweep protects all Office documents stored on the local computer.

  If an unauthorized user tries to open the file only a cover page displays. However, you can grant access to an external user, and the cover page provides links for viewing the encrypted file on a mobile device or the Data Guardian web portal.
- **Content Based Protection** (previously *Data Classification*) - For users who classify Office documents that contain sensitive information, like account numbers, credit card numbers, or healthcare data, a Data Guardian sweep can encrypt specified classification types to prevent unauthorized access when data is at rest or in motion.
- **Outlook email protection** - Based on policy, users can protect email attachments or the entire email. If sent to an external person, the user can later revoke access of the key so the external user can no longer open it.
- **Cloud protection** - Documents uploaded to the cloud from Android or iOS mobile devices are protected.

You can use Data Guardian from the following platforms:

- Windows
- Mac
- Mobile devices - iOS, Android, Chromebook
- Data Guardian web portal, if set up by your administrator. The web portal allows internal and external users to view or edit encrypted files in a web browser, without installing the Data Guardian client.

NOTE:

Data Guardian can open files encrypted by the other platforms. Some files may be read-only.

Encryption Options for Data Guardian

Based on the level of security established by your enterprise, your administrator sets policies to protect data at rest and data in motion. Your administrator will tell you which policies apply to your enterprise.

This list provides an overview of some encryption options and, for some platforms, the location of policy settings.

Basic File Protection (Windows, Mac, mobile, and web portal)

Your administrator can configure a policy to specify non-Office applications and file types to be encrypted. Your administrator will inform you which file extensions will be swept and protected (like .txt or .png) and the applications that can open the file type to your enterprise.

Option	Description
Basic File Protection and Windows Mac Mobile web portal • Examples: .txt or .png	**Windows and Mac** - These files are swept and encrypted. • **Mac** - for file extensions set by the administrator, encrypts those file types in the */Users* folder. **Web portal** - Also based on policy, these files may be read-only or user can edit.

Office Document Protection (Windows, Mac, mobile, and web portal)

Data Guardian can protect these Office documents:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm
- .pdf - If protected with Data Guardian, open with Adobe Acrobat Reader DC or Microsoft Word but not from the network.

Office Document Protection - Windows and Mac

Policy can be set to protect Office documents. Encryption behavior may differ depending on the platform and mode.

Windows and Office documents	Mac and Office documents
Mode options: **Opt-in mode** - You have some options in determining which Office documents to protect. • A **Secure Documents** folder is added to the root of your Documents folder. This provides another way to encrypt a file. **Force-Protected Mode** - Your enterprise requires a higher level of security. Data Guardian performs a sweep to encrypt files. • Another policy can add an **Unprotected Documents** folder to the root of your Documents folder. Place Protected Office documents or Basic File Protection types in this folder to decrypt them.	For Mac, see the online Help. **Opt-in mode** - You have some options in determining which Office documents to protect. • A **Secure Documents** folder is added to the root of your Documents folder. This provides another way to encrypt a file. **Force-Protected Mode** - Your enterprise requires a higher level of security. Data Guardian performs a sweep to encrypt files. • Another policy can add an **Unprotected Documents** folder to the root of your Documents folder. Place Protected Office documents or Basic File Protection types in this folder to decrypt them. • **Mac** - Protects files in **/Users**. Dell Data Guardian interface **Mac** - Upload a protected document to encrypt. Download a protected document to decrypt. After editing a protected document, changes are saved to the original file, either in the cloud or locally.

Office documents - Windows

Your administrator can set additional Data Guardian policies to control or prevent data loss through these options. Encryption behavior may differ depending on the mode.

Options for protected Office documents in Windows	Description
• Protected Save As	Save Office files
Content Based Protection (Windows with Opt-in mode)	If a policy is enabled and configured to protect sensitive information, such as Social Security Numbers or credit card numbers, Office documents with that data are encrypted.

Options for protected Office documents in Windows	Description
TITUS classification (Windows with Opt-in mode)	If a Data Guardian policy is enabled for a TITUS classification, selecting that classification also encrypts the file. This provides another way for users to protect an Office document.

Office documents - mobile and web portal

Your administrator will inform you which apply to your enterprise.

Encryption option	Description
Mobile - within the Data Guardian app • Onscreen watermark	**Mobile** - Based on policy: • Office documents within the Data Guardian app are protected. • When a protected Office document is opened, the screen displays a watermark with the computer name and user name.
Web portal • Onscreen watermark	**Web portal** - You can upload protected or unprotected documents, but any uploaded file is protected when you click Download. When a protected Office document is opened, the screen displays a watermark with the computer name and user name.

Additional options

Your administrator will inform you which apply to your enterprise.

Option	Description (Opt-in and Force Protect modes)
Share protected Office documents with **external users**. (Windows, Mac, mobile, and web portal) A cover page lists links for registering and information for installing Data Guardian on a mobile device or the web portal to view the encrypted file.	• External users and **Windows** - You can also add a **date restriction (embargo)** on protected Office documents and PDFs. • **Web portal** - You can upload shared files to the web portal. You cannot share a file from within the web portal, but you can share it after you download it.
Tampered file or cover page (Windows, Mac, mobile, and web portal)	For Office files, Data Guardian can scan protected documents and detect some forms of tampering.
Outlook email encryption (Windows)	Based on policy, a *Protect* button allows you to encrypt the content of an email and attachments.
Access Groups (on-prem and SaaS) (Windows, Mac, mobile, and web portal) Encryption behavior may differ depending on the platform and mode.	When enabled by your administrator, only people in your access group can view your encrypted files. You can also grant access to internal and external users for individual files and they can request access. Based on additional policy, you can right-click an Outlook email labeled as [PROTECTED] and remove access for individual users and groups.
Geofencing (mobile)	Only users in a specified area can access files from their mobile phones.

Hosted or On-prem

If you have to install Data Guardian yourself, your administrator will confirm which option applies to your enterprise.

NOTE:

For mobile applications, if you have Workspace ONE installed, you can authenticate to Data Guardian with single sign-on.

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.	An on-prem Server located within the enterprise network for managing Dell Data Security software.
If your enterprise is multi-tenant, your administrator will provide an Installation ID. When a cover page displays for a user who does not yet have access to a protected document, information about the Installation ID is included on the cover page.	Your administrator will provide the name of the Dell Server URL.
All platforms - if a tenant fails to pay for a specified time, that tenant can be suspended.	

Cloud Encryption

Encryption behavior may differ depending on the platform and mode. Your administrator will inform you which apply to your enterprise.

Platforms	Description
Mobile	See Use Cloud Protection with Mobile.
Mac	See the online Help.
Web portal	See the online Help.
Windows	Currently, Data Guardian's Cloud Encryption protection has been disabled on Windows to prevent compatibility issues with newer functions of cloud service providers. To view .xen files already protected with Cloud Encryption, use Data Guardian's Mobile app, web portal, or Data Guardian with Mac.

Policy settings

Some platforms include a partial list of policy settings for your device.

Platform	Location of policy settings
Mac	*Preferences* pane
Mobile	**Settings** icon > **About**
Web portal	**Settings** icon > **About**

Additional Support

Should you need additional support beyond this document, contact your administrator.

2

Requirements

Client hardware and software requirements are provided in this chapter.

Topics:

Dell Server

Data Guardian for Windows, Mac, and Mobile requires Security Management Server or Security Management Server Virtual v9.6 or higher. The Data Guardian web client requires Security Management Server or Security Management Server Virtual v9.8 or higher. For the purposes of this document, both Servers are referred to as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Security Management Server Virtual).

Data Guardian for Windows

- 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 supported with specific versions of Microsoft Office 2016 and also Microsoft Office 365 Business and Business Premium. It is not supported with Office 365 Business Essentials.
- Data Guardian for Windows is compatible with Workspace ONE. The Data Guardian installer for Workspace ONE and an MSI installation has an .msi extension.
- Data Guardian v2.4 and higher on Windows is supported in Air Gap environments, but with some limitations. Currently, geolocation data in audit events and embargo files are not supported. Web beacon requires some configuring.
- 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 users should familiarize themselves with how these applications operate 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.
- Protected Office documents are supported with Mozy, a companion solution to Data Guardian, as well as other cloud, email, and NFS storage products.
- 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 or Windows Insider Preview.
- Microsoft's Folder Redirection is not supported with Data Guardian.
- Be sure to periodically check dell.com/support for the most current documentation and Technical Advisories.

Prerequisites

.exe prerequisites

If not already installed, the installer installs Microsoft Visual C++ 2017 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.

.msi prerequisites

You must install Microsoft Visual Studio C++ 2017 Redistributable Package (x86 and x64).

NOTE:

In addition, if running MSI, you must also install Visual Studio 2010 Tools for Office Runtime (x86 and x64).

General prerequisite

Microsoft .Net 4.7.2 (or later) is required for Data Guardian. However, this may not be pre-installed on computers shipped from the Dell factory. Also, 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 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 4.7.2, go to https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows.

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

Operating Systems

The following table details supported operating systems.

Windows Operating Systems (32-bit and 64-bit)
• Windows 7 SP1: Enterprise, Professional, Ultimate • Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition • Windows 10: Education, Enterprise, Pro Version 1703 (Creators Update/Redstone 2) through Version 1903 (May 2019 Update/19H1)

NOTE:

The client must be on one of these operating systems, or it will be blocked. If needed, a setting in a registry key allows the administrator to override the block.

For Redstone 4 support, you must upgrade the agent before upgrading the operating system. See https://www.dell.com/support/article/us/en/04/sln307922.

NOTE:

Data Guardian is not compatible with Microsoft's Windows Defender Exploit Guard (WDEG) in Redstone 3 and higher or with Enhanced Mitigation Experience Toolkit (EMET) in Redstone 2 and lower.

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

Data Guardian does not support multiple versions of Office on one computer.

Microsoft Office

Data Guardian supports the following versions of Office. However, you must have just one version of Office installed.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019
• Office 365 ProPlus: versions 1705, 1708, and 1803 (Semi-Annual Channel)

Data Guardian for Mac

The following lists supported hardware for the Mac client.

Mac Hardware
• Intel Core 2 Duo, Core i3, Core i5, Core i7, or Xeon processor
• 2 GB RAM
• 10 GB free disk space

Operating Systems

The following lists supported operating systems.

Mac Operating Systems
• macOS Sierra 10.12.6
• macOS High Sierra 10.13.6
• macOS Mojave 10.14.4 - 10.14.6

Cloud Storage Providers

Based on policy settings, the following can display in the Data Guardian for Mac interface. The user does not need to download or install the cloud sync client.

Cloud Storage Providers
• Dropbox
• Box
• Google Drive **NOTE:** ***Google Backup and Sync* is not supported.**
• OneDrive
• OneDrive for Business

Microsoft Office

Data Guardian for Mac supports the following versions of Office.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Data Guardian for Mobile Application

The following lists operating systems supported with Data Guardian for Mobile.

Android Operating Systems
• 5.0—5.1.1 Lollipop
• 6.0—6.0.1 Marshmallow
• 7.0—7.1.2 Nougat
• 8.0—8.1 Oreo
• 9.0 Pie

iOS Operating Systems
• iOS 10.x—10.3.3
• iOS 11.x—11.4.1
• iOS 12.x—12.3

Chromebook Operating System
Chrome OS version M53 or higher is required to run Android applications on Chrome OS. These devices are validated to run Android apps on Chrome OS, but confirm your option with your sales representative:
• https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

Data Guardian for Mobile Application can open files created with the following versions of Office.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Data Guardian for Web

To enable the Data Guardian web client, the administrator sets up a virtual machine that hosts the web client and communicates with the Dell Server v9.8 or later.

The following virtualized environments can be used to deploy the Data Guardian web client.

Virtualized Environments

- **VMware ESXi 6.7**
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-67/index.jsp for more information
- **Microsoft Hyper-V**
  - 64-bit Processor with Second Level Address Translation (SLAT)
  - 8 GB RAM minimum recommended
  - Hardware must conform to minimum Hyper-V requirements
  - See https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements for more information.

NOTE:

These minimums represent twenty-five or fewer simultaneous connections to a single web portal.

Cloud Storage Providers

Based on policy settings, Data Guardian's web portal can access these cloud storage providers.

Cloud Storage Providers
• OneDrive for Business

Microsoft Office

Data Guardian for Web can open files created with the following versions of Office.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Other Requirements

Currently, Amazon Cognito's multi-factor authentication (MFA) is not supported with any Data Guardian platform.

Web Browsers

You can use Data Guardian with Internet Explorer, Mozilla Firefox, Google Chrome, and Microsoft Edge.

For Mac, Safari is also supported.

Adobe Acrobat

For Windows and Mac, protected .pdf files can be opened with Adobe Acrobat Reader DC.

NOTE:

The following are not supported: Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC, and Adobe Acrobat DC.

3

Install or Uninstall Data Guardian on Windows

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

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

Topics:

Overview of Installation Tasks for Windows

This overview summarizes the sequence for installing Data Guardian.

Install Data Guardian

Task	Description	For More Information
Install Data Guardian	Determine the following: User must install Data Guardian Administrator already installed Data Guardian - continue to next step.	User installs: See Install Data Guardian Interactively on Windows. Reboot and continue to the next step.
Confirm activation status	Confirm on the notification area that the Data Guardian icon has a green checkmark  .	If the icon has an orange exclamation point, see Possible Issues With Activating. **NOTE:** **If you open an Office document and a cover page displays with installation or activation information, your administrator may have set policies to protect Office documents. Confirm that Data Guardian is installed and activated.**

Options for Windows

Task	Description	For More Information
View notification area menu	Provides helpful information about files, folders, and troubleshooting.	Understand the Data Guardian Notification Area Menu Items

Install Data Guardian Interactively on Windows

You must be a local administrator to install Data Guardian. If users will install the product, inform them of the location of the installation media.

