

Dell Data Protection | Secure Lifecycle

User Guide v1.1



Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

© 2016 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, and Dell Data Protection | Secure Lifecycle suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Secure Lifecycle User Guide

2017 - 02

Rev. A01

Contents

1 Secure Lifecycle Introduction.....	5
Overview.....	5
Additional Support.....	5
2 Secure Lifecycle Requirements.....	6
Server.....	6
Encryption Client.....	6
Client Prerequisites.....	6
Windows Client Hardware.....	6
Operating Systems.....	7
Cloud Sync Clients.....	7
Web Browsers.....	8
3 User Tasks - Cloud Encryption and Protected Office.....	9
Overview of Tasks.....	9
Install Secure Lifecycle with Cloud and Protected Office.....	10
Pre-existing Folders with Unencrypted Files.....	10
Install Secure Lifecycle on Windows.....	11
Secure Lifecycle and Cloud Encryption.....	11
Install a Cloud Sync Client.....	12
Work with Folders and Files.....	14
View Folders and Files on the Local Computer and in the Cloud.....	14
Sharing a Folder with an Internal User.....	18
Use Office Documents with Secure Lifecycle's Protected Mode.....	19
Working without an Internet Connection.....	26
Character Limit for Folder Path Names.....	26
Dropbox for Business.....	26
OneDrive for Business/ Unified OneDrive.....	28
Dropbox.....	29
Box.....	30
Google Drive.....	31
OneDrive.....	32
Understand the Secure Lifecycle System Tray Menu Items.....	33
Manage Folders Menu.....	34
Check for Policy Updates.....	34
Locate Log Files.....	34
Upgrade Secure Lifecycle.....	35
Provide Feedback to Dell.....	35
Possible Issues With Activating - Cloud and Protected Office.....	35
Activate Secure Lifecycle.....	35
4 User Tasks - Protected Office without Cloud Encryption.....	37
Overview of Tasks.....	37



Install Secure Lifecycle for Protected Office.....	38
Install Secure Lifecycle on Windows.....	38
Use Office Documents with Secure Lifecycle's Protected Mode.....	38
Observe File Menu Options to Determine the Level of Security for Office Documents.....	39
Work with File Menu Options.....	41
Determine Which Opt-in Mode Documents are Protected.....	43
Additional Menu Options for Protected Office Documents.....	43
Tampering and Protected Office Documents.....	43
External Users and Protected Office Documents.....	44
Understand the Secure Lifecycle System Tray Menu Items.....	46
Manage Folders Menu.....	47
Locate Log Files.....	47
Check for Policy Updates.....	47
Upgrade Secure Lifecycle.....	47
Provide Feedback to Dell.....	47
Possible Issues With Activating - Protected Office.....	48
Activate Secure Lifecycle.....	48
5 Using Secure Lifecycle Mobile with iOS or Android.....	49
Prerequisite.....	49
Get Started with Secure Lifecycle Mobile.....	49
Secure Lifecycle on an iOS device.....	50
Troubleshooting iOS and Secure Lifecycle.....	51
Secure Lifecycle on an Android device.....	51
Security Considerations with Secure Lifecycle and Sync Clients.....	52
Logs.....	52
Send Feedback to Dell.....	52
6 Using Secure Lifecycle as an External User.....	54
Internal User Tasks.....	54
.....	55
External User Tasks.....	55
Activate Secure Lifecycle.....	56
View a Protected Office Document.....	57
7 Uninstall Sync Client or Secure Lifecycle.....	58
Uninstall a Cloud Sync Client.....	58
Uninstall Secure Lifecycle.....	58
8 Frequently Asked Questions.....	59
Miscellaneous FAQs.....	59
Office Documents and Protected-Mode FAQs.....	60



Secure Lifecycle Introduction

The *Dell Data Protection | Secure Lifecycle User Guide* provides the information needed to install and use Secure Lifecycle.

Overview

Based on policies set by an administrator, Secure Lifecycle protects data, for example:

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

 **NOTE:**

Your administrator will inform you if your enterprise uses Secure Lifecycle with cloud storage only, Office documents only, or both.

You can use Secure Lifecycle on the following platforms:

- Windows
- iOS
- Android
- Both this product and Secure Lifecycle for Mac can open files encrypted by the other.
 - This document covers Secure Lifecycle for Windows only.
 - For user information about Secure Lifecycle for Mac, refer to the online help within the software.

Additional Support

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



Secure Lifecycle Requirements

Client hardware and software requirements are provided in this chapter.

NOTE: IPv6 is not supported.

Server

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

Encryption Client

- Although the Encryption client is not required, any Encryption client used with Secure Lifecycle should be v8.12 or later.
- Secure Lifecycle is not supported with Microsoft Office 365.
- If running Office 2010 and your administrator enables policies to protect Word, PowerPoint, and Excel, you must have Office 2010 Service Pack 1 or higher (v14.0.6029 or higher). See <https://support.microsoft.com/en-us/kb/2121559> to determine whether a service pack has been applied to your Microsoft Office 2010 suite. Without this update, protected documents cannot be accessed.
- Secure Lifecycle does not support the Windows System Restore tool.

Client Prerequisites

If not already installed, the installer installs Microsoft Visual C++ 2010 SP1 Redistributable Package (x86 and x64).

Microsoft .Net 4.5.2 (or later) is required for Secure Lifecycle. All computers shipped from the Dell factory are pre-installed with .Net 4.5.2. However, if you are not installing on Dell hardware or are upgrading Secure Lifecycle on older Dell hardware, you should verify which version of .Net is installed and update the version, if needed, prior to installing Secure Lifecycle 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](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx).

Windows Client Hardware

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

Windows Hardware

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

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

Operating Systems

The following table details supported operating systems.

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

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

Android Operating Systems

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

iOS Operating Systems

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

Cloud Sync Clients

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

Sync Clients

- Dropbox
- Dropbox for Business (Windows only)

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

- Box

i | **NOTE: Box Tools and Box Edit are not supported with Secure Lifecycle. Using Box Tools may cause a blue screen condition.**

- Google Drive
- OneDrive
- OneDrive for Business




- Unified OneDrive

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

Web Browsers

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

 **NOTE:** Secure Lifecycle > Cloud Encryption does not support Microsoft Edge browser.



User Tasks - Cloud Encryption and Protected Office

Your administrator has already configured policies for Secure Lifecycle and will inform you if your enterprise uses Secure Lifecycle:

- To manage your cloud sync client
- To manage your cloud sync client plus additional protection on Office documents - If your enterprise only protects Office documents but does not manage a cloud sync client, follow the steps in [User Tasks - Protected Office without Cloud Encryption](#).



If your enterprise uses Secure Lifecycle with cloud storage:

- Before deploying Secure Lifecycle, see the online help for your cloud storage provider/cloud sync client to understand how your cloud storage application works. This document primarily explains how to use Secure Lifecycle.
- Typically, install and work with one cloud sync client. Your company may have a preferred cloud sync client and set a policy to allow you to use that one only.

Overview of Tasks

This overview summarizes the sequence for installing and using Secure Lifecycle.

Install Secure Lifecycle and a Cloud Sync Client

Task	Description	For More Information
If a cloud sync client is installed before Secure Lifecycle	Pre-existing folders and files that sync up to the cloud are not encrypted.  NOTE: Pre-existing folders and files that sync down from the cloud are encrypted.	See Pre-existing Folders with Unencrypted Files .
Install Secure Lifecycle	Determine the following: User must install Secure Lifecycle Administrator already installed Secure Lifecycle - continue to next step.	User installs: See Install Secure Lifecycle on Windows . Reboot and continue to the next step.
Confirm activation status	Confirm on the system tray that the Secure Lifecycle icon has a green checkmark  .	If the icon has an orange exclamation point, see Possible Issues With Activating - Cloud and Protected Office .
If policies protect documents in the cloud, install one cloud sync client	Business sync client or Basic sync client	Business Cloud Sync Client Accounts or Basic Cloud Sync Client Accounts



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 Secure Lifecycle is installed and activated. See [Possible Issues With Activating - Cloud and Protected Office](#).

Use Secure Lifecycle

Task	Description	For More Information
View the cloud sync client in File Explorer	After you install both Secure Lifecycle and a cloud sync client, a DDP SL virtual drive displays in File Explorer.	Work with Folders and Files Access Sync Client Folders and Files on Local Computer
Work with the cloud sync client on the DDP SL virtual drive	On the DDP SL virtual drive, you can add subfolders to the cloud sync client and then drag files or create files in those subfolders. After syncing, files are secure in the cloud: Office files can be opened but only a cover page displays; other files are encrypted as .xen files. However, on the local virtual drive, they are decrypted and display in cleartext. For more information, click the appropriate link for your cloud sync client.	Business account: Dropbox for Business OneDrive for Business/Unified OneDrive Basic account: Dropbox Box Google Drive OneDrive
View system tray menu	Provides helpful information about files, folders, and troubleshooting.	Understand the Secure Lifecycle System Tray Menu Items
Protect Office and macro-enabled documents, if policy is activated	Protect an Office document (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) when you create it. It will be secure when you share it with others or store it on removable media.	Use Office Documents with Secure Lifecycle's Protected Mode <ul style="list-style-type: none"> Observe File Menu Options to Determine the Level of Security for Office Documents Work with File Menu Options
Share a cloud folder with others to collaborate on files	Share a folder with: Internal user (has a domain email address) External user (has a non-domain email address) - work with your administrator.	Internal user - See the online help for your cloud storage provider. External user - See Using Secure Lifecycle as an External User .

Install Secure Lifecycle with Cloud and Protected Office

Pre-existing Folders with Unencrypted Files

Before deploying Dell Data Protection | Secure Lifecycle (DDP|SL), it is best if the target devices do not yet have a cloud storage provider account set up.

If you already have a cloud storage provider account with folders that are synced to your local computer and then install Secure Lifecycle:

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



If you want pre-existing files to be encrypted, navigate to the DDP|SL virtual drive, create a new subfolder within the cloud sync client and move the pre-existing files into that folder.

or


For large content, a manager or administrator can temporarily request the [Manage Folders Menu](#).

Install Secure Lifecycle on Windows

You must be a local administrator on the computer to install Secure Lifecycle.

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

Be prepared to restart your computer after Secure Lifecycle is installed.