Before you begin

Depending on the environment and Data Guardian product, determine which of these you need:

Hosted Dell Security Center	On-prem Dell Management Server
If your hosted environment is multi-tenant, you will need an Installation ID.	Be sure you know the name of the Dell Server.

Install Data Guardian

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, and copy it to the local computer. Here are sample installer names:
   - Hosted Dell Security Center - installer names have an .exe extension
   - On-prem - installer names have:
     - .exe extension
     - .msi extension for Workspace ONE and an MSI installation
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++ 2017 Redistributable Package or Microsoft .NET Framework 4.7.2 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\Data Guardian\`.

   Do not install Data Guardian in the `C:\Users` or `C:\Windows` folders or at the root of any drive.
10. Select one of these:

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software. a. Select **Hosted Dell Security Center**. b. Optionally, if your enterprise is multi-tenant, enter an Installation ID. **NOTE:** **If your enterprise is multi-tenant and you do not enter an Installation ID, you can enter it when you activate or the administrator can add it to the Registry later.** c. Click **Continue**. d. Continue with step 11.	An on-prem Server located within the enterprise network for managing Dell Data Security software. a. Select **On-prem Dell Management Server**. b. In the *Dell Management Server Name:* field, enter the Dell 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. **NOTE:** **Do not clear the *Enable SSL Trust Verification* check box unless your administrator instructs you to do so.** c. Click **Next**. d. In the Confirm Dell Management Server Information screen, confirm that the Dell Server URL address is correct. The installer adds www or http(s) and the port. Click **Next**. e. Continue with step 11.

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

    A status window displays the installation progress.
12. Click **Finish** when the Installation Complete screen displays.
13. Click **Yes** to restart.

Installation of Data Guardian is complete.

14. Users must confirm activation. The Data Guardian notification area icon should have a green check mark  .

NOTE:

Depending on the way Data Guardian is deployed within the enterprise, activation may not be immediate. However, if activation does not occur, the user must manually activate.

Possible Issues With Activating

If you have installed Data Guardian, but the Data Guardian icon in the notification area does not have a green checkmark  , be aware of the following depending on whether you have cloud encryption, protected Office, or both:

Data Guardian option	Possible issue
Protected Office	• Data Guardian may convert existing Office documents to protected mode before you activate. If so, when you open an Office document, a cover page displays with information on how to activate.

Do one of these:

- Reboot and log back in with a UPN suffix, for example, user_name@domain.com.
- Confirm with your administrator whether or not you should select the *Enable SSL Trust Verification* check box when you installed Data Guardian.
- Contact your system administrator about having your computer configured to manually activate. See Activate Data Guardian.

Activate Data Guardian

Typically, Data Guardian auto-activates after you install and reboot. If your administrator tells you to manually activate, follow these steps:

1. Log in to Windows.

   In the notification area, a shield icon with an orange exclamation point displays.
2. Click the **Data Guardian** icon in the notification area and select **User Activation**.
3. Enter your domain email address and domain password, and click **Activate**.

   For a Hosted Dell Security Center (SaaS) environment, you may be prompted for the IID.

   After activation is complete, a green check displays on the Data Guardian notification area icon  .
4. Confirm your user mode status. Click the notification area icon and select **Details**.
5. At the top, confirm User Mode:

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

NOTE:

If User Mode lists Unregistered, your Data Guardian is not yet activated.

Hosted Dell Security Center and Suspended Tenant

With Hosted Dell Security Center, if a tenant fails to make payments for a specified period of time, that tenant can be suspended. This applies to Windows, Mac, mobile, and web portal.

Internal and external users of Data Guardian may experience the following:

- All platforms - If you try to install Data Guardian, activate, or log in, a dialog displays stating that the tenant is suspended.
- Mac – If your tenant is suspended while Data Guardian, the suspended tenant dialog displays after you close Explorer and all files and then try to open a protected file.
- Web portal:
  - If already logged in and you upload an encrypted file, a message states Upload failed.

- If an encrypted or unencrypted file has been uploaded and then the tenant is suspended, a Download failed message displays.
- If you log out and try to log in again, a dialog displays stating that the tenant is suspended.

External users with access to some keys may also see a message that the tenant is suspended.

Contact your administrator.

Understand the Data Guardian Notification Area Menu Items

Details Screen

The Data Guardian Details screen provides helpful information, for example:

- For technical support, you can provide status or version information.
- To search for a file name, select Copy at the bottom right and paste the contents into a Word file.

To access the Details screen:

Right-click the **Data Guardian** notification area icon, and then click **Details**.

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

Service Status: Status of the Data Guardian Windows Service. Values are: Stopped, StartPending, StopPending, Running, ContinuePending, PausePending, Paused

Run State: The device activation state. Values are: Active, Reactivating, Suspended, Suspending

User Mode:

- **Internal user** - a user within this domain address
- **Unregistered** - a user whose Data Guardian is not activated

Registration Email: For Internal users, this is the domain email address.

Server URL: Dell Server that communicates with this client.

Policy Last Modified: Date and time stamp of when the policy was last modified and consumed by the client.

Policy Version: Policy version generated by the Dell Server.

The **Files** area of the Details screen displays files that are waiting to be encrypted and the following information:

Name: Name of the file

Cloud: This feature has been disabled so no longer has data.

File State: This value indicates the owner of the folder. Value is determined by the Key ID.

Processing State: Lists whether the file needs a key or is *Complete*.

Enterprise: Lists default server. If a message displays in this column, *Error: Key Not From Your Server*, the key does not belong to your enterprise's server. The key for an encrypted file must belong to your enterprise's server.

Key: Key ID assigned to that file (new files use that key for encryption).

Folder: The full path name of the folder.

Last Modified: The date the file was modified.

Persistence State: This indicates whether the file is on disk.

XEN File Read: This feature has been disabled.

Browser Created: *True* or *False*.

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

NOTE:

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

Previously, Data Guardian's Cloud Encryption had a **Folders** area of the Details screen. Currently, Cloud Encryption has been disabled.

Check for Policy Updates

If your administrator modifies a policy and notifies you of a policy update, go to the Windows notification area, click the **Dell Data Guardian** icon, and select **Check for Policy Updates**.

If your administrator modifies a policy to protect files created in Microsoft Word, you must close Word for that update to be applied.

Locate Log Files

For troubleshooting, your administrator may request log files.

To locate log files:

1. Navigate to `C:\ProgramData\Dell\Dell Data Protection\Data Guardian`.
2. Select **Xendow.Service.log**.

   NOTE:

   After Xendow.Service.log reaches 3 MB, it is saved as Xendow.Service1.log, then Xendow.Service2.log.

Upgrade Data Guardian

The best practice is to uninstall your previous version and then install the current version. See Uninstall Data Guardian.

For Data Guardian v2.8 and higher, external users are no longer supported. If an external user upgrades a v2.7 or earlier version, a dialog displays to inform them. Dell recommends that external users uninstall Data Guardian. External users can use the Data Guardian mobile client or web portal to view protected documents.

Uninstall Data Guardian on Windows

For internal users, if your administrator installed Data Guardian, only your administrator should uninstall the product.

For Data Guardian v2.8 and higher, external users are no longer supported. If you have Data Guardian v2.7 or earlier on an external computer, you should uninstall the product from that external computer.

Uninstall Data Guardian

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

Copy Files to Your Local Drive

If you uninstall Data Guardian from your computer or device, files on the cloud storage provider website still need to be secure so they remain encrypted.

1. Before you uninstall, determine if you need to access any files.
2. Copy those files to your local drive.

The folders and files on the cloud storage provider website will be encrypted, even if you download them. To view them, you must reinstall Data Guardian. Or, you can view them in the Data Guardian web portal or mobile device.

Uninstall Data Guardian

1. Use the Windows Control Panel to uninstall the program.
2. Select **Dell Data Guardian** and click **Uninstall** on the top menu.
3. Click **Next** when the Welcome screen displays.
4. Select **Remove** and click **Next**.
5. A warning displays to confirm Dell Data Guardian uninstallation. If so, click **Next**.
6. At Remove the Program screen, click **Remove**.

   A status window displays the progress.
7. If you get an error dialog from the sync client, click **Continue**.
8. If a dialog states you have an Office document open, click **OK**, close the Office document, and begin the uninstall again.
9. Click **Finish** when the Completed screen displays.
10. Click **Yes** to restart.

Uninstallation of Data Guardian is complete.

Provide Feedback to Dell

If your administrator enabled feedback, you can provide feedback to Dell about this product. The brief form includes two questions about your satisfaction level with a comment area and a rating scale (where 10 indicates the highest satisfaction level).

To access, click the Data Guardian icon in the notification area, and select **Send Feedback**.

If this feature is not enabled by policy, the option does not display.

4

Use Data Guardian with Windows

Your administrator has already configured policies to protect documents and will tell you which of these options apply to your enterprise.

Topics:

Overview of Options

This overview summarizes possible options for Data Guardian based on policy set by your administrator. These documents will be secure whether your data is in use, at rest, or in motion as you share them with others or store them on removable media.

Option	Description	For More Information
Basic File Protection	These are applications and file types that your enterprise wants to encrypt and your administrator has configured.	See Protect Non-Office File Extension Types with Data Guardian.
Office and macro-enabled documents	These include .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm, and .pdf.	See Protect Office Documents and PDFs with Data Guardian. You will have one of these modes: • Opt-in • Force-Protected
Content Based Protection	Used with Windows and opt-in mode.	See Content Based Protection.
Additional menu options	These may apply to Office documents, basic files, or both.	See Additional Options for Data Guardian.
Outlook Email and attachments		See Outlook Email.
Share a file with an external user	User who has a non-domain email address (either someone from a different enterprise or an internal user who wants to access protected files from a non-domain email address.	See Use Data Guardian as an External User. **NOTE:** **External users can only install Data Guardian on a mobile client or the web portal.**

Work Online with Protected Documents

When creating protected documents, the best practice is to work online because keys are generated for those documents. If your computer is re-imaged and you created protected documents offline, be sure to notify your administrator.

File Properties > Dell Data Guardian tab

With protected Office documents, you can right-click and select **Properties**. A **Dell Data Guardian** tab displays with information, such as the file's Key ID and access and embargo data.

Overlay icons for Windows

For Data Guardian 2.2 and higher, overlay icons display on protected files in File Explorer. If you right-click that protected file, a Dell Data Guardian tab provides more information.

NOTE:

If you open an Office document and a cover page displays with installation or activation information, your administrator may have set policies to protect Office documents. Confirm that Data Guardian is installed and activated. See Possible Issues With Activating - Cloud and Protected Office.

Protect Non-Office File Extension Types with Data Guardian

Your administrator will inform you if policies allow additional applications and file types to be encrypted. If an unauthorized person opens a file encrypted with Basic File Protection but does not have Data Guardian installed, the content is unreadable.

Overview of Basic File Protection

Applications

These are examples of applications that your administrator may want to encrypt:

- Notepad
- Wordpad
- Visio
- MS Paint

NOTE:

Some applications are only partially supported with Data Guardian, and your administrator will inform you of those.

File types

These are examples of additional file types that can be configured: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Basic File Protection and Windows

When the Basic File Protection policy is configured, Data Guardian sweeps users' computers and encrypts all local files with those extensions. Files encrypted with Basic File Protection can only be viewed and edited using the application associated with the file extension.

NOTE:

Files in specific system folders are not encrypted, such as AppData. Also folders that relate to protected Office documents, such as the Secure Documents folder.

Overlay icons for Windows

For Data Guardian 2.2 and higher, overlay icons display on protected files in File Explorer. If you right-click that protected file, a Dell Data Guardian tab provides more information.

Exclude some files from the sweep (before the sweep is enabled)

If your enterprise decides to encrypt an additional file type, like .txt, you may not want or need all files with that extension to be swept and encrypted.

Before enabling Basic File Protection for that extension, your administrator can set another policy that allows you to add a folder to your local computer and files in that folder are not swept. Your administrator can set a policy, create a folder name, provide the name of the folder, and suggest where you can add that folder. These may be files needed by your system or files that do not require protection.

NOTE:

You must create the folder before the administrator enables the Basic File Protection policy.

1. Use the folder name and path provided by your administrator.
2. Add files with the specified extension, like .txt, that do not need to be encrypted. Optionally, you can add subfolders with user-created names.

NOTE:

If you have files with that extension that were previously encrypted, placing them in that folder will not decrypt them. They remain encrypted. If you have an Unprotected Documents folder, which your administrator can create through another policy, you can place Basic File Protection types in this folder to decrypt them.

3. After Basic File Protection is enabled, if you have unprotected files with that extension on a network or external drive, you can copy those into the excluded folder. It remains unencrypted. Otherwise, they are encrypted.

If your computer has more than one user, only the current logged-in user can place files in that folder and have them excluded from the sweep. Any files that another user places in that folder will be swept and encrypted.

Removal of a file extension

Your administrator may decide to remove a file extension. If so, your computer is swept to decrypt those file types.

- The encrypted file's *Properties* > *Dell Data Guardian* tab no longer displays.
- If you had file overlay icons, those no longer display.
- The files may take several minutes to complete decrypting. If a file with that extension is still encrypted, it may have been open during the sweep or stored on a file server or other location.

Contact your administrator to request recovery of any files with that extension that will not decrypt.

Office applications

You can use an Office application to open a file encrypted with Basic File Protection but the content is read-only.