- 1 To download the Secure Lifecycle installer, go to the location specified by your administrator.
- 2 Based on your operating system, select either the 32-bit or 64-bit installer, typically **setup32.exe** or **setup64.exe**, and copy it to the local computer.
- 3 Double-click the file to launch the installer.
- 4 If you get a Security Warning, click **Run**.
- 5 Select a language and click **OK**.
- 6 If prompted to install Microsoft Visual C++ 2010 Redistributable Package or Microsoft .NET Framework 4.0 Client Profile, click **OK**.
- 7 At the Welcome screen, click **Next**.
- 8 Read the license agreement, accept the terms, and click **Next**.
- 9 At the Destination Folder screen, click **Next** to install in the default location of **C:\Program Files\Dell\Dell Data Protection\Secure Lifecycle**.
On **C:**, do not install Secure Lifecycle in the Users or Windows folders or at the root of any drive. You will get an error.
- 10 In the *Server Name* field, enter the Server Name that this computer will communicate with, such as server.domain.com. You do not need to include www or http(s). This information is supplied by your administrator.
Do not clear the *Enable SSL Trust Verification* check box unless your administrator instructs you to do so.
- 11 Click **Next**.
- 12 In the Confirm Activation Server Information screen, confirm that the Server URL address is correct. The installer adds www or http(s) and the port. Click **Next**.
- 13 In the Management Type window, select this option:
 - Internal Use - A user with an email address within the company's domain.
- 14 Click **Install** to begin the installation.
A status window displays the installation progress.
- 15 Click **Finish** when the Installation Complete screen displays.
- 16 Click **Yes** to restart.
Installation of Secure Lifecycle is complete.
- 17 After you reboot, confirm on the system tray that the Secure Lifecycle icon has a green checkmark .

Secure Lifecycle and Cloud Encryption

If your enterprise set policies to protect data in the cloud and you already installed and logged in to a sync client, a DDP|SL virtual drive displays in Windows Explorer.

 **NOTE: Secure Lifecycle does not support unmounting the virtual drive.**

If you need to install and log in to a sync client, see [Install a Cloud Sync Client](#).



Install a Cloud Sync Client

Download and Install

Typically, an enterprise suggests that all users install the same cloud sync client. If applicable, use your company's preferred cloud sync client.

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

NOTE:

Currently, Secure Lifecycle does not support a sync client installed to a mount point.

1 Install either a business or basic cloud sync client:

- **Business Cloud Sync Client Accounts**

If your company offers a business account option, your administrator will provide you with a link for downloading and installing it. Options are:

- **Dropbox for Business** - If you install Dropbox for Business, you must also [Authenticate Dropbox for Business](#).
- **OneDrive for Business/Unified OneDrive** - For detailed steps, see <https://support.microsoft.com/en-us/kb/2903984>.

- **Basic Cloud Sync Client Accounts**

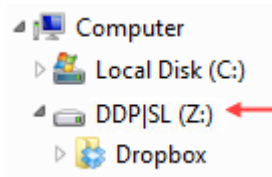
- **Dropbox** - see <https://www.dropbox.com/install>
- **Box Sync** - see <https://www.box.com/box-for-devices>
- **Google Drive** - <https://www.google.com/drive/download/>
- **OneDrive/Unified OneDrive (Windows 7 and 8)** - see <https://onedrive.live.com/about/en-us/download/>

On Windows 8.1 and higher, OneDrive is preinstalled. If you have Windows Updates enabled, Unified OneDrive replaces OneDrive.

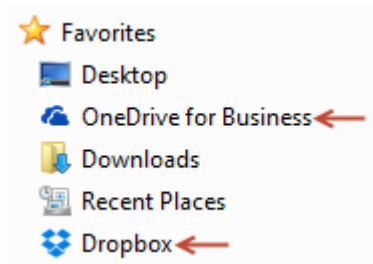
2 After you install and log in, the following display:

- In File Explorer, a DDP|SL virtual drive is added. The cloud sync client folder is added to this virtual drive. If you install more than one cloud sync client, each displays a folder on this drive.

NOTE: Secure Lifecycle does not support unmounting the virtual drive.



- In File Explorer > Favorites, a folder is added for your cloud sync client.



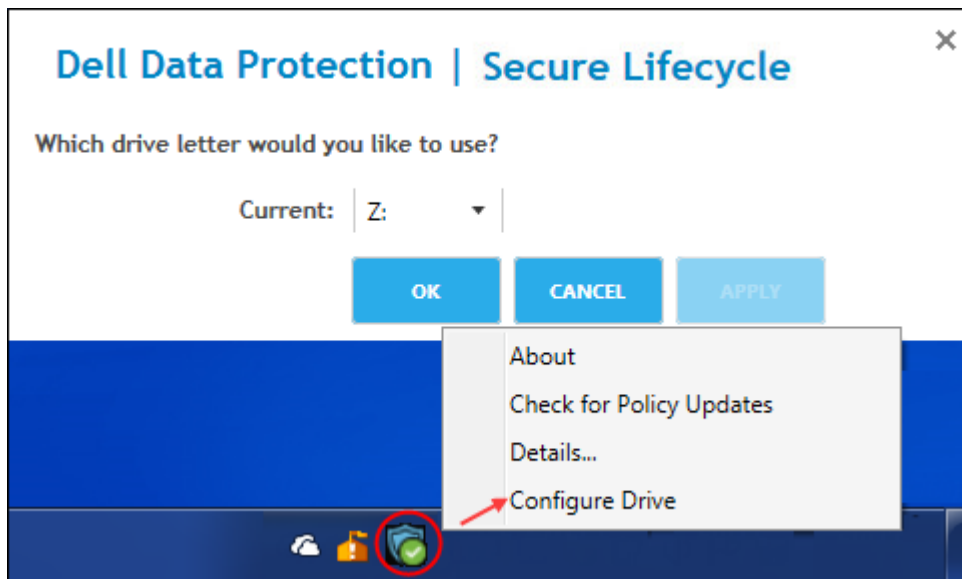
- In the system tray, the sync client icon displays.
- Depending on the cloud storage provider, a sync client shortcut may be automatically added to the desktop.
- With Opt-in mode only (but not Force-Protected mode) - a Secure Documents folder is added to the root of the Documents folder. See [Documents > Secure Documents folder](#).

Change the Virtual Drive Letter or Create a Shortcut

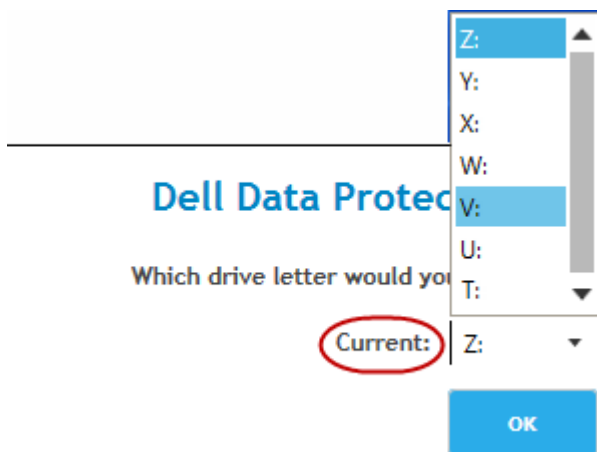
After you install Secure Lifecycle plus a cloud sync client, the DDP|SL virtual drive icon displays in File Explorer. The drive letter is assigned, using an available letter from the end of the alphabet.

To change the drive letter:

- 1 In the system tray, click the Secure Lifecycle icon and select **Configure Drive**.



- 2 Select an available letter from the *Current* list.



- 3 Click **Apply** or **OK**.

To add the DDP|SL virtual drive icon to the desktop, right-click the drive and select **Create shortcut**.

Authenticate Dropbox for Business

If you install Dropbox for Business, Secure Lifecycle prompts for authentication.

To authenticate:

- 1 After you install Secure Lifecycle, an Authentication window may open, or click the Secure Lifecycle icon and then select **Dropbox > Connect**.

The Authentication window notifies you that Secure Lifecycle must have access to your Dropbox account and may give instructions about business and personal accounts.

For the user, this provides context menu options. For the enterprise and your administrator, this is essential as it provides additional security measures.

- 2 At the Authentication window, click **Next**.



- 3 If a Network Threat Protection window opens, click **Yes**.
- 4 In the Authentication window, enter your domain email and Dropbox password.
- 5 Click **Sign In**.
- 6 If you have linked your Dropbox business and personal accounts, you will be prompted to select one now. You must select your business account.
- 7 Click **Finish** or wait for the window to close.

Work with Folders and Files

Secure Lifecycle works transparently with your cloud sync client. When your administrator sets a policy to enable Secure Lifecycle, files are encrypted and secure in the cloud when synced from your local computer.

Follow instructions in the cloud storage provider help to do the following:

- Create folders
- Upload/download folders and files

NOTE:

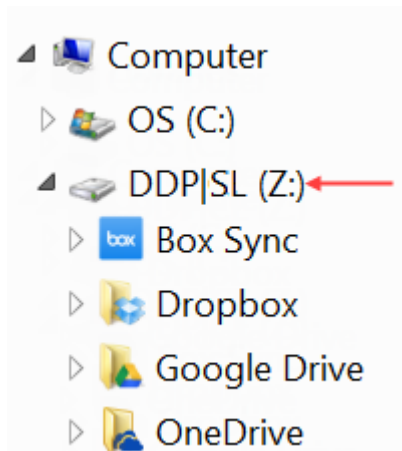
To upload files, copy or drag files to folders on the DDP|SL virtual drive. Secure Lifecycle does not support dragging files from your local computer to the web or creating files directly in the cloud storage provider's website.

- Use selective syncing of folders
- Share folders or files with internal users who have Secure Lifecycle. See [Sharing a Folder with an Internal User](#).
- Share folders or files with external users. See [Using Secure Lifecycle as an External User](#).
- Unshare folders

View Folders and Files on the Local Computer and in the Cloud

Access Sync Client Folders and Files on Local Computer

To access synced folders and files, click the **DDP|SL** virtual drive in File Explorer. Your cloud sync client displays.