Protect Office Documents and PDFs with Data Guardian

To enhance enterprise security, your administrator may enable a policy to protect files for these Office applications:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm
- .pdf

If an unauthorized person accesses a protected file, the file remains encrypted, for example when you:

- Attach it to an email
- Move it in a browser - in some cloud sync clients, you can right-click a file name and select **Move**.
- Share it on the network
- Store it on removable media

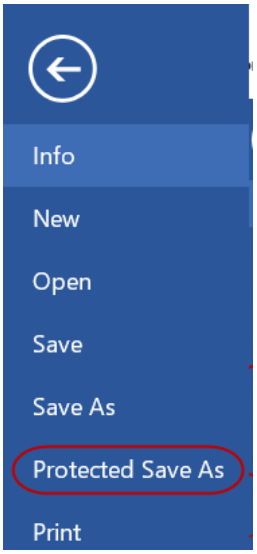
For Office documents, a cover page may display with instructions for installing or activating Data Guardian, for example:

- You need to install Data Guardian.
- You need to activate Data Guardian.
- You opened a protected Office document in the cloud.
- You downloaded an Office file from your computer that has Data Guardian to a personal device that does not have it.
- An unauthorized user accesses one of your Office files - The cover page displays with an enterprise-specific message, but the user cannot view the content of the file.

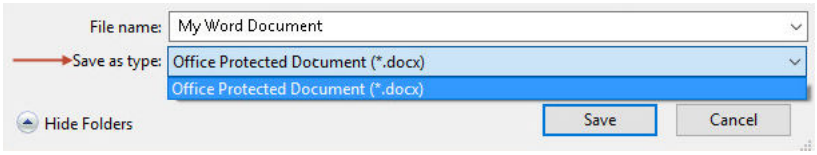
Observe File Menu Options

Protected Save As

To determine if your administrator has enabled Data Guardian policies, open an Office document and select **File**. If *Protected Save As* displays in the left pane, you have additional protection on Office documents.



If you select **Protected Save As**, the only option in the *Save as type* field is *Protected*.



File > Info

- *Add Date Restriction* displays if your administrator enabled that policy. See Enhance Security by Adding Date Restrictions.
- Properties information about this Office document, such as author and date, is hidden for greater security.
- Read-Only status: See below for more information.

NOTE:

The *Protect Document* option in File > Info relates to Microsoft Office not Data Guardian's Protected mode.

If you open an Office document and it indicates read-only mode, check the following:

- If *Protected Save As* does not display in the left pane, read-only is not related to Data Guardian policies.

Determine the Level of Security for Office Documents

To determine the level of security, observe options that are enabled or disabled:

- **Opt-in mode** - You have some options in determining which Office documents to protect.
  - **Documents > Secure Documents** folder - With Opt-in mode (but not Force-Protected mode), a Secure Documents folder is added to the root of the Documents folder. Office documents in this folder are encrypted. If you remove a protected Office document from this folder, it remains encrypted. If you rename the folder, the renamed folder's contents are encrypted. If you delete the folder, it is recreated.
- **Force-Protected mode** - Your enterprise requires a higher level of security.
  - With Force-Protected mode, policy also enables specific times for sweeping your computer to locate any unprotected Office files and change them to Protected mode. You must be logged in and be connected to the network for Data Guardian to sweep any unprotected Office files.
  - **Documents > Unprotected** folder - If enabled by policy in Force-Protected mode (but not Opt-in mode), an Unprotected folder is added to the root of the Documents folder. Office documents in this folder are decrypted. If you delete the folder, it is recreated.

Protect Office Documents and PDFs with Opt-in Mode

If your enterprise uses Data Guardian's Protected mode, see the following:

- Work with File Menu Options for Opt-in Mode
- Additional Options for Office Documents

Work with File Menu Options for Opt-in Mode

This table lists File menu options for Office documents.

NOTE:

Currently, embedded Office documents are not supported with protected Office mode.

File menu	Opt-in mode and Protected Office documents
Open	Files open as usual
Save	• Options: Already protected document - Saves as protected. Unprotected - Saves as unprotected. To protect it, click **Protected Save As**. • Read-only document - A dialog states you cannot save an unprotected document. A *Save As* window opens, and you must save it with a different file name.
Save As	Has the standard options (but not Protected mode)
Protected Save As	Only option in the Save as type field is *Protected (Documents, Presentation, Workbook, or PDF)*.
Share	**Enabled** for protected Office documents. If you share a protected Office document with an external user, they can only view it in a mobile device with Data Guardian or through the Data Guardian web portal. **Disabled** for unprotected documents.

Content Based Protection and Opt-in Mode

If this policy is enabled, your administrator can set rules for specific content, such as Social Security Number, credit card number, or other sensitive information. Your administrator will inform you which type of information will be protected. When you save a document that contains information based on those content rules, the document is encrypted.

If you use Tags in an Office document to trigger a classification used in the policy's file tag metadata, the tag you use in the Office document is case sensitive and must match the case used by your administrator in the policy.

NOTE:

If this policy is enabled, a sweep will cause files that meet the content rules to be encrypted. However, when you create the file, you can right-click and select Protect File.

See also Outlook email encryption.

Local Report for Protected Office Documents Encrypted with Content Based Protection (Opt-in Mode)

To protect sensitive information in Office documents and PDFs, your administrator may set a policy to sweep and then encrypt files based on Content rules. Sensitive information may include Social Security Numbers, credit card numbers, United States addresses, or enterprise-specific data. Your administrator will inform you of sensitive information that will cause your files to be encrypted.

To view a local report of files encrypted due to classification rules and the reason for that encryption:

1. Navigate to **C:\Users\<username>\AppData\Local\Dell\Data Guardian**.
2. Open the **Classification Report.log**.

   NOTE:

   If a file is in the process of being encrypted, the entry may have multiple lines until the encryption is complete.

TITUS Classification and Opt-in Mode

If a policy is enabled, your administrator configures some TITUS classifications to encrypt a document with that classification. You can right-click an unprotected Office document and select that TITUS classification. This provides another way to protect an Office document.

Determine Which Opt-in Mode Documents are Protected

If you have Opt-in mode and want to confirm if a document is protected or not, open the document and the title bar lists it as protected.

NOTE:

If you have Force-Protected mode, all Office documents are protected.

Protect Office Documents and PDFs with Force-Protected Mode

If your enterprise uses Data Guardian's Protected mode, see the following:

- Work with File Menu Options for Force Protected Mode
- Additional Options for Data Guardian

Work with File Menu Options for Force Protected Mode

This table lists File menu options for Office documents.

NOTE:

Currently, embedded Office documents are not supported with protected Office mode.

File menu	Force-Protected mode for Protected and Unprotected
Open	Unprotected documents are swept and encrypted. If your administrator enables the following by policy, you can create or add unprotected documents in these locations and open them in *Edit* mode: • *Unprotected Documents* folder at the root of your *Documents* folder • *Excluded* folder with a name given by your administrator
Save	• The document is protected. • Read-only document - You can edit it but cannot save the original. When you click Save, the Save As Protected window opens, and you must save it in Protected mode with a new name. • Remote documents - if you open a document in a remote location and it is not protected, you must save it to your local drive to modify and save. You cannot save to the remote location. **NOTE:** **Clicking Save opens a Save As window, and the only option in the Save as type field is Office Protected (Documents, Presentation, or Workbook).**
Protected Save As	Only option in the Save as type field is Protected.

Additional Options for Office Documents

Additional Menu Options for Protected Office Documents

The type of Office document, protected or unprotected, can affect the following.

Right click > Protect

You can right-click an Office document and select **Protect**. You must add content for the menu option to display. You cannot protect a blank document.

Open and edit a protected PDF with Adobe Acrobat Reader DC

When using Acrobat Reader DC:

- You can add annotations to a protected .pdf file or complete a form. When you save the file, a new protected .pdf file is created that includes the changes. This is Acrobat Reader DC functionality.
- To enhance security, when one protected .pdf file is open with Acrobat Reader DC, Internet access is blocked until Acrobat Reader DC is closed.
- To enhance security, if a protected .pdf is open, a user cannot email from that instance.

NOTE:

You cannot open a protected .pdf file from the network. You can use Word to open a protected .pdf file from the network.

Print for Envelopes and Labels

If your administrator has set a policy to add a watermark when you print a protected Office document, follow these steps to print envelopes or labels:

1. In a Word document, select the **Mailings** tab.
2. Select the **Envelopes** or **Labels** option.
3. After you enter the address or return address, click **Print**.

NOTE:

If you use another option to print and your administrator set a policy to add a watermark for printed Office documents, a watermark will display on your envelope or label.

Protect Outlook Emails and Attachments with Data Guardian

Attach a Protected Document to an Outlook Email

When attaching a protected document to an Outlook email, select **Insert** instead of *Insert as Text*. *Insert as Text* pastes the document content directly into the body of the email, and the content is no longer protected.

You can attach a protected Office document, additional protected file type based on policy, or a .xen file.

For Windows with Data Guardian, if you attach a protected document, Data Guardian appends information for accessing the encrypted file within that email.

- Internal users - Information displays with a link for downloading a client.
- External users - Information displays with a link for registering and downloading a mobile client or Data Guardian's web portal to view the document.

NOTE:

For the appended information to display, you must send the email from Microsoft Office Outlook, not the web-based version of Outlook.

Outlook Email Encryption with Data Guardian

Based on policy with Data Guardian v2.0.1 and higher, internal users have a *Protect* option in the upper left of Outlook to encrypt both email and attachments. Sender and receiver must both have Data Guardian installed and activated.

Data Guardian's Outlook email encryption is supported with Office 2013 and higher but not with web mail.

To use:

1. In the upper-left, click **Protect**.
2. For an external email address, click **Yes** to confirm key sharing or **No** if you decide not to send the email. See *For recipients of Outlook email* below.

The best practice is to have one email open at a time. If you have more than one opened, be sure to click the email to bring it into focus before clicking the Protect button. The Protect button should be gray when you do not hover over it.

For recipients of Outlook email

When opening an encrypted Outlook email, a warning displays that the document is protected and the user must double-click to open the file. No email content displays in the preview, only a cover page. The cover page lists either the Dell Server Name for on-prem or an Installation ID for that specific tenant if your Hosted Dell Security Center is multi-tenant. External users can a download the Data Guardian client for mobile or web portal to view the document.

- The cover page also includes links for internal users to download the Data Guardian client for Windows.
- External users can click links on the cover page to download and install Data Guardian on a mobile device or the Data Guardian web portal. The external user will have access to the key for the encrypted file that you shared.

Email classification

If your enterprise also enables a classification policy for Data Guardian and Outlook email, if any data specified in the classification policy, like Social Security Number or account number, is in the email, the email will be protected.

Tampering and Protected Office Documents

Data Guardian can scan protected Office documents to detect some forms of tampering.

If an internal user tampers with a protected Office document:

- Data Guardian can repair or restore some tampering.
- For tampering that cannot be repaired, a dialog may display notifying you that the file has been tampered with and to contact your administrator.

If an unauthorized user opens a protected Office document, only the cover page displays. If the unauthorized user modifies the cover page, Data Guardian restores the cover page when an authorized users saves it again as protected.

Share Protected Office Documents with External Users

With Data Guardian, you can share a protected Office document through email, removable media, a network share, or you can upload it to the cloud and share it:

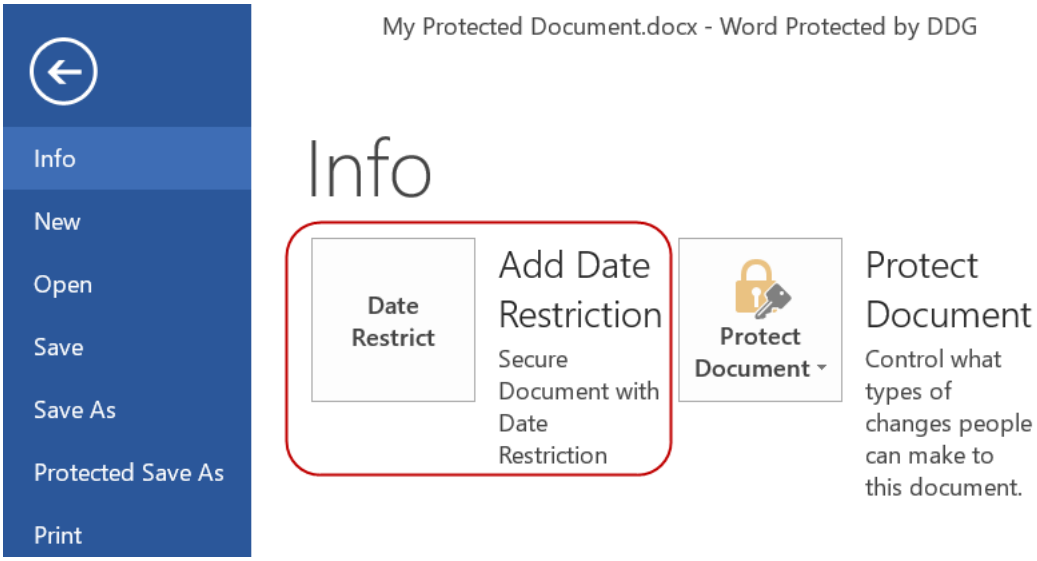
- All internal Data Guardian users can view it.
- Based on policy, external users can view it.

When you attach the document and click *Send*, a confirmation dialog displays reminding you that the key for that protected document will be shared with the external user.

Enhance Security by Adding Date Restrictions

Optionally, for enhanced security with external users, you can embargo a protected Office document or PDF by adding a date restriction to limit the amount of time that an external user can view it.