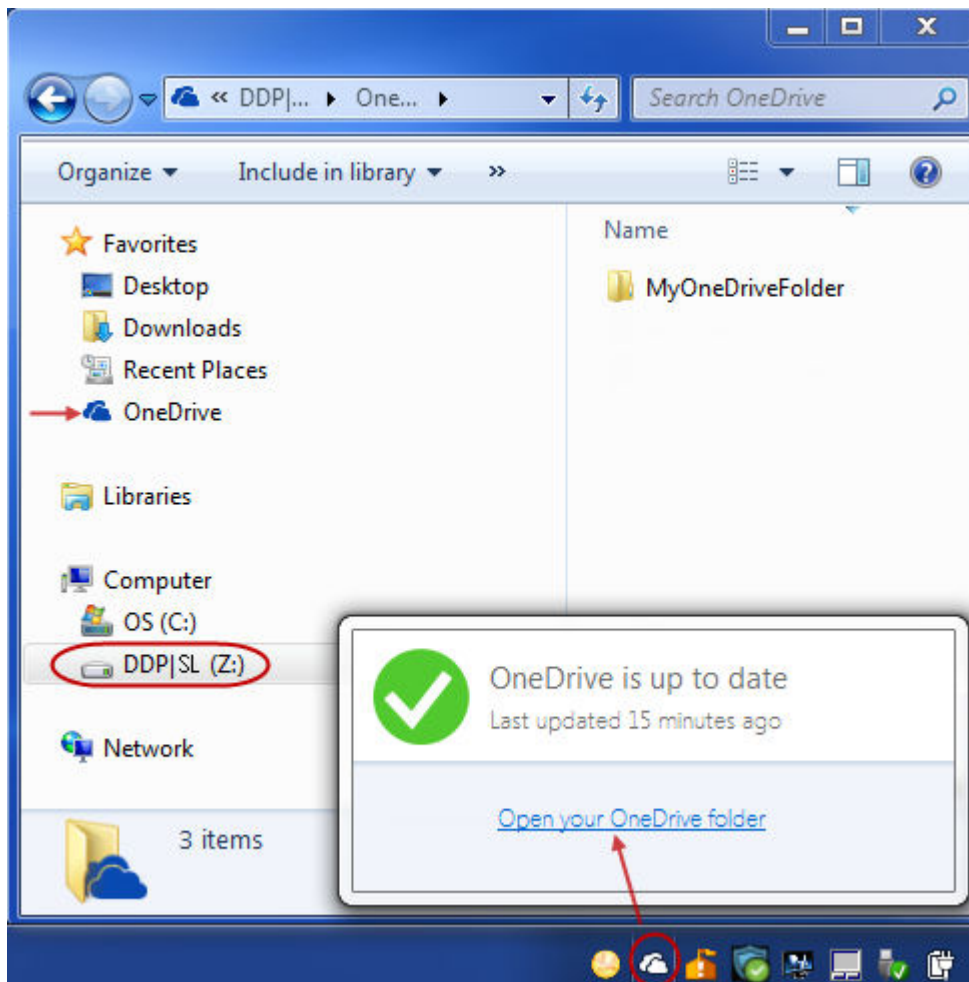
Here are other ways to access your cloud sync client.

- In the system tray, select the sync client icon and open the sync client folder. For more information, see the cloud storage provider help.



- In Favorites, click the sync client icon.

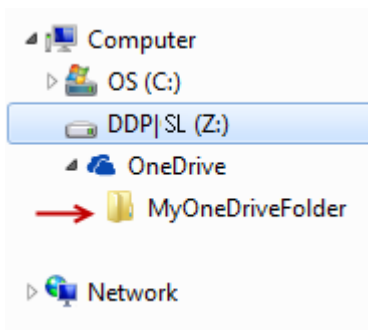
When you click the sync client icon in the system tray or in Favorites, note that the DDP|SL virtual drive is highlighted. Secure Lifecycle redirects you to this virtual drive, which allows you to view your locally decrypted folders and files in cleartext.



You can also access the DDP|SL virtual drive folders and files through a desktop shortcut. See [Change the Virtual Drive Letter or Create a Shortcut](#).

Add Folders

With Secure Lifecycle, you must add subfolders to the cloud sync folder. Do not add files at the root of the DDP|SL virtual drive.



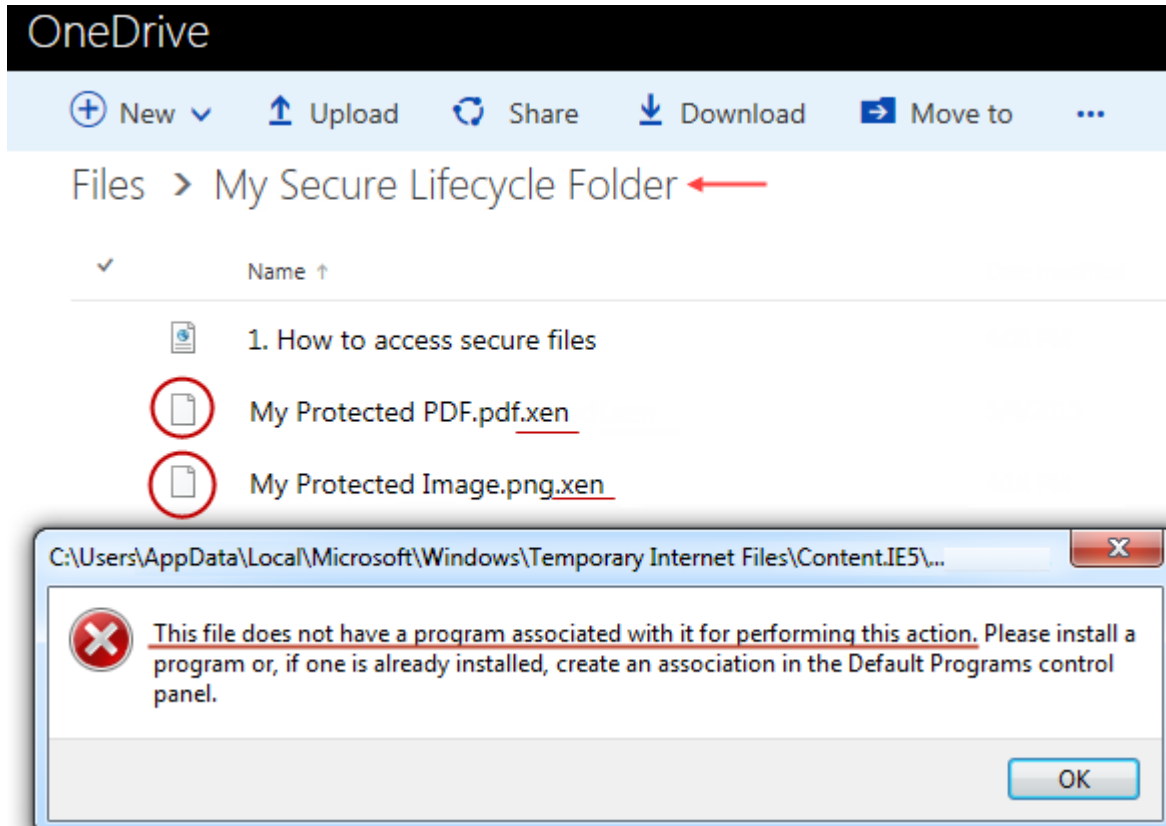
Add Files



When you add a file to a folder, Secure Lifecycle automatically adds a file to the folder on the web. Secure Lifecycle uses the `How to access secure files.html` file when you share a folder with external users. You do not need to open or download this file. See [Using Secure Lifecycle as an External User](#).

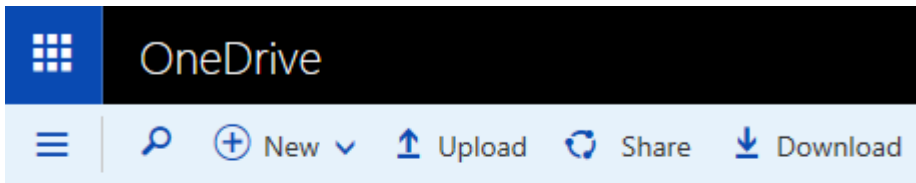
View Sync Client Folders and Files in the Cloud

Secure Lifecycle encrypts your data in the cloud, and filenames have a `.xen` extension. The icon by the file may differ for each cloud storage provider, but it does not display content. You cannot open files in the cloud. Therefore, if someone gains access to your cloud storage account, they cannot open or view your files. This increases security in the cloud. You can only view files in cleartext on the DDP|SL virtual drive.



Occasionally, when you download a `.xen` file to your desktop and it decrypts, a copy of the file with a `.xen` extension remains. You can delete the downloaded copy of the `.xen` file.

If your enterprise requires additional protection for folders and files in the cloud, your administrator can set a policy to obfuscate the filenames in the cloud and when downloaded. If someone gains access to your cloud storage account, they cannot open the files and they cannot read the filenames.



Files > Documents

✓	Name ↑
	43a94624-013f-5e9a-89b7-749b750ce074.xen ←

View Sync Client Folders and Files on a Local Computer with Secure Lifecycle and a Virtual Drive Installed

To make Secure Lifecycle easy to use on your local computer, when you open a folder on the DDP|SL virtual drive, files from the cloud are automatically decrypted and display in cleartext even though they are protected as encrypted files in the cloud.

Protect Folders and Files on Devices That Do Not have Secure Lifecycle

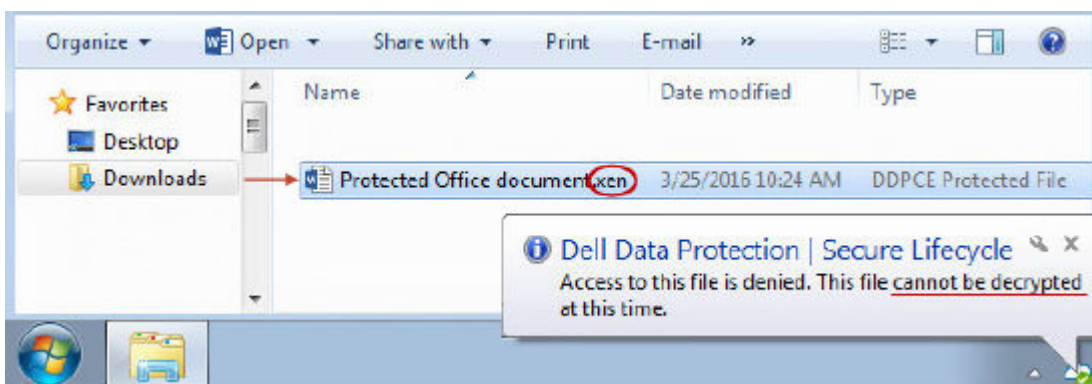
If an unauthorized person downloads a protected file from the cloud to a device does **not** have Secure Lifecycle installed, the person cannot access your data. Based on policies set by your administrator:

- Office documents - the document opens, but only a cover page displays with an enterprise-specific message.
- Non-Office documents - the file is downloaded as a .xen file. The person cannot open the file.

NOTE:

For internal users, if you download a file from a computer that has Secure Lifecycle to a device that does not, you cannot view that file unless you install Secure Lifecycle as an external user.

Occasionally, a .xen file may display on a computer that has Secure Lifecycle installed. For example, if the Internet connection was severed before the download was completed, the key may not be available to open the file. A dialog states that the file cannot be decrypted.



Secure Lifecycle does not allow edits to files without extensions. These files are treated as read-only files. To edit a file without an extension, download it from the cloud storage provider website, edit it, then upload it through the DDP|SL virtual drive.

Search File Names and Content on the DDP|SL Virtual Drive

If you want to search for file names or content on the DDP|SL virtual drive, you must enable Windows Search Indexing for that drive.



NOTE:

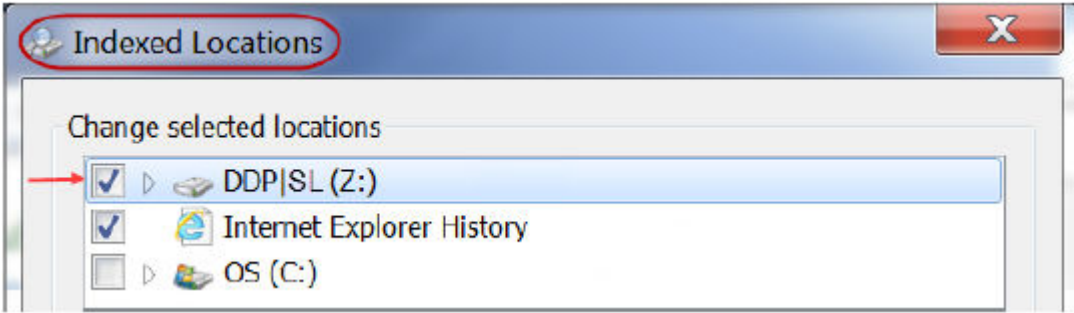
Windows Search Indexing is only enabled for the Users folders.

To enable Windows Search Indexing for the DDP|SL virtual drive:

- 1 In Control Panel, enter **Search Indexing** in the Search field.
- 2 Select **Indexing Options**.
- 3 In *Change selected locations*, select the check box for the DDP|SL virtual drive.

NOTE:

The remaining steps may vary depending on your operating system.



- 4 Click **OK**.
- 5 In Indexing Options, click **Close**.

You can now perform a search on the DDP|SL virtual drive.

Sharing a Folder with an Internal User

An internal user has an email address within your company's domain.

To share a folder with an internal user, you must access the website for your cloud storage provider and select **Share**. See the online help for the cloud storage provider.

Sharing a Folder using Secure Lifecycle and Box

On the Box website, select one of these options.

Box website option	Options	Description
Share	Available for folders and files	When the Share window opens, be sure Allow Downloading is set to Yes .
	View access	After downloading folders or files, those sharing must extract the zipped folder and then move folder and files to the DDP SL virtual drive.
Invite Collaborators	Available for folders	When the Invite window opens, you can select Editor or Viewer .
	View or Edit access	Those sharing can sync the folder to their computer, and it syncs to the DDP SL virtual drive.



Use Office Documents with Secure Lifecycle's Protected Mode

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

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

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 filename and select **Move**.
- Share it on the network
- Upload it to a cloud storage provider
- Store it on removable media

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

- You need to install Secure Lifecycle.
- You need to activate Secure Lifecycle.
- You open a protected Office document in the cloud.
- You downloaded an Office file from your computer that has Secure Lifecycle 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.

If your enterprise uses Secure Lifecycle's Protected mode, see the following:

- [Observe File Menu Options to Determine the Level of Security for Office Documents](#)
- [Work with File Menu Options](#)
- [Determine Which Opt-in Mode Documents are Protected](#)
- [Additional Menu Options for Protected Office Documents](#)
- [External Users and Protected Office Documents](#)

Observe File Menu Options to Determine the Level of Security for Office Documents

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

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

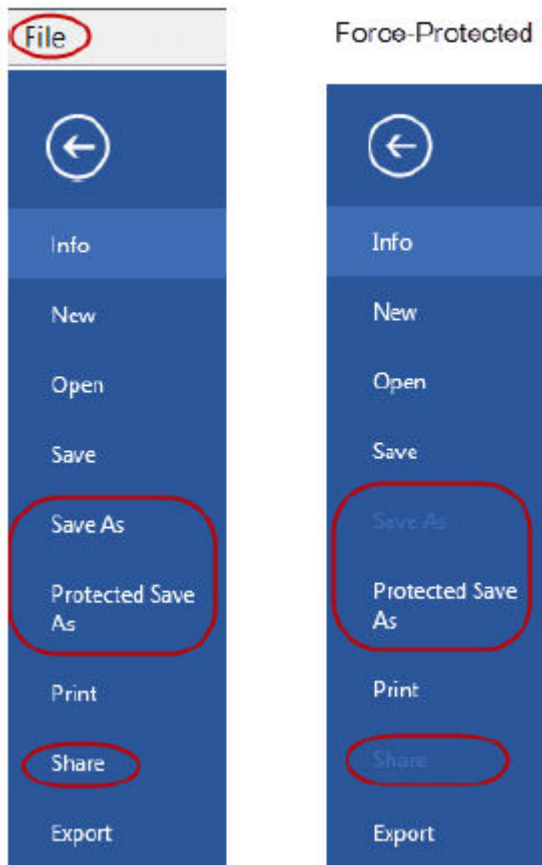
- **Opt-in mode** - You have some options in determining which Office documents to protect.
 - *Save As* and *Protected Save As* are enabled - If you opt to protect an Office document, select **Protected Save As**.
 - *Print* and *Export* may be enabled or disabled depending on policy.
 - *Share* (*Save and Send* for Office 2010) is enabled.
 - **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.
 - *Save As* is disabled and *Protected Save As* enabled - You must save all Office documents in Protected mode.
 - *Print* and *Export* may be enabled or disabled based on policy.



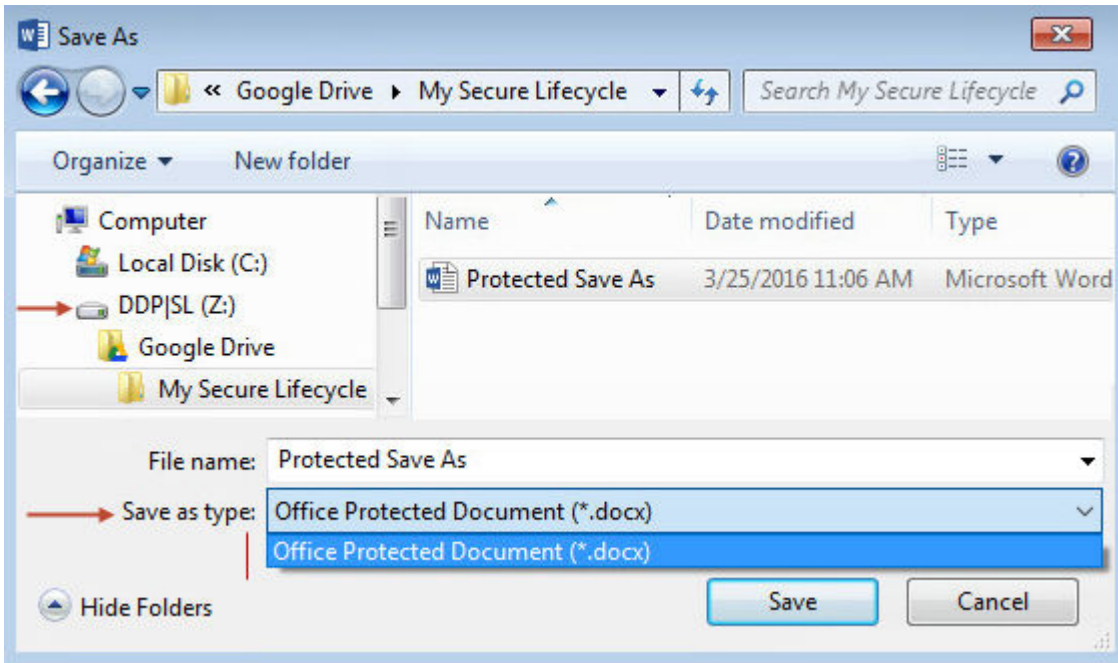
- *Share* (*Save and Send* for Office 2010) is disabled.

NOTE: 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 Secure Lifecycle to sweep any unprotected Office files.

Opt-in mode

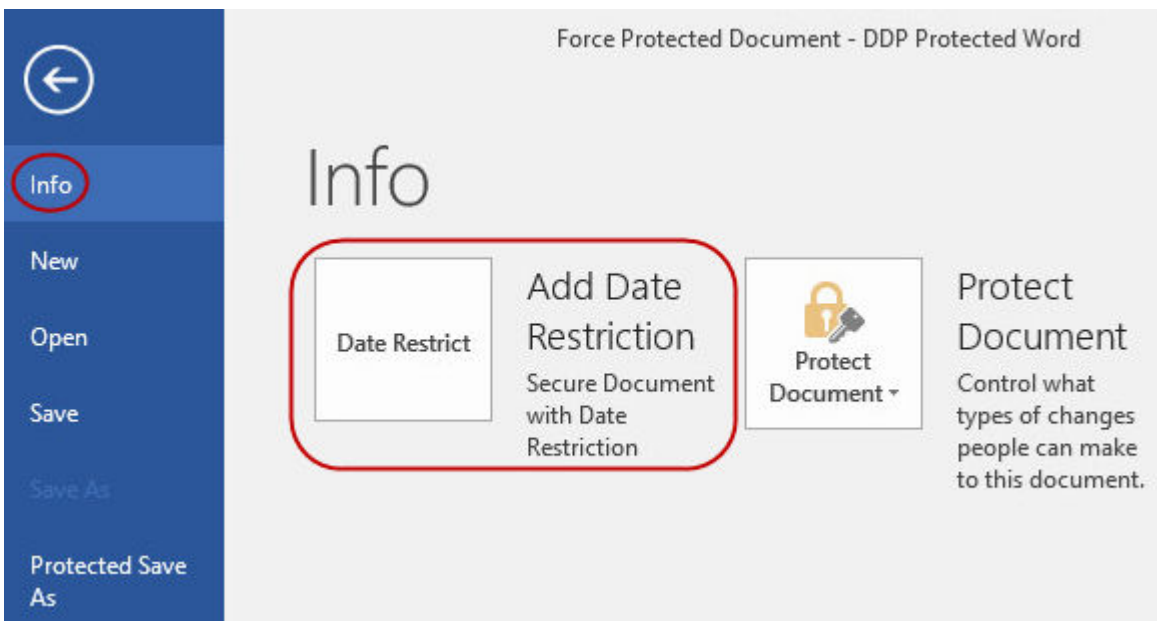


- If you select **Protected Save As**, the only option in the *Save as type* field is *Office Protected*.