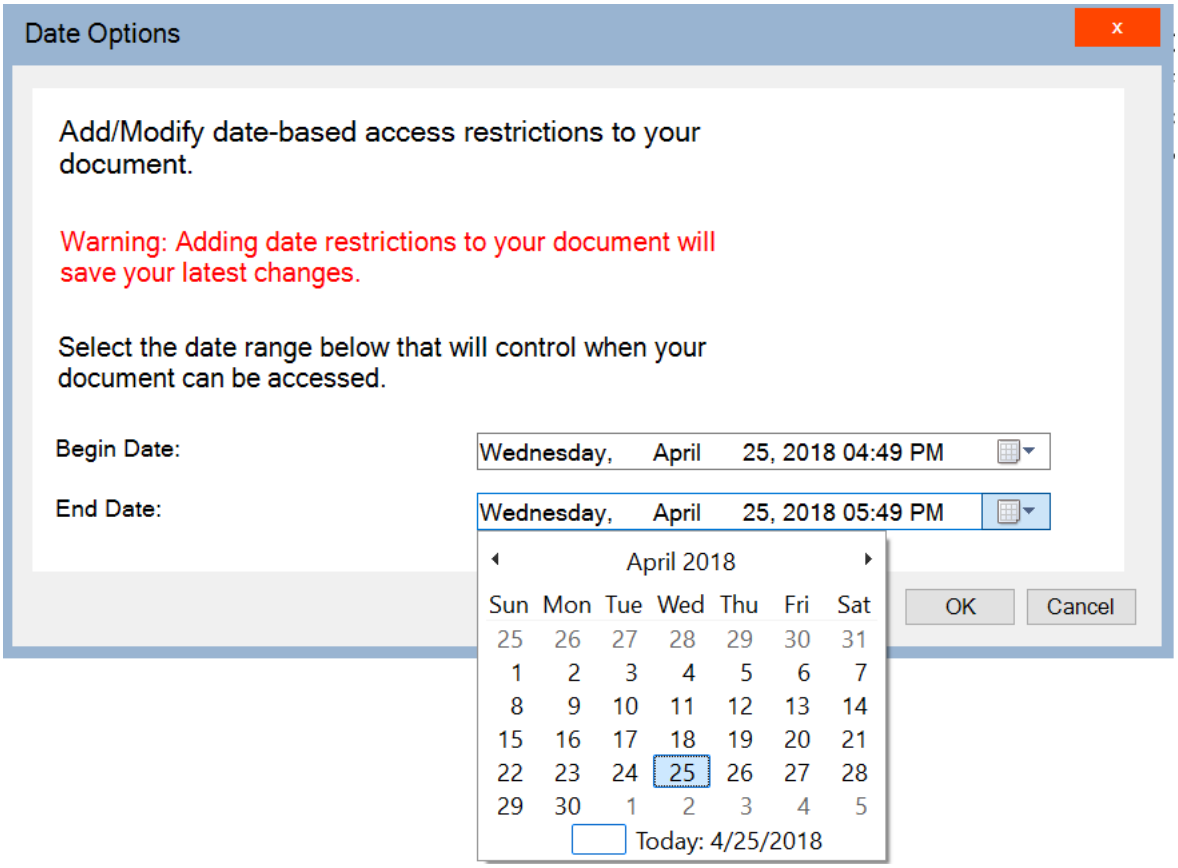
1. Right-click and select **Embargo**, or select **File > Info > Date Restrict**.



2. From the drop-down menu, select a Begin and End date and time for an external user to view the document.

NOTE:

The Begin date and time can be future if you want to send the document but prevent the external user from viewing it until the targeted date and time.



3. Click **OK**.

   The document is saved, protected, closed, and then reopened.

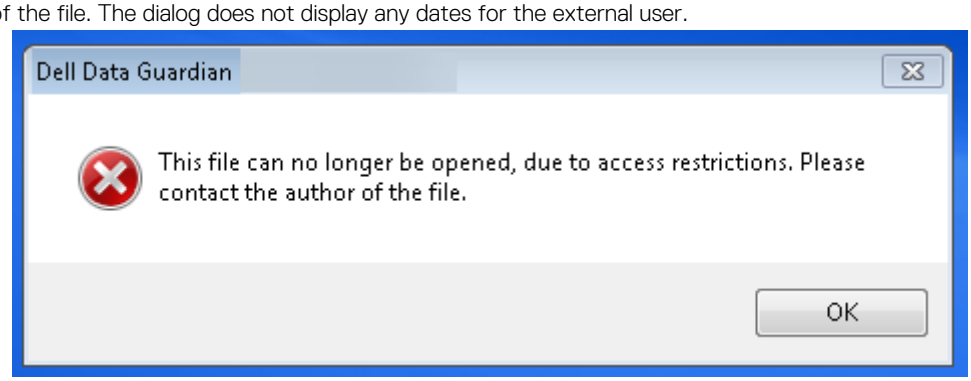
NOTE:

If you modify the dates for an unprotected Office document and then click Cancel, Data Guardian still protects the file.

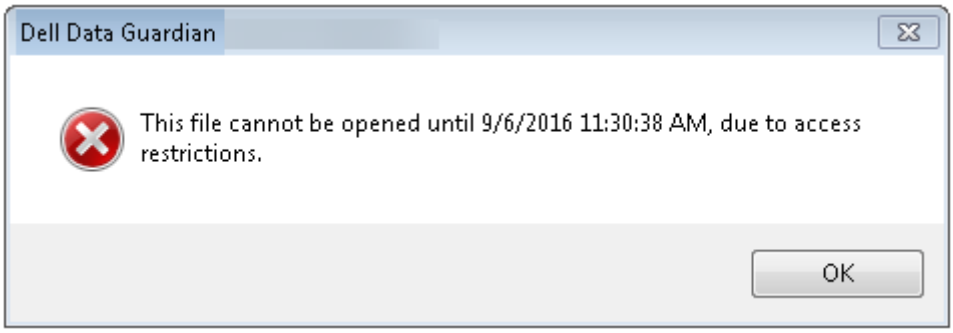
NOTE:

Currently, when adding date restrictions to a protected Office document and planning to save it to a network drive, you must save the file locally and then copy it to the network.

If an external user opens a file after the date and time range, a dialog states that the file has access restrictions and the external user can contact the author of the file. The dialog does not display any dates for the external user.



If you set the *Begin Date* field to a future date or time and the external user opens it prior to that time, a message explains that the file cannot be opened until that date and time due to access restrictions.


Dell Data Guardian
This file cannot be opened until 9/6/2016 11:30:38 AM, due to access restrictions.
OK

5

Install and Use Data Guardian with Mac

Data Guardian for Mac has embedded Help for specific screens that provides information on:

- Dell Data Guardian interface where users can upload files to encrypt them
- Cloud Encryption
- External users and access restrictions
- Tampering

Most of the user information about Data Guardian for Mac is within the software as online help. In the Dell Data Guardian interface for Mac, click the Help icon.

Topics:

Install Client for Mac

If your administrator has added you to your enterprise's whitelist, you can register at: https://yoursecurityservername.domain.com:8443/cloudweb/register.

After registering, you receive an email directing you to https://yoursecurityservername.domain.com:8443/cloudweb to log in and download the appropriate client.

You must be a local administrator.

To install Data Guardian for Mac:

1. For Data Guardian Client, locate the Installer in **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2. Use the **.pkg** file inside Dell-Data-Guardian-0.x.x.xxxx.dmg to install or upgrade.
3. Double-click the **Dell-Data-Guardian-x.x.x** package.
4. Click **Continue**.
5. On the Introduction window, click **Continue**.
6. On the Software License Agreement window, click **Continue**.
7. Click **Agree** to continue.
8. On the Configuration Type window, select one of these:

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.	An on-prem Server located within the enterprise network for managing Dell Data Security software.
a. Select **Hosted Dell Security Center**. b. Click **Continue**. c. Continue with step 9.	a. Select **On-prem Dell Management Server**. b. In the *Dell Management Server Name:* field, enter the Dell 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. c. Click **Continue**. d. Continue with step 9.

9. On the Installation Type window, do one of these:
   - Click **Install**, then go to step 10.
   - Click **Change Install Location**.
     a. On the Destination Select window, select all users. Currently, this is the only option.
     b. Click **Continue**.

c. Click **Install**, then go to step 10.

10. In the dialog, enter your user name and password and click **Install Software**.
11. On the Summary window, click **Close**.
12. When prompted, either keep the .pkg file or move it to *Trash*.
13. Do one of these:

Hosted Dell Security Center	On-prem Dell Management Server
The Credentials window automatically opens after you install. If your enterprise is multi-tenant, you will need an Installation ID. 1. In the Credentials window, enter your login account email and click **Continue**. 2. Do one of these: • If your enterprise is multi-tenant, enter an Installation ID, click **Continue**, and continue with step 3. **NOTE:** **If an error displays, check your credentials. If you notice an incorrect email address or Installation ID, click Restart Initialization to re-enter your Credentials.** • For single tenants, continue with step 3. 3. At the Microsoft window, enter your password and click **Sign in**. 4. In the Azure window, enter your password. 5. Click **Login**. **NOTE:** **If an error displays, check your credentials. If you notice an incorrect email address, click Restart Initialization to re-enter your Credentials.** 6. The Dell Data Guardian interface opens. See Dell Data Guardian application.	1. Close the .dmg window to open Finder. 2. See End User Activation.

NOTE:

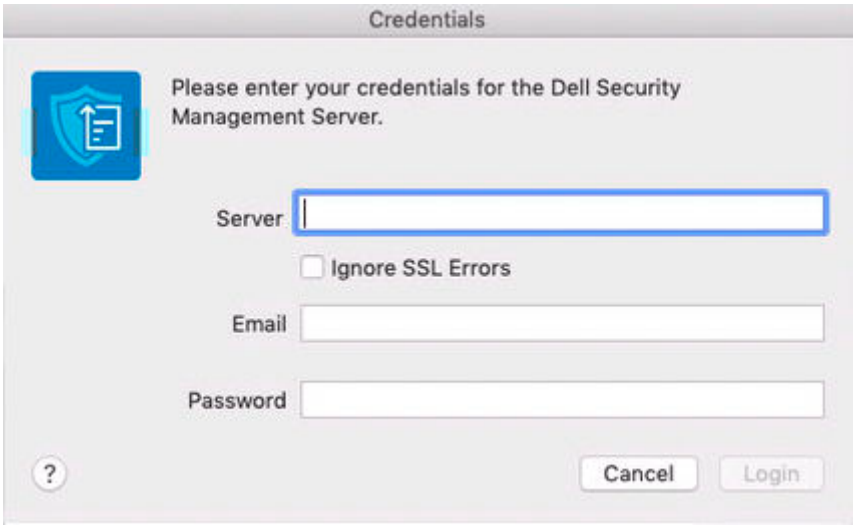
If the enterprise upgrades from Cloud Edition to Data Guardian, you must authenticate and re-link Data Guardian with their cloud storage provider. For more information on authentication, see the online Data Guardian Help.

End User Activation (On-prem)

Activation for On-prem Dell Management Server

With on-prem, after you open Dell Data Guardian for the first time, you must log in to activate:

1. In Finder, select **Applications**, and double-click **Dell Data Guardian**.
2. When the Credentials window opens, enter the Dell Server address, for example, company.server.com). This information is supplied by your administrator. By default, the port number is 8443. If your enterprise modifies the default port to a custom port number, your administrator will inform you.



NOTE:

Do not select the SSL Errors check box unless your administrator instructs you to do so.

3. Enter your email address and password.
4. Click **Login** to activate Data Guardian.
5. See *Dell Data Guardian application* below.

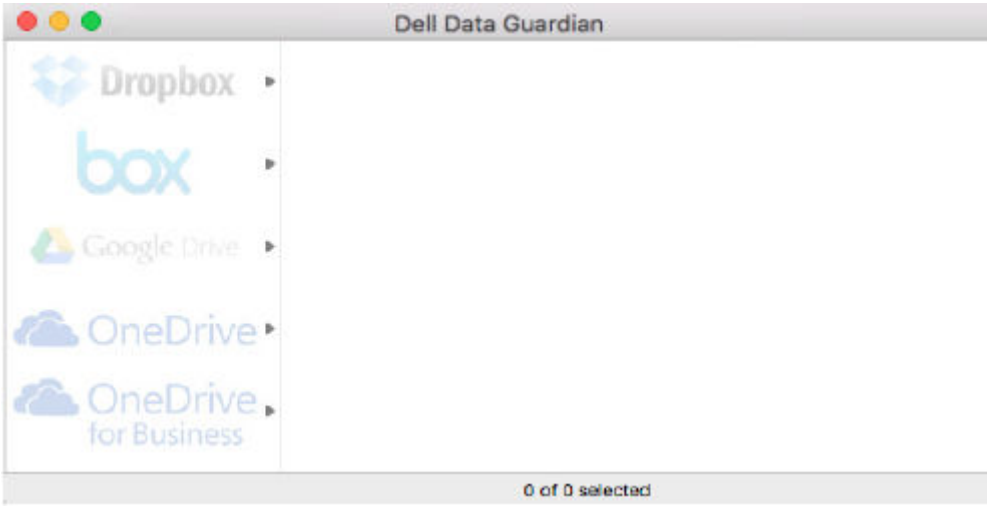
For more information on authentication, see the online Dell Data Guardian Help.

Dell Data Guardian application

When the Dell Data Guardian application opens and activation is successful, the faded cloud storage provider name displays in the left pane.