- **File > Info** differs, for example:
 - For both Opt-in and Force-Protected modes: *Add Date Restriction* displays if your administrator enabled that policy. See [Enhance Security by Adding Date Restrictions](#).
 - For both Opt-in and Force-Protected modes: 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 Secure Lifecycle'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 Secure Lifecycle policies.
- If your administrator set policies to Force-Protected mode, with a higher level of security, unprotected Office documents open in read-only mode.



NOTE: For OneDrive, if you open a protected Office document through File > Open > OneDrive and the document is read only, confirm that you have installed and set up the OneDrive sync client.

Work with File Menu Options

This table lists File menu options for Office documents. Depending on the level of security, some options are grayed out.

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

File menu	Opt-in mode and Protected Office documents	Force-Protected mode for Protected and Unprotected
Open	Files open as usual	Unprotected documents open in read-only mode.
Save	<ul style="list-style-type: none"> Options: <ul style="list-style-type: none"> 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 filename. .xen file - You can open and save it in Protected mode, but the .xen file is removed from the cloud. The Office document has its usual extension, but it is protected. <p>NOTE: On the virtual drive, if you right-click to create a new Office document, it is a .xen file. You must manually save it as Protected.</p>	<ul style="list-style-type: none"> 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. <p>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).</p> <ul style="list-style-type: none"> .xen file - You can open and save it in Protected mode, but the .xen file is removed from the cloud. The Office document has its usual extension, but it is protected.
Save As	Has the standard options (but not Protected mode)	Disabled
Protected Save As	Only option in the Save as type field is Office Protected	Only option in the Save as type field is Office Protected
Print	May be enabled or grayed out based on policies set by your administrator. If the menu option is enabled, a policy may place a watermark, containing the user name, domain name, and computer ID, on each page when you print.	Depending on policy, this option may be enabled or grayed out. If the menu option is enabled, a policy may place a watermark, containing the user name, domain name, and computer ID, on each page when you print.
Share	Enabled	Disabled
Save and Send (Office 2010)	Enabled	Disabled If Print is enabled, you can select Print to print the document as a PDF.
Export (Office 2013 and higher)	May be enabled or grayed out based on policies set by your administrator.	May be enabled or grayed out based on policies set by your administrator.
Protected Export (Office 2013 and higher)	If the Export menu option is grayed out and Protected Export is enabled, the document exports with a watermark, containing the user name, domain name, and computer ID, on each page. NOTE: If you export a Protected-mode document to an external user, they can open and view it but not export or print it.	If the Export menu option is grayed out and Protected Export is enabled, the document exports with a watermark, containing the user name, domain name, and computer ID, on each page. NOTE: If you export a Protected-mode document to an external user, they can open and view it but not export or print it.

Work Online with Protected Office Documents

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



Work Online with Protected Macro-enabled Documents

With a protected macro-enabled document, the macro exists but is blocked. However, currently, Secure Lifecycle can only control a macro-enabled document after the newly protected document (.docm, .pptm, .xlsm) is closed and re-opened. Also, if you save a protected document with a macro as unprotected, you must close and re-open the document in order for the macro to run.

Troubleshooting for Opt-in Mode

In File > Info, if your Print is grayed out, a Secure Lifecycle policy has disabled printing for protected Office documents. Currently though, when you right-click a protected Office file in Windows Explorer, the Print option is not grayed out. However, if you select Print, the following occurs:

- Word - A dialog indicates that Word has stopped working.
- Excel - A dialog indicates that Print is disabled by policy.
- Powerpoint - A dialog indicates that Print is disabled by policy. If you click OK, a cover page is printed stating that the document is protected.

Determine Which Opt-in Mode Documents are Protected

If you have Force-Protected mode, all Office 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.

Additional Menu Options for Protected Office Documents

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

Paste

If your administrator sets a policy to protect Office documents:

- You can copy and paste data into the original protected document.
- You cannot copy or paste from a protected document to an unprotected document. Nothing displays on the Clipboard, and an enterprise-specific text message states that you cannot paste to the unprotected or non-managed document.

NOTE: If you cut text from a protected document and get the message in an unprotected document, click **Undo** in the protected document to retrieve the text.

Drag and Drop in Protected mode

You can drag and drop content into a protected Word document. Currently, drag and drop are disabled for protected Power Point and Excel files.

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.

Tampering and Protected Office Documents

Secure Lifecycle can scan protected Office documents to detect some forms of tampering.



If an internal user tampers with a protected Office document:

- Secure Lifecycle 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, Secure Lifecycle restores the cover page when an authorized users saves it again as protected.

External Users and Protected Office Documents

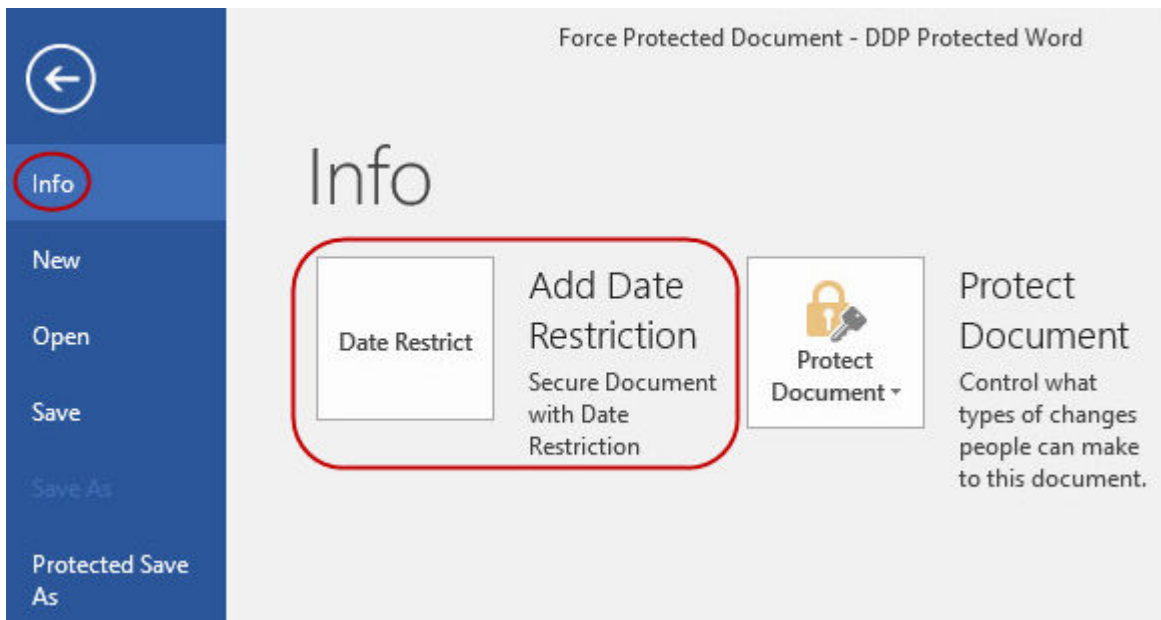
Enhance Security by Adding Date Restrictions

With Secure Lifecycle, you upload a protected Office document to the cloud and share it:

- All internal Secure Lifecycle users can view it.
- Based on policy, external users can view it.

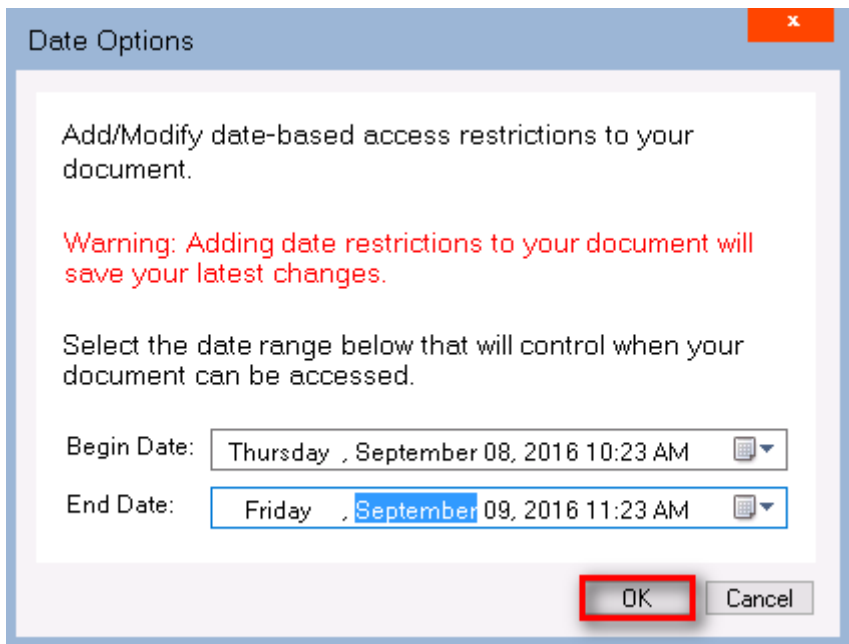
Optionally, for enhanced security with external users, you can add a date restriction to limit the amount of time that an external user can view a protected Office document.

- 1 Select **File > Info > Date Restrict**.



- 2 From the dropdown option, 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.

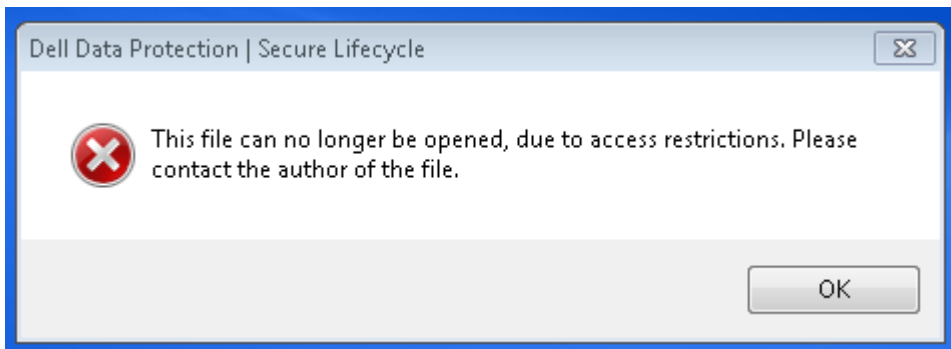


3 Click **OK**.

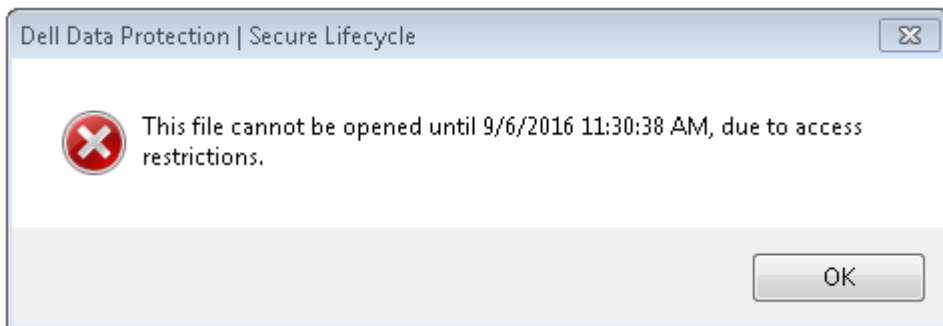
The document will be saved, protected, closed, and then reopened.

- NOTE:** If you modify the dates for an unprotected Office document and then click **Cancel**, **Secure Lifecycle** 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 dialog displays stating that the file cannot be opened until that date and time due to access restrictions.



Working without an Internet Connection

Without an Internet connection, you can still view cloud sync files on your local drive through File Explorer. However, the DDP|SL virtual drive does not display. Also, changes will not sync in the cloud until you connect to the Internet.

Character Limit for Folder Path Names

Windows path names have a limit of 248 characters.

In the Cloud, that limit does not exist. Therefore, you can create folders and subfolders with a path name that goes beyond that limit. However, locally, in Windows, any path names that exceed that limit, the folders are not created. Therefore, be sure to limit path names of folders and subfolders to 248 characters.

Dropbox for Business

Dropbox for Business has specific requirements. See [Install a Cloud Sync Client](#).

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. Dropbox for Business support is at:

<https://www.dropbox.com/help>.

Even though you can upload files on the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

Connect Secure Lifecycle and Dropbox for Business

If your company uses Dropbox for Business, you must allow Secure Lifecycle to stay connected.

To connect:

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

Set Up Selective Sync for Folders

To selectively sync folders:

- 1 In the system tray, click the **Dropbox for Business** icon.
- 2 Click the **Settings** icon, and select **Preferences**.
- 3 Click the **Account** tab, then click **Selective Sync**.
- 4 Select only folders or subfolders that you want to sync from your computer.
- 5 Click **Update**.



- 6 On the Update confirmation dialog, click **OK**.
- 7 On the Dropbox Preferences window, click **OK**.

A pop-up displays in the system tray that folders are being synced.

Your enterprise will determine if you can have a business account only or if you can use both business and personal folders. If you want pre-existing folders, with either personal files or data that does not need to be encrypted, deselect those folders before installing Secure Lifecycle. Otherwise, your personal data might be encrypted.

Use the Dropbox for Business System Tray Icon

In the system tray, click the Dropbox icon.

- For the website - Select the Globe icon.

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

- For the folder - Select the Dropbox folder icon. This redirects you to the DDP|SL virtual drive.

Use Dropbox for Business Context Menu

In Windows Explorer when Secure Lifecycle is installed, Dropbox for Business has a context menu.

NOTE: You must connect Secure Lifecycle to Dropbox.

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

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

Use Business and Personal Dropbox Accounts

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

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

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

Decrypting Folders in a Personal Account

If a personal folder is accidentally encrypted, the administrator can grant temporary access to allow you to manage encryption of your folders. Deselect folders that should be unencrypted. Also, you can remove folders from syncing by unlinking the account or un syncing personal folders that should remain unencrypted.



OneDrive for Business/ Unified OneDrive

NOTE: Secure Lifecycle is not supported with Microsoft Office 365.

NOTE:
Data sharing in OneDrive for Business is not supported.

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. OneDrive for Business support is at

<http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.

Even though you can upload files on the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

Set Up Selective Sync for Folders

To selectively sync folders:

- 1 In the system tray, right-click the **OneDrive for Business/ Unified OneDrive** icon, and click **Sync a new library**.
- 2 Enter your library URL.
- 3 Select **Sync now**.
- 4 Select **Show my files**.

Use the OneDrive for Business System Tray Icon

In the system tray:

- For the website - Right-click and select **Go to OneDrive.com**.
- For the folder - Right- or left-click and select **Open your OneDrive for Business folder**. This redirects you to the DDP|SL virtual drive.

Security Considerations with Secure Lifecycle and OneDrive or OneDrive for Business

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

- When downloading, do not select Cancel. This will cause an error. If you want to delete the file, wait until the download has completed.
- For Windows 8.1, Microsoft OneDrive has placeholder files that appear to exist in the sync client but are not actually downloaded. Therefore, Secure Lifecycle cannot encrypt them. If you open a placeholder file, Secure Lifecycle displays a dialog that the file will not be protected. You can right-click and select **Download** and then **Secure Lifecycle** converts it to a .xen file.



Dropbox

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. Dropbox support is at <https://www.dropbox.com/help>.

Even though you can create files in the cloud or upload files to the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

NOTE:

For Dropbox and Secure Lifecycle, if you create an Office file in the cloud and sync it down, it is encrypted as a .xen file. Therefore, on the virtual drive, it opens in read-only mode. You cannot edit it.

Set Up Selective Sync for Folders

To selectively sync folders:

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

Use the Dropbox System Tray Icon

In the system tray, click the Dropbox icon.

- For the website - Select the Globe icon.

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

- For the folder - Select the Dropbox folder icon. This redirects you to the DDP|SL virtual drive.

Security Considerations with Secure Lifecycle and Dropbox

If you are running in a virtual machine, do not drag a file from the server desktop into the browser. The file will not be protected. Do one of these: In the browser, use the Upload option or, on the desktop, drag the file to the DDP|SL virtual drive.

Dropbox FAQs

Question

My Dropbox account has many conflicted files. When I delete them from the cloud, they keep being created.

Answer



Sometimes, when a folder has already been shared and then multiple Secure Lifecycle accounts are activated at the same time, these files are seen as being created at the same time. In an effort to preserve the original, Dropbox will create multiple files of the same name and type and place them into the cloud. Therefore, Secure Lifecycle will allow all the files to be created without interfering.

Solution

- 1 Everyone who is sharing that file must collaborate on deselecting that folder for sync from the Dropbox application. See [Dropbox for Business](#).
- 2 After all the files and the folder have been removed from each local machine, one person must access the cloud and delete the duplicate files.

Then, each person can use the selective sync to re-add the folder to be synced.

Box

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. Box support is at <https://support.box.com/home>.

Even though you can upload files on the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

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

Set Up Selective Sync for Folders

To selectively sync folders:

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

Use the Box System Tray Icon

In the system tray, right-click the Box icon.

- For the website - Select Open Box Website.
- For the folder - Select Open Box Sync folder. This redirects you to the DDP|SL virtual drive.

Box Sync Client FAQs

Question

I am using the Box sync client. I created a new folder locally and added some files. The sync client appears to be working, but nothing has been created in the cloud.

Answer

The Box sync client may require some time to collect information about new folders and files. The process can take several minutes compared to other sync clients. Be sure to wait for several minutes for the sync client to complete before creating new folders and files.



Question

I am using the Box sync client. I ran out of room on my primary partition, so I moved it to another drive. Now, the My Box Files folder has one or more folders created and named **New Folder**.

Answer

Currently, when files are being synced between two computers to the same file share, if one person moves that folder to another location, then any new folders that other people create in that file share will create an empty folder named **New Folder**.

Solution

Delete the New Folder directly from the cloud. It will be removed from all systems that are sharing that folder.

Security Considerations with Secure Lifecycle and Box

If you create a file in the Box Cloud website, it will sync. However, it will download as an encrypted file.

Google Drive

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. Google Drive support is at <https://support.google.com/drive/?hl=en#topic=14940>.

Even though you can upload files on the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

Set Up Selective Sync for Folders

To selectively sync folders:

- 1 In the system tray, click the **Google Drive** icon.
- 2 Select the Settings icon.
- 3 Select **Preferences**.
- 4 To selectively sync, click **Only these folders**.
- 5 Clear the check box for folders that do not need to be protected in the cloud.
- 6 Click **Apply**.
- 7 To confirm, click **Continue**.

Use the Google Drive System Tray Icon

In the system tray, click the Google Drive icon.

- For the website - Select **Visit Google Drive on the Web**.
- For the folder - Select **Open Google Drive** folder. This redirects you to the DDP|SL virtual drive



Security Considerations with Secure Lifecycle and Google Drive

Secure Lifecycle encrypts folders and files to protect data. As Secure Lifecycle works with sync clients, be aware of these considerations.

- Corporate security policy prohibits use of Google Docs with Secure Lifecycle. When you install Secure Lifecycle, a dialog informs you of this policy. For more information, contact your IT administrator.

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, and the files are not encrypted. For Windows and Secure Lifecycle, any Google Docs that you create display in your Google Docs sync client folders.

However, if you open the folder, a dialog warns you that Secure Lifecycle cannot encrypt that document. Also, to ensure secure data, your administrator may be running reports to identify Google Docs that are being synced in order to help provide security.

- Google Drive options have both **Remove** (removes to trash) and **Delete**. Google Drive with Secure Lifecycle has Delete only, to be consistent with other Secure Lifecycle functionality.