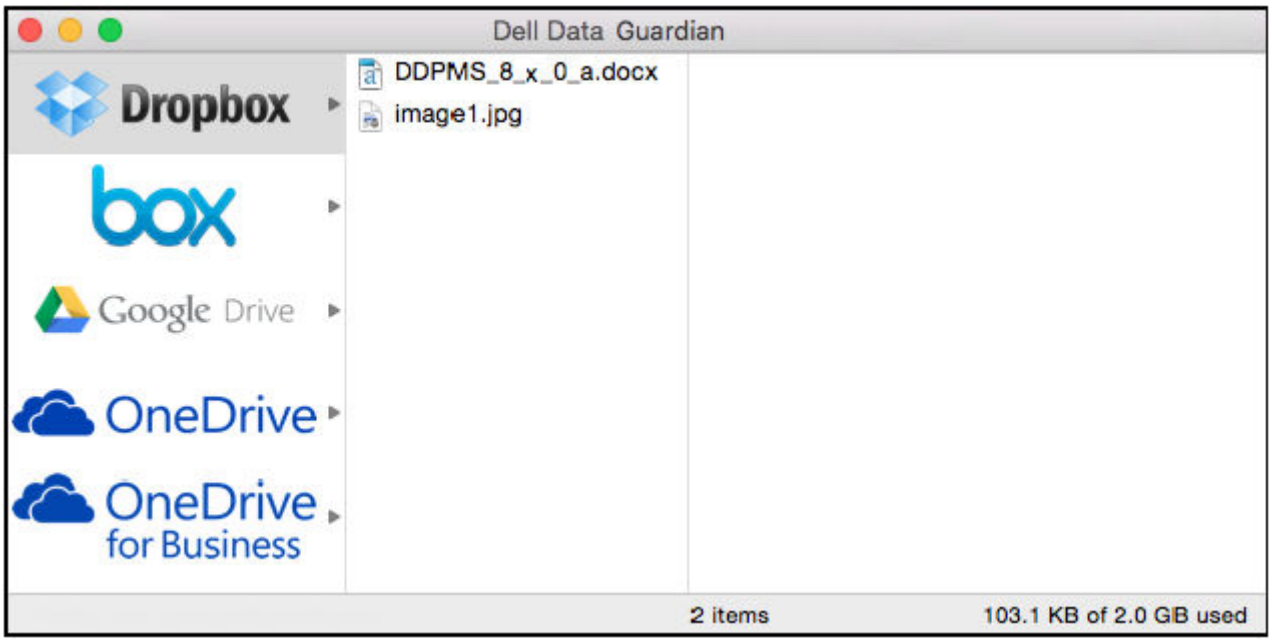
If an enterprise wants all users to collaborate using the same cloud provider, the administrator can set a policy to enable only that provider and to block the others from displaying.

If authentication for Data Guardian is revoked or expires, the cloud storage provider name is also grayed out.



1. In the left pane, select the cloud storage provider.
2. A window opens, prompting for your credentials. Enter your credentials.

   When authenticated, the cloud storage provider name is activated.



Hosted Dell Security Center and Suspended Tenant

With Hosted Dell Security Center, if a tenant fails to make payments for a specified period of time, that tenant can be suspended. This applies to Windows, Mac, mobile, and web portal.

Internal and external users of Data Guardian may experience the following:

- All platforms - If you try to install Data Guardian, activate, or log in, a dialog displays stating that the tenant is suspended.
- Mac – If your tenant is suspended while Data Guardian, the suspended tenant dialog displays after you close Explorer and all files and then try to open a protected file.
- Web portal:
  - If already logged in and you upload an encrypted file, a message states Upload failed.
  - If an encrypted or unencrypted file has been uploaded and then the tenant is suspended, a Download failed message displays.
  - If you log out and try to log in again, a dialog displays stating that the tenant is suspended.

External users with access to some keys may also see a message that the tenant is suspended.

Contact your administrator.

Protect Non-Office File Extension Types with Data Guardian

Your administrator will inform you if policies allow additional applications and file types to be encrypted. If an unauthorized person opens a file encrypted with Basic File Protection but does not have Data Guardian installed, the content is unreadable.

Overview of Basic File Protection

Applications

These are examples of applications that your administrator may want to encrypt:

- Notepad
- Wordpad
- Visio
- MS Paint

NOTE:

Some applications are only partially supported with Data Guardian, and your administrator will inform you of those.

File types

These are examples of additional file types that can be configured: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Basic File Protection and Mac

When the Basic File Protection policy is configured, Data Guardian sweeps users' computers and encrypts all local files with those extensions. Files encrypted with Basic File Protection can only be viewed and edited using the application associated with the file extension.

NOTE:

Files in specific system folders are not encrypted, such as AppData. Also folders that relate to protected Office documents, such as the Secure Documents folder.

Exclude some files from the sweep (before the sweep is enabled)

If your enterprise decides to encrypt an additional file type, like .txt, you may not want or need all files with that extension to be swept and encrypted.

Before enabling Basic File Protection for that extension, your administrator can set another policy that allows you to add a folder to your local computer and files in that folder are not swept. Your administrator can set a policy, create a folder name, provide the name of the folder, and suggest where you can add that folder. These may be files needed by your system or files that do not require protection.

NOTE:

You must create the folder before the administrator enables the Basic File Protection policy.

1. Use the folder name and path provided by your administrator.
   - For Mac, navigate to **Preferences pane > Basic File Protection Exclusions**. The folder name to create and path to display are here.
2. Add files with the specified extension, like .txt, that do not need to be encrypted. Optionally, you can add subfolders with user-created names.

   NOTE:

   If you have files with that extension that were previously encrypted, placing them in that folder will not decrypt them. They remain encrypted. If you have an Unprotected Documents folder, which your administrator can create through another policy, you can place Basic File Protection types in this folder to decrypt them.
3. After Basic File Protection is enabled, if you have unprotected files with that extension on a network or external drive, you can copy those into the excluded folder. It remains unencrypted. Otherwise, they are encrypted.

If your computer has more than one user, only the current logged-in user can place files in that folder and have them excluded from the sweep. Any files that another user places in that folder will be swept and encrypted.

Removal of a file extension

Your administrator may decide to remove a file extension. If so, your computer is swept to decrypt those file types.

- The encrypted file's *Properties* > *Dell Data Guardian* tab no longer displays.
- The files may take several minutes to complete decrypting. If a file with that extension is still encrypted, it may have been open during the sweep or stored on a file server or other location.

Contact your administrator to request recovery of any files with that extension that will not decrypt.

Office applications

You can use an Office application to open a file encrypted with Basic File Protection but the content is read-only.

6

Install and Use Data Guardian Mobile with iOS or Android

This section describes basic information on using Data Guardian Mobile with iOS or Android devices. When your administrator sets a policy to enable Data Guardian, files are encrypted and secure. The Data Guardian app must be installed on your mobile device to view or work with encrypted files.

Topics:

Prerequisite

Before you use the Data Guardian app, determine which of these you need based on your environment:

Hosted Dell Security Center	On-prem Dell Management Server
If your hosted environment is multi-tenant, you will need an Installation ID.	Be sure you know the name of the Dell Server, such as server.domain.com. This information is supplied by your administrator.

Get Started with Data Guardian Mobile

Follow this sequence as you use Data Guardian Mobile.

Task	Description	See this section
Install Data Guardian - Determine an option:	Administrator already installed User must install	Administrator installed: Tap the Data Guardian app and log in. User installs: See one of these: • Install on an iOS device • Install on an Android device
Determine which policies apply to mobile	Your administrator will tell you which policies apply.	You can have: • Protected Office Documents • Cloud Protection • Additional options
Navigate in File Manager	See Data Guardian options.	Navigate in File Manager

Task	Description	See this section
If Cloud Protection policy is enabled, access your cloud storage provider account	On the device, navigate to the File Manager screen of the Data Guardian app and tap your cloud storage provider.	See Access your Cloud Storage Provider account.

Based on Data Guardian policies, you can have:

- Protected Office files (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) retain their file extension.
- Additional applications and file types, such as .txt.
- Non-Office files in the cloud have a .xen extension.

On mobile devices with Data Guardian, you can:

- Create folders and files
- Delete folders and files
- Share a document with an external user (if the policy is enabled for external viewers)

Install or Uninstall Data Guardian on an iOS Device Through the App Store

Install on an iOS device

Prerequisite: If your device supports a Touch ID fingerprint scanner and you want to use that instead of a PIN, you must configure your device for Touch ID before installing Data Guardian.

1. On your device, tap **App Store** and search for **Data Guardian Mobile**.
2. Select and install the **Data Guardian** app.
3. Tap the checkbox to accept the license agreement.
4. Select one of these options:

Hosted Dell Security Center	On-prem
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.	An on-prem Server located within the enterprise network for managing Dell Data Security software.
a. Tap **Hosted Dell Security Center**. b. Enter your email. c. Tap **Submit**. **NOTE:** **If your email address is found on more than one tenant, type your Installation ID.** d. At the Microsoft Azure window, enter your password. e. Tap **Sign In**.	a. Tap **On-prem**. b. For the Server field at the login screen, enter the name of your company's Dell Server, such as server.domain.com. c. Enter your user name and password. d. Tap **Sign In**.

5. When prompted, either tap the fingerprint sensor or create a PIN.

Your account is now activated, and the Data Guardian File Manager screen displays.

Uninstall the Data Guardian app

1. In the iOS Apps drawer, tap and hold the **Data Guardian** icon.
2. Tap **x**.
3. Tap **Delete**.

Install or Uninstall Data Guardian on an iOS Device with Workspace ONE

If you have Workspace ONE installed, you can authenticate to Data Guardian with single sign-on. These steps are the same for Hosted Dell Security Center or On-prem Dell Management Server.

Your administrator will push the Data Guardian app to your device.

1. When prompted whether you want to install the **Data Guardian** app, tap **OK**.
2. Launch the **Data Guardian** app.
3. At the license agreement, tap **Accept**.
4. At the option to select Workspace ONE or Data Guardian, tap **Workspace ONE** to have single sign-on.
5. Enter your password.
6. When prompted, create a PIN.

   NOTE:

   If you sign in to Workspace ONE, you will only need to enter your PIN for Data Guardian.

Your account is now activated, and the Data Guardian File Manager screen displays.

Install or Uninstall Data Guardian on an Android Device Through Google Play

Install on an Android device

Prerequisite: If your Android device supports a fingerprint scanner and you want to use that instead of a PIN, you must configure your device for fingerprint support before installing Data Guardian.

1. On your device, access **Google Play** and search for **Data Guardian Mobile**.
2. Select and install the **Data Guardian** app.
3. Tap the check box to accept the license agreement.
4. Select one of these options:

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.	An on-prem Server located within the enterprise network for managing Dell Data Security software.
a. Tap **Hosted**. b. Enter your email. c. Tap **Submit**. **NOTE:** **If your email address is found on more than one tenant, type your Installation ID.** d. At the Microsoft Azure window, enter your password. e. Tap **Sign In**.	a. Tap **On-prem**. b. For the Server field at the login screen, enter the name of your company's Dell Server, such as server.domain.com. c. Enter your user name and password. d. Tap **Sign In**.

5. When prompted, either tap *Fingerprint Unlock* and select **Use Fingerprint**, or create a PIN.

   NOTE:

   You can modify this option in *Settings*.

Your account is now activated, and the Data Guardian File Manager screen displays.

Uninstall the Data Guardian app

1. In the Android Apps drawer, tap **Settings**.
2. In **Settings**, tap **Apps**.
3. Tap and hold the **Data Guardian** icon.
4. Drag the icon to the Uninstall option.
5. Tap **OK**.

Install or Uninstall Data Guardian on an Android Device with Workspace ONE

If you have Workspace ONE installed, you can authenticate to Data Guardian with single sign-on. These steps are the same for Hosted Dell Security Center or On-prem Dell Management Server.

1. On your device, tap **Hub**.
2. Tap **App Catalog**.
3. At the Dell Data Guardian app, tap **Install**.
4. At *Confirm Installation*, tap **Install**.
5. At *Google Play Protect*, tap **Allow**.
6. At the App installed message, tap **Done**.
7. Tap **Open** to launch the Data Guardian app.
8. At the option to authenticate with Workspace ONE or Data Guardian, tap **Workspace ONE** to have single sign-on.
9. At the license agreement, tap the checkbox.
10. Tap **Single Sign On**.
11. When prompted, create a PIN.

NOTE:

If you sign in to Workspace ONE, you will only need to enter your PIN for Data Guardian.

Your account is now activated, and the Data Guardian File Manager screen displays.

Uninstall the Data Guardian app

1. In the Android Apps drawer, tap **Settings**.
2. In **Settings**, tap **Apps**.
3. Tap and hold the **Data Guardian** icon.
4. Drag the icon to the Uninstall option.
5. Tap **OK**.

Navigate File Manager

In Data Guardian's File Manager, you can use local storage or the cloud. File Manager opens when you open Data Guardian.

File Manager screen

Default folders for the File Manager screen include:

- Documents
- Downloads
- Photos

Create New screen

Tap the Add (**+**) icon and the *Create New* screen displays with these options:

- Document
- Spreadsheet
- Presentation (PowerPoint)
- Photo
- Folder
- Cloud Service

Navigation drawer options

Tap the Navigation drawer icon. Options include:

- **Browser**
- **File Manager**
- **Settings** icon:
  - **Change PIN** button (if enabled by policy)
  - **Browser**
  - **File Manager (Settings)** - Use these options
    - **Refresh Interval** - How frequently Data Guardian syncs your cloud services. Dell recommends *Manual* or *Daily*. Other options are , *Hourly* or *Weekly*.
    - **10 MB download warning** - Enable or disable. Use this if you are not on Wi-Fi and the download size exceeds 10 MB.
    - **Clear cache** - Clears temporary files.

- (iOS) - **Touch ID** or **Face ID**, depending on the iOS version and if you have preconfigured fingerprint or facial recognition. Tap to enable or disable when using Data Guardian.
- (Android) - **Fingerprint Unlock**, if you have preconfigured Android's fingerprint feature. Tap to enable or disable when using Data Guardian.
- **About** - see Data Guardian policies and version
- **Exit Data Guardian** button
- **Cloud accounts** - Indicates whether they are Linked or Unlinked.