NOTE: If you delete multiple files from the Secure Lifecycle virtual drive and some still display in the browser or command line, delete them in the browser or from the command line.

- With Google Drive, you may get a warning that properties are stripped when copying files to the DDP|SL virtual drive. These are security attributes.

OneDrive

NOTE:

Secure Lifecycle is not supported with Microsoft Office 365.

Cloud Storage Provider Help

Before using Secure Lifecycle, be sure to learn about the cloud storage provider. OneDrive support at <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.

Even though you can upload files on the cloud storage provider's website, the best practice is to work with folders and files on the DDP|SL virtual drive.

Set Up Selective Sync for Folders

To selectively sync folders:

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

Use the OneDrive System Tray Icon

In the system tray:

- For the website - Right-click and select **Go to OneDrive.com**.
- For the folder - Right- or left-click and select **Open your OneDrive folder**. This redirects you to the DDP|SL virtual drive.

Security Considerations with Secure Lifecycle and OneDrive or OneDrive for Business

See [Security Considerations with Secure Lifecycle and Sync Clients](#).

Understand the Secure Lifecycle System Tray Menu Items

Details Screen

The Secure Lifecycle Details screen provides helpful information, for example:

- For technical support, you can provide status or version information.
- To see an unobfuscated filename that is associated with a.xen file, select **Files > File State**.
- To search for a filename, select Copy at the bottom right and paste the contents into a Word file.
- To see who owns a folder, select Folders and scroll to the FOLDER OWNERSHIP column.

To access the Details screen:

Click the **Secure Lifecycle** system tray icon, and then click **Details...**

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

Service Status: Status of the Secure Lifecycle 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

External user - a user outside of this domain address

Registration Email: For Internal users, this is the domain email address. For External users, this is the email under which they registered.

Server URL: DDP EE Server/VE Server that communicates with this client.

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

Policy Version: Policy version generated by the DDP EE Server/VE Server.

The **Files** area of the Details screen displays the following information:

Name: Name of the file

Cloud: Lists the obfuscated filename or whether the file is *Unprotected*.

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 folder (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: *True or False.*

Browser Created: *True or False.*

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

NOTE:

Log files can be also be found at **C:\ProgramData\Dell\Dell Data Protection\Secure Lifecycle**.

The **Folders** area of the Details screen displays the following information:

Name: Name of the folder

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

Sync Client: The last sync client to sync that folder (See [Cloud Sync Clients](#).)

Folder Ownership: This value indicates the owner of the folder. Value is determined by the Key ID.

Override: Options are *None* and *Pre-existing*. Pre-existing files are not protected. Also, if you have access to Folder Management and unprotected some files, this column indicates that they are not protected.

Obfuscation Type: If your enterprise manages your cloud storage, this is a policy set on each folder indicating what type of .xen files will be created in the cloud. This is a policy set by your administrator. If your administrator selects *Extension only*, the actual filename with the ".xen" extension will be displayed. If your administrator selects *Guid*, a scrambled filename with the ".xen" extension will display. This is a policy setting that takes effect on new folders only. The default is *Extension only*.

Manage Folders Menu

Some managers or administrators may need to temporarily troubleshoot folders shared by more than one user. You can request permission from your administrator for the Manage Folders option. Typically, this is a temporary option.

Check for Policy Updates

If your administrator modifies a policy and notifies you of a policy update, go to the Windows system tray, click the **Dell Data Protection | Secure Lifecycle** 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
- 2 Select **Xendow.Service.log**.



① | **NOTE:** After `Xendow.Service.log` reaches 3 MB, it is saved as `Xendow.Service1.log`, then `Xendow.Service2.log`.

Upgrade Secure Lifecycle

The best practice is to uninstall your previous version and then install the current version. See [Uninstall Secure Lifecycle](#).


Provide Feedback to Dell

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

To access the form, click the Secure Lifecycle icon in the system tray, and select **Send Feedback**.

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

Possible Issues With Activating - Cloud and Protected Office

If you have installed Secure Lifecycle, but the Secure Lifecycle icon in the the system tray does not have a green checkmark , be aware of the following depending on whether you have cloud encryption, protected Office, or both:

- Access is blocked to cloud sync websites
- Cloud sync applications are blocked from connecting to their web services
- Local synced folders are not updated during this time
- Secure Lifecycle 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 Secure Lifecycle.
- Contact your system administrator about having your computer configured to manually activate. See [Activate Secure Lifecycle](#).

Activate Secure Lifecycle

Typically, Secure Lifecycle 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 system tray, a shield icon with an orange exclamation point displays.
- 2 Click the **Secure Lifecycle** icon in the system tray and select **User Activation**.
- 3 Enter your domain email address and domain password, and click **Activate**.
If you are an internal user (with a domain email address), ignore the Register button. Only external users need to register.

After activation is complete, a green check displays on the Secure Lifecycle system tray icon .

- 4 Confirm your user mode status. Click the system tray icon and select **Details**.
- 5 At the top, confirm User Mode:
Internal: A user with an email address within the company's domain.



External: A user with a non-domain email address. For more information, see [Using Secure Lifecycle as an External User](#).



User Tasks - Protected Office without Cloud Encryption


Your administrator has already configured policies for Secure Lifecycle to protect Office documents.

NOTE: If your enterprise also manages your cloud sync client, see [User Tasks - Cloud Encryption and Protected Office](#).

Overview of Tasks

This overview summarizes the sequence for installing and using Secure Lifecycle.

Install Secure Lifecycle

Task	Description	For More Information
Install Secure Lifecycle	Determine the following: User must install Secure Lifecycle Administrator already installed Secure Lifecycle - continue to the next step.	User installs: See Install Secure Lifecycle on Windows . Reboot and continue to the next step.
Confirm activation status	Confirm on the system tray that the Secure Lifecycle icon has a green checkmark  .	If the icon has an orange exclamation point, see Possible Issues With Activating - Protected Office .

Use Secure Lifecycle

Task	Description	For More Information
View system tray menu	Provides helpful information about files, folders, and troubleshooting.	Understand the Secure Lifecycle System Tray Menu Items
Protect Office and macro-enabled documents, if policy is activated	Protect an Office document (.docx, .pptx, .xlsx, .docm, .pptm, .xslm) when you create it. It will be secure when you share it with others or store it on removable media.	Use Office Documents with Secure Lifecycle's Protected Mode <ul style="list-style-type: none"> Observe File Menu Options to Determine the Level of Security for Office Documents Work with File Menu Options
Share a folder with others to collaborate on files	Share a folder with: Internal user (has a domain email address) External user (has a non-domain email address) - work with your administrator.	Internal user - See the online help for your cloud storage provider. External user - See Using Secure Lifecycle as an External User .



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 Secure Lifecycle is installed and activated. See [Possible Issues With Activating - Protected Office](#).


Install Secure Lifecycle for Protected Office

Install Secure Lifecycle on Windows

You must be a local administrator on the computer to install Secure Lifecycle.

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

Be prepared to restart your computer after Secure Lifecycle is installed.

- 1 To download the Secure Lifecycle installer, go to the location specified by your administrator.
- 2 Based on your operating system, select either the 32-bit or 64-bit installer, typically **setup32.exe** or **setup64.exe**, and copy it to the local computer.
- 3 Double-click the file to launch the installer.
- 4 If you get a Security Warning, click **Run**.
- 5 Select a language and click **OK**.
- 6 If prompted to install Microsoft Visual C++ 2010 Redistributable Package or Microsoft .NET Framework 4.0 Client Profile, click **OK**.
- 7 At the Welcome screen, click **Next**.
- 8 Read the license agreement, accept the terms, and click **Next**.
- 9 At the Destination Folder screen, click **Next** to install in the default location of **C:\Program Files\Dell\Dell Data Protection\Secure Lifecycle**.
On **C:**, do not install Secure Lifecycle in the Users or Windows folders or at the root of any drive. You will get an error.
- 10 In the *Server Name* : field, enter the Server Name that this computer will communicate with, such as server.domain.com. You do not need to include www or http(s). This information is supplied by your administrator.
Do not clear the *Enable SSL Trust Verification* check box unless your administrator instructs you to do so.
- 11 Click **Next**.
- 12 In the Confirm Activation Server Information screen, confirm that the Server URL address is correct. The installer adds www or http(s) and the port. Click **Next**.
- 13 In the Management Type window, select this option:
 - Internal Use - A user with an email address within the company's domain.
- 14 Click **Install** to begin the installation.
A status window displays the installation progress.
- 15 Click **Finish** when the Installation Complete screen displays.
- 16 Click **Yes** to restart.
Installation of Secure Lifecycle is complete.
- 17 After you reboot, confirm on the system tray that the Secure Lifecycle icon has a green checkmark .

Use Office Documents with Secure Lifecycle's Protected Mode

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

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

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 filename and select **Move**.
- Share it on the network
- Upload it to a cloud storage provider
- Store it on removable media

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

- You need to install Secure Lifecycle.
- You need to activate Secure Lifecycle.
- You open a protected Office document in the cloud.
- You downloaded an Office file from your computer that has Secure Lifecycle 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.

If your enterprise uses Secure Lifecycle's Protected mode, see the following:

- [Observe File Menu Options to Determine the Level of Security for Office Documents](#)
- [Work with File Menu Options](#)
- [Determine Which Opt-in Mode Documents are Protected](#)
- [Additional Menu Options for Protected Office Documents](#)
- [External Users and Protected Office Documents](#)

Observe File Menu Options to Determine the Level of Security for Office Documents

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

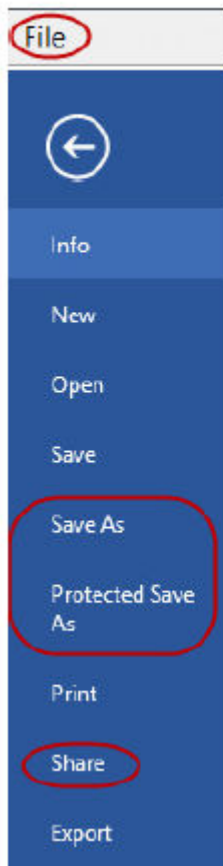
To determine the level of security, observe options that are enabled or disabled:

- **Opt-in mode** - You have some options in determining which Office documents to protect.
 - *Save As* and *Protected Save As* are enabled - If you opt to protect an Office document, select **Protected Save As**.
 - *Print* and *Export* may be enabled or disabled depending on policy.
 - *Share* (*Save and Send* for Office 2010) is enabled.
 - **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.
 - *Save As* is disabled and *Protected Save As* enabled - You must save all Office documents in Protected mode.
 - *Print* and *Export* may be enabled or disabled based on policy.
 - *Share* (*Save and Send* for Office 2010) is disabled.