- **Browser**
- **File Manager** - To return to the File Manager screen.
- **Lock Data Guardian**

Additional options

- Add a file to Favorites
  - For iOS, see the navigation drawer.
  - For Android, press and hold the file name.

Determine Policies for Data Guardian Mobile

Your administrator will tell you which policies are set for your enterprise.

View Data Guardian policies and version

Some Data Guardian policies are listed in **About**. To view these policies or the Data Guardian version:

1. In the Data Guardian navigation drawer, tap **Settings > About**.
2. Tap **Policy**.
   Based on policies set by your administrator, the list may include:
   - PIN Length
   - Inactivity Time Out
   - Login Failure
   - Copy and Paste - Allows you to copy from a protected document to a protected document.

   Version
3. Determine additional policy options.
   These may include:
   - Protected Office documents
   - Cloud Protection
   - Additional policies

Use Protected Office Documents with Mobile

Your administrator will tell you which options are enabled for your enterprise. When you have Data Guardian installed and open a protected Office document, a message displays that the document is decrypting.

Data Guardian Options for Office Documents

These Data Guardian options display.

- **Create** - Based on the policy setting, the document is protected when you create it. The header of this file displays *Protected Document*.
- **Copy/Paste** - With a protected Office document, you can only copy to another protected Office document.
- **Print** - Based on additional policy settings, you may have a watermark when you print.
- **Export** - Based on additional policy settings, you may have a watermark when you export.

When an Office document is open, tap the icon in the upper left for these options:

- **Save**
- **Save as**
- **Export**

- **Exit**

Additional Office options based on policy:

- **Edit** - You can edit .docx and .ppt Office files.

  NOTE:

  Currently, .csv and .csv.xen files cannot be edited on mobile devices.
- **Hidden watermark** - Based on policy, protected Office documents may have a hidden watermark that identifies the user. If you print or share the document, the watermark persists.
- **Onscreen watermark** - When any protected Office document is open, a watermark displays on the client screen.

Additional information for Office documents

Protected Office Documents When Offline

When your create a protected Office document or protected macro-enabled document and are offline, a key is created for that document. When the device comes online, the keys are uploaded to the Dell Server. If a device is offline for three days, a notification states that Data Guardian has not been able to contact the Dell Server. The notification displays daily until you connect to the network. To view the encrypted files, the mobile device must be online.

Troubleshooting protected Office documents

On an iOS device, if you open a protected Office document greater than 25 MB and a low memory dialog displays, the warning is from Polaris Office, not Data Guardian. If the device has sufficient memory, close the file and reopen it.

Protect Non-Office File Extension Types with Data Guardian

Your administrator will inform you if policies allow additional applications and file types to be encrypted. If an unauthorized person opens a file encrypted with Basic File Protection but does not have Data Guardian installed, the content is unreadable.

Overview of Basic File Protection

Applications

These are examples of applications that your administrator may want to encrypt:

- Notepad
- Wordpad
- Visio
- MS Paint

  NOTE:

  Some applications are only partially supported with Data Guardian, and your administrator will inform you of those.

File types

These are examples of additional file types that can be configured: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Basic File Protection and mobile devices

Files encrypted with Basic File Protection can only be viewed and edited using the application associated with the file extension.

Office applications

You can use an Office application to open a file encrypted with Basic File Protection but the content is read-only.

Use Cloud Protection with Mobile

If your administrator enables Cloud Protection, you will need two apps:

- Cloud sync client app - See the online help for that cloud sync client.
- Data Guardian Mobile app lists the cloud sync client used with your company and allows you to download it.

If an unauthorized person accesses your cloud storage account and downloads a file to a mobile device that does **not** have Data Guardian installed, the person cannot open or view your files. If they open a protected Office document, only a cover page displays indicating that the person cannot view the document without Data Guardian. This makes your data more secure.

Access your Cloud Storage Provider account

To access a cloud storage provider account:

1. On the File Manager screen, tap the Add (**+**) icon.
2. Tap **Cloud Service**.

   A Data Guardian policy determines which cloud storage providers display. Your administrator may designate one or more specific cloud storage providers for use within the enterprise and block the others.
3. Do one of these by following the online instructions:
   - Create an account with the cloud storage provider.
   - Sign in to an existing cloud storage provider account.

     NOTE:

     For more information, see your cloud storage provider help.

NOTE:

If you download the cloud sync client app to your device, Data Guardian does not encrypt any folders or files that you upload directly from that app. To encrypt and protect files, you must use the Data Guardian app to upload them.

Use Cloud Protection

On mobile devices with Data Guardian, you can:

- Create folders
- Upload and download files

  NOTE:

  With Data Guardian, you must initiate upload and download on the device. For files to be encrypted when uploaded to the cloud, you must upload them from the Data Guardian Home screen, not a cloud sync client app. When you tap a file, Data Guardian automatically decrypts it and displays it in cleartext within the app. However, in the cloud, the file remains secure as a .xen file.
- Delete folders and files
- Accept a shared folder from an internal user

  NOTE:

  If an internal user shares a folder with you through Data Guardian, you must go to the cloud storage website and move it to the root folder or download the shared folder in order to view it on the device.
- **File > Copy** - Based on policy set by your administrator, you can copy a file from one cloud provider to another.
- For Android with OneDrive or Dropbox, if you are unable to share a file from Applications and the file shares a link with the Data Guardian app, then share the file from the File Browser app on the device.

Unlink a Cloud Storage Provider

If you have more than one account with the same cloud storage provider, you cannot be logged in to both at the same time. You must clear the check box to unlink and log out of the current account and then log in with the other credentials.

1. Open the Data Guardian navigation drawer and tap **Settings > File Manager > Cloud Service**. When you grant access to a cloud storage provider, a check mark displays in the check box.
2. Do one of these:

   Android

   a. Tap **Linked**.
   b. Tap **Yes**.

   iOS

   a. Tap **Unlinked**.

This removes access to and files from Data Guardian. However, this does not remove files from the cloud.

Troubleshooting Cloud Protection

With Dropbox for Business, if you mark a file as available Offline and then rename the file in the Dropbox website, the file will not open on the iOS device with the Data Guardian app.

Use Additional Policies with Mobile

Your administrator will tell you which of these policies have been set for your enterprise.

Use a PIN

Your administrator may set a policy requiring a PIN and setting its length.

Tampering

Data Guardian can scan protected Office documents to detect some forms of tampering.

Additional Protection Through Geofencing

Based on policies set by your administrator, mobile devices can have additional protection in that protected Office documents and .xen files cannot be opened outside a specific region. You must be in an approved region to open protected files. Currently, the regions are the United States and Canada. You must enable Location services on the device for geofencing to function. If the geofencing feature is enabled by your administrator and location services are set to Off, file access is denied.

Security Considerations with Data Guardian and Sync Clients

Data Guardian encrypts folders and files to make data secure. As Data Guardian works with sync clients, be aware of these considerations.

Google Drive

Google Drive contains a Google Docs app that allows users to collaborate on documents in real-time. However, the collaboration occurs on a Google server, not on the Dell Server. Therefore, the files are not encrypted. For Android and iOS devices with Data Guardian, access to these Google Docs is blocked. It differs slightly for each platform:

- Android
- iOS - A message is displayed.

NOTE:

***Google Backup and Sync* is not supported.**

OneDrive and OneDrive for Business

With OneDrive for Business, if you download several files and cancel the download, OneDrive for Business will cancel the ones that have not been downloaded but will continue with the one that is in process of downloading. This is a Microsoft issue. Therefore, allow the files to download completely before you cancel.

Logs

For security reasons, no log files are available on mobile devices.

Hosted Dell Security Center and Suspended Tenant

With Hosted Dell Security Center, if a tenant fails to make payments for a specified period of time, that tenant can be suspended. This applies to Windows, Mac, mobile, and web portal.

Internal and external users of Data Guardian may experience the following:

- All platforms - If you try to install Data Guardian, activate, or log in, a dialog displays stating that the tenant is suspended.
- Mac – If your tenant is suspended while Data Guardian, the suspended tenant dialog displays after you close Explorer and all files and then try to open a protected file.
- Web portal:

- If already logged in and you upload an encrypted file, a message states Upload failed.
- If an encrypted or unencrypted file has been uploaded and then the tenant is suspended, a Download failed message displays.
- If you log out and try to log in again, a dialog displays stating that the tenant is suspended.

External users with access to some keys may also see a message that the tenant is suspended.

Contact your administrator.

Send Feedback to Dell

If your administrator enabled a feedback policy, you can provide feedback to Dell about this product. If this feature is not enabled by policy, the option does not display.

To send feedback:

1. In the Data Guardian navigation drawer, tap **Feedback**.
2. The brief questions allow you to rank your satisfaction level (10 indicates the highest satisfaction level) and enter a comment.

7

View or Edit Protected Files on a Web Client

If your administrator sets up a Data Guardian web portal, you can link to a URL for that web client and view encrypted files without installing a Data Guardian client. Based on policy, you can also edit a file.

Based on policy set by your administrator, you can view the following:

- Protected Office documents: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- .xen files - Office or non-Office files that Data Guardian encrypted when uploaded to the cloud.
- Additional file types, such as Notepad.

Based on policy set by your administrator, you can access a cloud storage provider.

Topics:

Access the Web Portal for Data Guardian

Steps vary slightly depending on the browser you use.

1. From your administrator, obtain the URL for accessing the web portal.
2. Click the URL.
   If you get a warning, click **Continue** or **Proceed**.
3. At the license agreement screen, click **Agree**.
   If you get a warning, click **Continue** or **Proceed**.
4. Enter your domain credentials.
5. Click **Login**.
6. If prompted to track your location, select an option.
7. To view or edit files, see the online Help available from the Data Guardian web portal.

   NOTE:

   For Mac, you must configure Safari to allow pop-ups.

Protect Non-Office File Extension Types with Data Guardian

Your administrator will inform you if policies allow additional applications and file types to be encrypted. If an unauthorized person opens a file encrypted with Basic File Protection but does not have Data Guardian installed, the content is unreadable.

Overview of Basic File Protection

Applications

These are examples of applications that your administrator may want to encrypt:

- Notepad
- Wordpad
- Visio
- MS Paint

NOTE:

Some applications are only partially supported with Data Guardian, and your administrator will inform you of those.

File types

These are examples of additional file types that can be configured: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Basic File Protection and the web portal

In Settings > Policies, if Basic File Protection is set to True, your administrator has added non-Office file types that Data Guardian will encrypt when downloaded from the web portal. Your administrator must tell you the file types.

NOTE:

If you upload a file type that is not yet supported, the content is unreadable in the web portal.

You can upload non-Office file types whether encrypted or unencrypted. However, when you download the non-Office file, the file extension varies.

Non-Office files (like .txt or .png)	Download description
Encrypted before you upload Example: Non-Office files already encrypted by Windows or Mac.	When downloaded from the web portal, it maintains that file extension, like .txt or .png.
Unencrypted files	When downloaded from the web portal, the file extension varies based on whether your administrator added the extension to a policy. However, they are encrypted. Examples for a .txt file downloaded from the web portal: • **filename.txt** - Your administrator added the .txt file type to a policy. • **filename.txt.xen** - The .txt file type is not included in policy. The file is encrypted but adds a .xen extension.

If the *Edit* policy is enabled for web portal, users can edit the non-Office files.

Use a cloud storage provider

Based on policy, the web portal can access a cloud storage provider. For more information, see the web portal online help.

Hosted Dell Security Center and Suspended Tenant

With Hosted Dell Security Center, if a tenant fails to make payments for a specified period of time, that tenant can be suspended. This applies to Windows, Mac, mobile, and web portal.

Internal and external users of Data Guardian may experience the following:

- All platforms - If you try to install Data Guardian, activate, or log in, a dialog displays stating that the tenant is suspended.
- Mac – If your tenant is suspended while Data Guardian, the suspended tenant dialog displays after you close Explorer and all files and then try to open a protected file.
- Web portal:
  - If already logged in and you upload an encrypted file, a message states Upload failed.
  - If an encrypted or unencrypted file has been uploaded and then the tenant is suspended, a Download failed message displays.
  - If you log out and try to log in again, a dialog displays stating that the tenant is suspended.

External users with access to some keys may also see a message that the tenant is suspended.

Contact your administrator.

8

Use Data Guardian as an External User

An external user who has a non-domain email address can also use Data Guardian on a mobile client or the web portal. Here are some examples.

- You have installed and activated Data Guardian as part of your enterprise, but you need to share protected files or collaborate on protected files with a user outside your company.
- Your company email address is within the enterprise's domain, but you also want to install and activate Data Guardian on a mobile device with your personal, non-domain email address. This allows you to interact with your protected files from a non-enterprise domain email address.

External users must meet Server Requirements. Also, the domain or user must not be on the enterprise's blacklist.

For a hosted environment, external users can only activate against one tenant.

Options for external users include:

- **Mobile - iOS, Android, or Chromebook**
- **Web Portal** - Instead of downloading a Data Guardian client, use the Data Guardian web portal. External users can view a protected Office document .pdf or .xen file. If your administrator configures additional file types, like .txt or .png, you can view those in the web portal if they are encrypted. Based on policy, the external user can edit the file. See External User and Web Portal.

Topics:

Internal User Tasks on Windows

To share protected files with an external user, you can:

- Use the *Protected File Access* option with protected Office documents
- Approve or deny access when an external user requests access
- Send a protected Office document through an Outlook email.

Grant access to one or more protected Office files

For all files that you share with external users, you must grant access.

1. Right-click a protected file and select **Protected File Access**. You can select a single or multiple files up to 50. The Protected Document Access Sharing window opens. Files can be in these locations:
   - Local folder or network drive
   - Email
   - Removable media
   - Network share
2. At the top-right *Email to share* field, enter the email address of the non-domain user and click **Add**.
3. Repeat this step to add up to ten email addresses.
4. Click **OK**.

   A dialog states either that sharing was successful or that the email address is not authorized to receive protected files.
5. As a best practice, for external users who are not yet registered, inform them that they will receive an email from you with instructions that allow them to register with a Dell Server, download and activate Data Guardian, and then view shared protected files.

Approve or deny access when an external user requests access

An external user who has Data Guardian installed on a mobile device can request access to a protected document if they do not have a key for that document.

1. If you receive an email from an external user, requesting access to a protected document, you can view the name of the external user and the file requested.
2. Select **Approve** or **Deny**.

   An email is sent to the external user. If you approve, the key for the protected document is shared.

   If you are not available, your administrator also has the option to approve or deny access.

Send a protected file through Outlook email

When you attach a protected file and click *Send*, a confirmation prompt reminds you that the key to the protected file will be shared.

NOTE:

If an external user emails a protected file, the keys are not shared.

External User Tasks on Windows

An internal user may decide to give you access to protected files. You may receive the following:

- Email with instructions for registering on a mobile device or the Data Guardian web portal
- Protected file with a cover page that contains a link for registering a valid email address

  NOTE:

  The cover page lists either the Dell Server Name for on-prem or an Installation ID for that specific tenant if your Hosted Dell Security Center is multi-tenant. The cover page also includes links for downloading the Data Guardian client on mobile or the web portal.

To open and view a Data Guardian document, the external user must install Data Guardian on one of these:

- Mobile device (iOS or Android) - see External User and Mobile.
- Data Guardian web portal -see External User and Web Portal.

If an earlier version of Data Guardian is installed on Windows, you cannot upgrade to v2.8. Dell recommends that you uninstall Data Guardian from Windows. You must have administrator rights on your computer.

Request Access From an Internal User

With Mobile, if an external user has installed and activated Data Guardian, the user can request access of a protected Office document or .pdf from an internal user. The external user must make a separate request for each file.

1. If you open a protected Office document and it states that you need to request access, click **Yes** or **No**.
   A dialog states that the request was successfully sent. The internal user can approve or deny access, and the external user receives an email with the result. If the external user opens the protected file before the internal user approves access, a message displays that the request is pending.
2. After 48 hours, the external user can again request access.
   In the notification area, the external user can right-click the Data Guardian icon and select the **Details** page. Click the **Security** tab. When the time for a request returns to *None*, the external user can request access again.

External User and Mac Tasks

Internal User Tasks for Mac

Share a document with an external user:

- Protected documents - Send to the external user by email, network share, or removable storage.
- If Data Guardian's Cloud Encryption is enabled - In the Dell Data Guardian interface, drag protected files to the column next to the cloud storage provider column.

External User Tasks

A cover page displays for Office documents and PDFs.

For Data Guardian v2.8, and higher, you cannot upgrade or install Data Guardian as an external user. An error message will display.

To open and view a document already encrypted with Data Guardian, the external user must install Data Guardian on one of these:

- Mobile device (iOS, Android, or Chromebook) - see External User and Mobile.
- Data Guardian web portal -see External User and Web Portal.

Through those platforms, you can request that an internal user grant access to the keys of another file or to a file if the embargo date has expired.

NOTE:

For Hosted Dell Security Center (SaaS), Mac may allow an external user to upgrade to v2.8 or higher but an error message will display and the external user will not be allowed to activate.

If an earlier version of Data Guardian is installed, Dell recommends that you uninstall Data Guardian from Mac. You must have administrator rights on your computer.

External User and Mobile

If an internal user shares a link through the cloud to a protected file, the file displays a cover page that contains a link for registering a valid email address.

NOTE:

The cover page lists either the Dell Server Name for on-prem or an Installation ID for that specific tenant if your Hosted Dell Security Center is multi-tenant. The cover page also includes links for downloading the Data Guardian client.

To open and view a Data Guardian document, the external user must:

- Register with Data Guardian
- Download and install Data Guardian - the external user must have administrator rights on their computer.

Register Data Guardian

The first time that an internal user shares a file, the external user must register.

To register Data Guardian:

1. On the cover page warning, click the link provided to register a valid email address.
2. Follow one set of steps based on the environment of your enterprise:

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software. a. When the Dell Data Guardian web portal opens, enter your email address. b. Scroll down and click **Agree**. c. At the Dell Security Center window, scroll down to *Need an account?* and click **Sign up**. d. On the new account page, enter an email, a given name, family name, and password. The password must be at least eight characters and include a lowercase letter, uppercase letter, special character, and number. e. Click **Sign up**. f. Navigate to the email you used to register and retrieve the Verification Code, and enter it. **NOTE:** **If you do not see an email, check spam.** g. Click **Confirm account**. If you are verified, the web portal opens. h. Drag the protected file to the web portal, and click **Upload Now**. i. You will receive a Welcome email after registering. This email contains a link for downloading a Windows client. **NOTE:** **If your Hosted Dell Security Center is multi-tenant, the email also lists an Installation ID that you will need.**	An on-prem Server located within the enterprise network for managing Dell Data Security software. **NOTE:** **For on-prem, you can install Data Guardian before registering. When you activate, click the Register link.** a. When the Dell Data Guardian window opens, enter your email address. b. Click **Register**. c. At the Register page, enter and confirm your password, and then click **Sign In**. A Registration Confirmation dialog displays, and an email is sent to the address entered by the internal user. If you do not see the email, check spam. d. In the Account Verification email from the Dell Server, click the hyperlink. **NOTE:** **If you do not see an email, check spam.** e. Continue to the webpage. f. At the Confirmation page, click **Continue to Login**. g. At the Login page, click **Forgot Password**. **NOTE:** **The Dell Server has assigned a random password, which you must reset.** h. At the Reset Password Page, enter and confirm your password, and then click **Register**. A Registration Confirmation dialog displays, and an email is sent to the address entered by the internal user. i. Open the account activation email and click the link. The email also lists the Dell Server name to use when you install Data Guardian. j. On the Login page, enter the email address and password you used to register. k. Click **Login**. A Data Guardian Download page opens.

Download and Install Data Guardian for Mobile

Do one of these:

- Install or Uninstall Data Guardian on an Android Device
- Install or Uninstall Data Guardian on an iOS Device

External User and Web Portal

Internal User Tasks

An internal user can do one of these:

- Send the external user the enterprise's URL for accessing the Data Guardian web portal.
- Send a protected file to the external user. When the user opens the file, a cover page displays.

The external user can only view protected Office document .pdf files and .xen files or edit files based on policy. However, the external user does not have to download a Data Guardian client.

External User Tasks for Web Portal

To register for Data Guardian Web Portal:

1. Click the web portal URL, either received from an internal user or on the cover page of a protected file.
2. At the license agreement screen, scroll down, and click **Agree**.
3. Do one of these, depending on whether your enterprise is hosted or On-prem.

Hosted Dell Security Center	On-prem Dell Management Server
A hosted Software as a Service (SaaS) solution for managing Dell Data Security software. a. Enter an email and password. b. Click **Sign in**. c. Enter an email, a given name, family name, and password. The password must be at least eight characters and include a lowercase letter, uppercase letter, special character, and number. d. Click **Sign up**. e. Navigate to the email you used to register and retrieve the Verification Code, and enter it. f. Enter the Verification Code and click **Confirm Account**. The Web Portal opens.	An on-prem Server located within the enterprise network for managing Dell Data Security software. a. b. Click **Don't have an account yet?** c. Enter an email address and click **Register**. **NOTE:** **For internal users who want to register as an external, this is a non-domain email address.** d. On the Register page, enter and confirm a password, then click **Register**. The Confirmation page states that a confirmation email was sent to the email address you provided. e. To complete activation of the account, open the email titled *Account Verification* and click the link. f. On the Registration Confirmation screen, click **Return to Login**. g. Enter the email address and password you used to register.
If an internal user does not share the key, you can access the web portal but not open the file.	

4. The Dell Data Guardian Upload page opens.
5. Click **Browse** to navigate to the file and upload it, or drag and drop the file to the web portal.
6. Click **?** to view online Help for each page.

To edit files, an administrator must modify a policy for that user. If granted after you register, you must log out of the web portal and then log back in.

Optionally, you can download a Data Guardian client. The cover page includes links for downloading the Data Guardian client. The cover page also lists either the Dell Server Name for on-prem or an Installation ID for that specific tenant if your Hosted Dell Security Center is multi-tenant.

Request Access from an Internal User

If you upload a protected Office document or .pdf and an *Upload failed* dialog states that you do not have access, you can request access from the author of the file:

1. On the *Upload failed* dialog, click **Yes**.
2. Wait for an email from the internal user stating whether access was granted or denied.

NOTE:

If you do not receive an email from the internal user, you must wait 48 hours before requesting access again. If you open the protected file before the internal user approves access, a message displays that the request is pending.

View a Protected Office Document

If an enterprise activates a policy to protect Office documents and an internal user sends a protected file to an external user, the external user must be connected to the Dell Server when first opening the document. After that, they can open and view the document offline for a specified time, for example, one week. The external user must then connect to the Dell Server and reopen the protected document.

For security purposes, an external user cannot do the following with a protected Office document.

- Print
- Export

- Save As
- Share

Hosted Dell Security Center and Suspended Tenant

With Hosted Dell Security Center, if a tenant fails to make payments for a specified period of time, that tenant can be suspended. This applies to Windows, Mac, mobile, and web portal.

Internal and external users of Data Guardian may experience the following:

- All platforms - If you try to install Data Guardian, activate, or log in, a dialog displays stating that the tenant is suspended.
- Mac – If your tenant is suspended while Data Guardian, the suspended tenant dialog displays after you close Explorer and all files and then try to open a protected file.
- Web portal:
  - If already logged in and you upload an encrypted file, a message states Upload failed.
  - If an encrypted or unencrypted file has been uploaded and then the tenant is suspended, a Download failed message displays.
  - If you log out and try to log in again, a dialog displays stating that the tenant is suspended.

External users with access to some keys may also see a message that the tenant is suspended.

Contact your administrator.

9

Enhance Security with Data Guardian's Access Groups

Data Guardian's Access Groups enhance security by creating user groups that can collaborate on encrypted data. Users outside a group cannot access or view the data unless the owner of the file grants access. Access Groups can include internal and external users. You can use Access Groups with Windows, Mac, mobile, and web portal, either in an on-prem environment or hosted (SaaS).

Select one of these options based on your enterprise:

- Enterprise Has Data Guardian Installed with Opt-in Mode
- Enterprise Has Data Guardian Installed with Force-Protected Mode
- Enterprise Does Not Yet Have Data Guardian and Opt-in Mode
- Enterprise Does Not Yet Have Data Guardian and Force-Protected Mode

You can also do the following:

- Change the Owner of an Encrypted File
- Revoke Access to a Key

Topics:

Enterprise Has Data Guardian Installed with Opt-in Mode

If your enterprise uses access groups to enhance security for sensitive data, you need to know who is in your access group. Initially, to ensure a smooth transition, your enterprise may provide a brief period for processing any existing shared and encrypted files. After the transition period is complete, those in your access group can view any shared, encrypted files that you create. You can grant access to individuals outside your access group.

Identify those in your access group

Your administrator will inform you who is in one or more of your access groups, depending on who needs access to specific files. This can include internal and external users. If you work on sensitive data with specific users, you can request that your administrator create an access group for that content.

Use a transitional period to process shared, encrypted files

If you already have Data Guardian installed and existing files are encrypted, the best practice for your enterprise is to have a brief, transitional period for encrypted files that are shared. To facilitate a smooth transition, be aware of the following for shared, encrypted files:

- Owner or author of the file, whether internal or external, continues to have access to the file.
- Internal or external users within your access group have access to most of the shared files. Based on the type of key associated with some files, you may lose access to some.
- Internal users outside your access group - Users should open any shared files during the transitional period to gain access to the key. If they do not open a shared, encrypted file during this brief period, they lose access to the file.
- External users not in your access group - If you already granted access to an encrypted file, the external user will continue to have access during and after the transitional period.

If you lose access to a file after the transitional period, you can request access from the owner.

Regain access to shared, encrypted files after the transitional period

For Windows and Mac in Opt-in mode, you can do the following to regain access:

- Protected Office documents - A dialog prompts internal and external users to request access, and the owner of the file can decide whether to grant access.
- Additional file types encrypted through Basic File Protection - No post-share prompt exists. The user must know the owner of the file and right-click the encrypted file to find the Key ID on the Data Guardian tab. The user can send that information to the owner and request access.

Collaborate on new encrypted files after the transitional period

For new files that you create and encrypt after the transitional period:

- Internal or external users within your access group - Have access to all shared, encrypted files.
  - Anyone who is removed from the access group loses access.
  - If the owner of a file is removed from the group, other users still have access.
- Internal or external users outside your access group - Cannot view an encrypted file.
  - An internal user within the access group can grant access.
  - If an external user is the owner of an encrypted file, they can grant access to another individual.
  - If an internal or external user outside the group receives a protected Office document and tries to open it, a dialog prompts them to request access.
  - If an internal or external user outside the group receives and tries to open a file type from Basic File Protection, the user can right-click the encrypted file to find the Key ID on the Data Guardian tab and then send that information to the owner.

Enterprise Has Data Guardian Installed with Force-Protected Mode

If your enterprise uses access groups to enhance security for sensitive data, you need to know who is in your access group. Initially, to ensure a smooth transition, your enterprise may provide a brief period for processing any existing shared and encrypted files. After the transition period is complete, those in your access group can view any shared, encrypted files that you create. You can grant access to individuals outside your access group.

Identify those in your access group

Your administrator will inform you who is in one or more of your access groups, depending on who needs access to specific files. This can include internal and external users. If you work on sensitive data with specific users, you can request that your administrator create an access group for that content.

Use a transitional period to process shared, encrypted files

If you already have Data Guardian installed and existing files are encrypted, the best practice for your enterprise is to have a brief, transitional period for encrypted files that are shared. To facilitate a smooth transition, be aware of the following for shared, encrypted files:

- Owner or author of the file, whether internal or external, continues to have access to the file.
- Internal or external users within your access group have access to most of the shared files. Based on the type of key associated with some files, you may lose access to some.
- Internal users outside your access group - Users should open any shared files during the transitional period to gain access to the key. If they do not open a shared, encrypted file during this brief period, they lose access to the file.

- External users not in your access group - If you already granted access to an encrypted file, the external user will continue to have access after the transitional period.

If you lose access to a file after the transitional period, you can request access from the owner.

Regain access to shared, encrypted files after the transitional period

For Windows and Mac in Force-Protected mode, you can do the following to regain access:

- Protected Office documents - A dialog prompts internal and external users to request access, and the owner of the file can decide whether to grant access.
- Additional file types encrypted through Basic File Protection - No post-share prompt exists. The user must know the owner of the file and right-click the encrypted file to find the Key ID on the Data Guardian tab. The user can send that information to the owner and request access.

Collaborate on newly created files after the transitional period

For new files that you create and encrypt after the transitional period:

- Internal or external users within your access group - Have access to all shared, encrypted files.
  - Anyone who is removed from the access group loses access.
  - If the owner of a file is removed from the group, other users still have access.
- Internal or external users outside your access group - Cannot view an encrypted file.
  - An internal user within the access group can grant access.
  - If an external user is the owner of an encrypted file, they can grant access to another individual.
  - If an internal or external user outside the group receives an encrypted file and tries to open it, a dialog prompts them to request access.

Enterprise Does Not Yet Have Data Guardian and Opt-in Mode

If your enterprise plans to use Data Guardian with access groups to enhance security for sensitive data, the best practice is to identify any files that you share with internal or external users and find out if those users will be in any access group that your administrator creates for you. Initially, to ensure a smooth transition, your enterprise may provide a brief period for processing any existing shared files. After the transitional period is complete, those in your access group can view any shared, encrypted files that you create. You can grant access to individuals outside your access group so that you can collaborate with them but have greater security.

Identify those in your access group

Your administrator will inform you who is in one or more of your access groups, depending on who needs access to specific files. This can include internal and external users. If you work on sensitive data with specific users, you can request that your administrator create an access group for that content.

Use a transitional period to process shared files

When Data Guardian is installed, a sweep occurs on Windows or Mac and encrypts the following files if your administrator enabled a policy for them.

- Additional file types, such as .txt or .png, configured for Basic File Protection
- Content Based Protection files - previously *Data Classification* (Windows)
- TITUS Classification files (Windows)

If you already collaborate on files or share them with internal or external users, those users may or may not be in your access group. The best practice for a smooth transition is to have a brief, transitional period to process any of those encrypted files that are shared with other users. You must log in to your computer during this transitional period.

Be aware of the following if you want to continue sharing or collaborating on those files:

- For shared files listed above, the first person to log in and have their computer swept then becomes the owner of any shared files.
- If another person becomes the owner of the file and the original author is not in their access group, the original owner must request access from the new owner. The original owner can also request that the administrator change ownership.
- External users' computers are not swept so any copies of unprotected shared files are not swept and encrypted.
- If Data Guardian's Cloud Encryption is enabled and users share folders or files on a cloud storage provider, those files will also be swept.

Collaborate on newly created files after the transitional period

For new files that you create and encrypt after the transitional period:

- Internal or external users within your access group - Have access to all shared, encrypted files.
  - Anyone who is removed from the access group loses access.
  - If the owner of a file is removed from the group, other users still have access.
- Internal or external users outside your access group - Cannot view an encrypted file.
  - An internal user within the access group can grant access.
  - If an external user is the owner of an encrypted file, they can grant access to another individual.
  - If an internal or external user outside the group receives an encrypted file and tries to open it, a dialog prompts them to request access.

Enterprise Does Not Yet Have Data Guardian and Force-Protected Mode

If your enterprise plans to use Data Guardian with access groups to enhance security for sensitive data, the best practice is to identify any files that you share with internal or external users and find out if those users will be in any access group that your administrator creates for you. Initially, to ensure a smooth transition, your enterprise may provide a brief period for processing any existing shared files. After the transitional period is complete, those in your access group can view any shared, encrypted files that you create. You can grant access to individuals outside your access group so that you can collaborate with them but have greater security.

Identify those in your access group

Your administrator will inform you who is in one or more of your access groups, depending on who needs access to specific files. This can include internal and external users. If you work on sensitive data with specific users, you can request that your administrator create an access group for that content.

Use a transitional period to process shared files

When Data Guardian is installed, a sweep occurs on Windows or Mac and encrypts the following files if your administrator enabled a policy for them.

- Office documents
- PDFs
- Additional file types, such as .txt or .png, configured for Basic File Protection

The best practice for a smooth transition is to have a brief, transitional period to process any of those encrypted files that are shared with other users. You must log in to your computer during this transitional period.

Be aware of the following if you want to continue sharing or collaborating on those files:

- For shared files listed above, the first person to log in and have their computer swept then becomes the owner of any shared files.
- If another person becomes the owner of the file and the original author is not in their access group, the original owner must request access from the new owner. The original owner can also request that the administrator change ownership.
- External users' computers are not swept so any copies of unprotected shared files are not swept and encrypted.
- If Data Guardian's Cloud Encryption is enabled and users share folders or files on a cloud storage provider, those files will also be swept.

Collaborate on newly created files after the transitional period

For new files that you create and encrypt after the transitional period:

- Internal or external users within your access group - Have access to all shared, encrypted files.
  - Anyone who is removed from the access group loses access.
  - If the owner of a file is removed from the group, other users still have access.
- Internal or external users outside your access group - Cannot view an encrypted file.
  - An internal user within the access group can grant access.
  - If an external user is the owner of an encrypted file, they can grant access to another individual.
  - If an internal or external user outside the group receives an encrypted file and tries to open it, a dialog prompts them to request access.

Change the Owner of an Encrypted File

During the transitional period for access groups, if another user was designated as the owner of a shared, encrypted document that you authored originally, you can request that your administrator designate you as the owner.

Revoke Access to a Key

If you grant access of an encrypted file to an external user, the user has the key to open that file.

Optionally, if you no longer want the external user to have access to the file, you can ask your administrator to revoke the key. This applies only to external users.

Pre-share Protected Files on Windows

You must have Data Guardian installed and be assigned to one or more access groups.

If an internal or external user is not in your access group, you can pre-share a protected file.

1. Right-click a protected file, and select **Protected File Access**.
   In the *Protected File Access Sharing* UI, the document name displays in File Selected.
2. In *Email to Share*, click **Add** and enter a valid email address of an external user or an internal user not in your access group.
   You can add up to ten individual addresses at a time.
3. To modify an email address, click **Modify**.
4. To delete an email address, select an entry and click **Delete**.

   NOTE:

   The name of the file owner is indicated and cannot be selected or deleted.
5. In Available Groups, your access groups display. Select one or more groups and use the arrows to add to *Shared Groups*.
6. Click **OK**. A success message displays.

   NOTE:

   External users cannot share the protected document with another external user.

If this is the first time for an external user to receive a Data Guardian protected file, the user must install Data Guardian or use the web portal to view the protected file.

Pre-share Protected Files on Mac

You must have Data Guardian installed and be assigned to one or more access groups.

If an internal or external user is not in your access group, you can pre-share a protected file.

1. Right-click a protected file, and select **Protected File Access**.
   In the *Protected File Access Sharing* UI, the document name displays in File Selected.
2. In *Email to Share*, click **Add** and enter a valid email address of an external user or an internal user not in your access group.
   You can add up to ten individual addresses at a time.
3. To delete an email address, select an entry and click **Delete**.

   NOTE:

   The name of the file owner is indicated and cannot be selected or deleted.
4. In Available Groups, your access groups display. Select one or more groups and use the arrows to add to *Shared Groups*.
5. Click **OK**. A success message displays.

   NOTE:

   External users cannot share the protected document with another external user.

If this is the first time for an external user to receive a Data Guardian protected file, the user must install Data Guardian or use the web portal to view the protected file.

Pre-share Protected Files on iOS or Android

If an internal or external user is not in your access group, you can pre-share a protected file.

1. Tap a protected file.
2. **NOTE:**

   On the *Users* tab, the name of the file owner displays but cannot be selected or deleted. If you have already shared the file with internal or external users, those names display.
3. On the *Users* tab, to add the email address of an external user or an internal user not in your access group, click the plus icon (+) at the bottom right.
4. To delete an email address, swipe and tap **Delete**.
5. Tap the **Groups** tab to view your access groups.
6. Tap a group to share a protected file.

   NOTE:

   A checkmark indicates a group with whom you choose to share the protected file.
7. On the upper right, tap **Share**.
   A success message displays. External users cannot share the protected document with another external user.

If this is the first time for an external user to receive a Data Guardian protected file, the user must install Data Guardian or use the web portal to view the protected file.

Pre-share Protected Files on the Web Portal

If an internal or external user is not in your access group, you can pre-share a protected file.

1. In the web portal, upload a protected document.
   If your administrator has placed you in one or more access groups, a *Protected File Access* icon displays next to the Download icon.
2. Click the **Protected File Access** icon.
   In the *Protected File Access Sharing* UI, the document name displays in File Selected.
3. In *Email to Share*, click **Add New**.
4. Enter a valid email address of an external user or an internal user not in your access group and click the checkmark to save it. You can add up to ten individual addresses at a time.

   NOTE:

   To delete an email address, click X. The name of the person sharing the document is highlighted and cannot be selected or deleted.
5. In Available Groups, your access groups display. Either click **Select All** or click the arrow icon next to an option to add to *Shared Groups* or to remove.
6. Click **OK**.

   NOTE:

   External users cannot share the protected document with another external user.

If this is the first time for an external user to receive a Data Guardian protected file, the user must install the web portal.

Pre-share Protected Files as an External User

You must have Data Guardian installed and be assigned to one or more access groups.

If you are the originator or owner of a protected file, you can pre-share the file with an internal user. You cannot share the protected document with another external user. If you do not own the file, you cannot share it.

- The *Email to Share* does not list the names of other users with whom the protected documented has been shared.
- No groups display in Available Groups. You can only share with individuals.

1. Right-click a protected file, and select **Protected File Access**.
   In the *Protected File Access Sharing* UI, the document name displays in File Selected.
2. In *Email to Share*, click **Add** and enter a valid email address of an external user or an internal user not in your access group.
   You can add up to ten individual addresses at a time.

3. To modify an email address, click **Modify**.
4. To delete an email address, select an entry and click **Delete**.

   NOTE:

   As the owner of the file, you cannot select or delete your name.
5. Click **OK**. A success message displays.

If this is the first time for a user to receive a Data Guardian protected file, the user must install Data Guardian or use the web portal to view the protected file.

Request Post-Share Access to an Encrypted File

If you are not in an access group and you receive an encrypted file, you can use the post-share dialog to request access. The owner of the file will decide whether to grant access.

Post-share requests vary based on operating system and platform:

- Windows - Internal users can request access to:
  - Protected Office documents and PDFs
  - Any non-Office protected file extension types, like .pmg or .txt, configured by policy
- Mac - Internal users can request access to protected Office documents or PDFs.
- Mobile - Internal and external users can request access to protected Office documents or PDFs.
- Web portal - Internal and external users can request access to protected Office documents or PDFs.

Modify who has access to protected emails

Based on policy set by your administrator, you can right-click an email that you protected and sent to users in your Access Group. You can modify who has access to that email.

1. In Outlook, right-click an email labeled as [PROTECTED].
2. At the bottom, select **Protected Email Access**.
   A list displays of users with whom you have shared access.
3. Remove individual users if you no longer want them to have access to the protected email.

10

Frequently Asked Questions

Miscellaneous FAQs

Question

I renamed my computer. Now, I am not getting any policy updates.

Answer

Currently, the Dell Server only recognizes the endpoint against which you originally activated. If you change the endpoint name, the Dell Server does not recognize the location for sending the policy and Data Guardian does not perform as expected.

Solution

Uninstall Data Guardian and then reinstall. You must have administrator rights to uninstall.

Office Documents and Protected-Mode FAQs

Question

I tried to open an Office document (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm), and a cover page displayed.

Answer

If your administrator set a policy to protect Office documents, either you or your administrator must install Data Guardian. Confirm that the Data Guardian icon in the notification area has a green checkmark, indicating that it is activated.

Solution

Determine if you need to install or activate Data Guardian. See Install Data Guardian or Possible Issues With Activating.

Question

I cannot open a protected Office document (Word, PowerPoint, or Excel).

Answer

Check the following:

- File Block Settings - If your administrator sets policies to protect Office documents, do not use this setting in **File > Options**.

Solution

To check for File Block Settings:

1. In an Office document, select **File > Options**.
2. Select **Trust Center** from the list.
3. On the right, click **Trust Center Settings**.
4. Select **File Block Settings** from the list.
5. For *Word/Excel/PowerPoint 2007 and later Documents and Templates*, ensure that the *Open* check box is cleared.
6. Click **OK**.