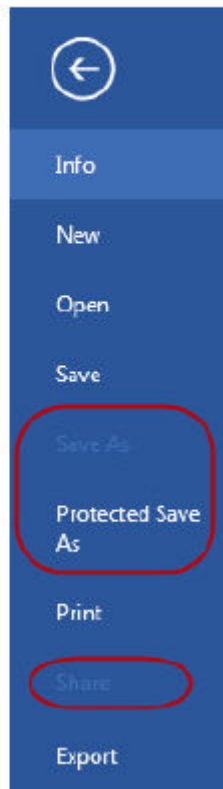
NOTE: With Force-Protected mode, policy also enables specific times for sweeping your computer to locate any unprotected Office files and change them to Protected mode. You must be logged in and be connected to the network for Secure Lifecycle to sweep any unprotected Office files.



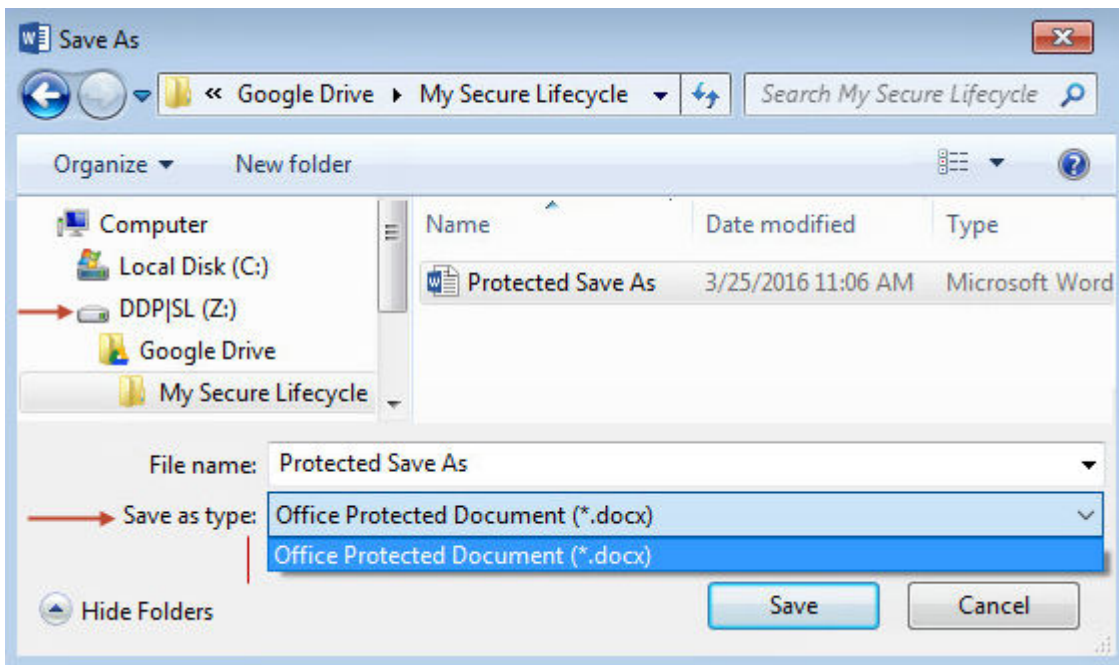
Opt-in mode



Force-Protected



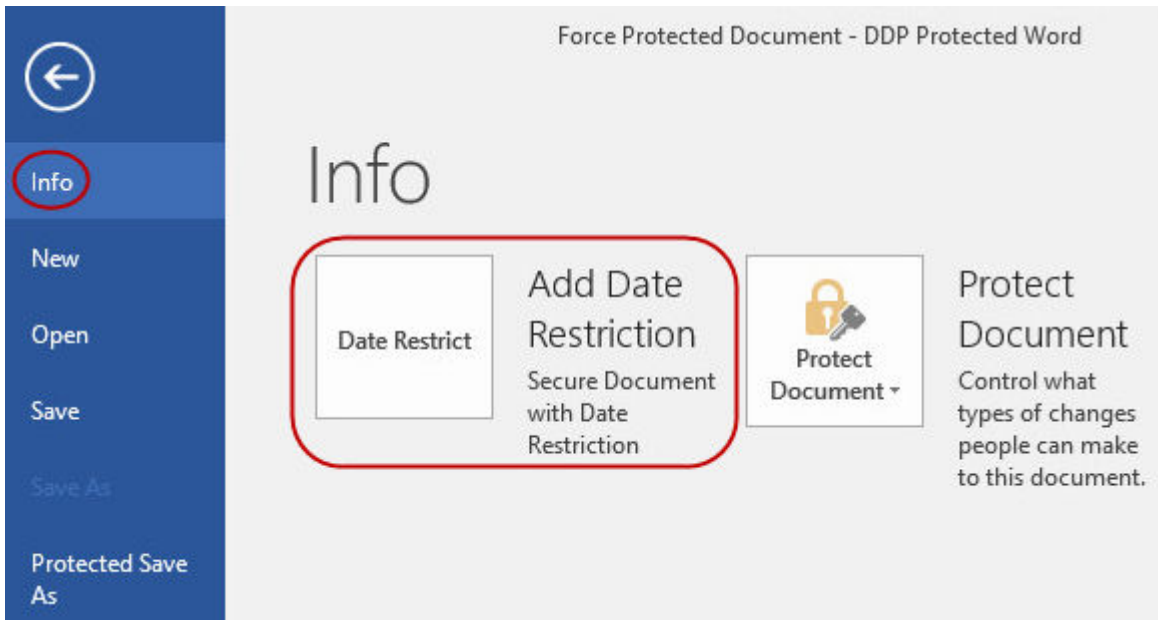
- If you select **Protected Save As**, the only option in the *Save as type* field is *Office Protected*.



- **File > Info** differs, for example:
 - For both Opt-in and Force-Protected modes: *Add Date Restriction* displays if your administrator enabled that policy. See [Enhance Security by Adding Date Restrictions](#).

- For both Opt-in and Force-Protected modes: 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 Secure Lifecycle'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 Secure Lifecycle policies.
- If your administrator set policies to Force-Protected mode, with a higher level of security, unprotected Office documents open in read-only mode.

NOTE: For OneDrive, if you open a protected Office document through **File > Open > OneDrive** and the document is read only, confirm that you have installed and set up the OneDrive sync client.

Work with File Menu Options

This table lists File menu options for Office documents. Depending on the level of security, some options are grayed out.

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



File menu	Opt-in mode and Protected Office documents	Force-Protected mode for Protected and Unprotected
Open	Files open as usual	Unprotected documents open in read-only mode.
Save	<ul style="list-style-type: none"> 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 filename. .xen file - You can open and save it in Protected mode, but the .xen file is removed from the cloud. The Office document has its usual extension, but it is protected. <p>NOTE: On the virtual drive, if you right-click to create a new Office document, it is a .xen file. You must manually save it as Protected.</p>	<ul style="list-style-type: none"> 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. <p>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).</p> <ul style="list-style-type: none"> .xen file - You can open and save it in Protected mode, but the .xen file is removed from the cloud. The Office document has its usual extension, but it is protected.
Save As	Has the standard options (but not Protected mode)	Disabled
Protected Save As	Only option in the Save as type field is Office Protected	Only option in the Save as type field is Office Protected
Print	May be enabled or grayed out based on policies set by your administrator. If the menu option is enabled, a policy may place a watermark, containing the user name, domain name, and computer ID, on each page when you print.	Depending on policy, this option may be enabled or grayed out. If the menu option is enabled, a policy may place a watermark, containing the user name, domain name, and computer ID, on each page when you print.
Share	Enabled	Disabled
Save and Send (Office 2010)	Enabled	Disabled If Print is enabled, you can select Print to print the document as a PDF.
Export (Office 2013 and higher)	May be enabled or grayed out based on policies set by your administrator.	May be enabled or grayed out based on policies set by your administrator.
Protected Export (Office 2013 and higher)	<p>If the Export menu option is grayed out and Protected Export is enabled, the document exports with a watermark, containing the user name, domain name, and computer ID, on each page.</p> <p>NOTE: If you export a Protected-mode document to an external user, they can open and view it but not export or print it.</p>	<p>If the Export menu option is grayed out and Protected Export is enabled, the document exports with a watermark, containing the user name, domain name, and computer ID, on each page.</p> <p>NOTE: If you export a Protected-mode document to an external user, they can open and view it but not export or print it.</p>

Work Online with Protected Office Documents

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

Work Online with Protected Macro-enabled Documents

With a protected macro-enabled document, the macro exists but is blocked. However, currently, Secure Lifecycle can only control a macro-enabled document after the newly protected document (.docm, .pptm, .xlsm) is closed and re-opened. Also, if you save a protected document with a macro as unprotected, you must close and re-open the document in order for the macro to run.

Troubleshooting for Opt-in Mode



In File > Info, if your Print is grayed out, a Secure Lifecycle policy has disabled printing for protected Office documents. Currently though, when you right-click a protected Office file in Windows Explorer, the Print option is not grayed out. However, if you select Print, the following occurs:

- Word - A dialog indicates that Word has stopped working.
- Excel - A dialog indicates that Print is disabled by policy.
- Powerpoint - A dialog indicates that Print is disabled by policy. If you click OK, a cover page is printed stating that the document is protected.

Determine Which Opt-in Mode Documents are Protected

If you have Force-Protected mode, all Office 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.

Additional Menu Options for Protected Office Documents

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

Paste

If your administrator sets a policy to protect Office documents:

- You can copy and paste data into the original protected document.
- You cannot copy or paste from a protected document to an unprotected document. Nothing displays on the Clipboard, and an enterprise-specific text message states that you cannot paste to the unprotected or non-managed document.

NOTE: If you cut text from a protected document and get the message in an unprotected document, click Undo in the protected document to retrieve the text.

Drag and Drop in Protected mode

You can drag and drop content into a protected Word document. Currently, drag and drop are disabled for protected Power Point and Excel files.

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.

Tampering and Protected Office Documents

Secure Lifecycle can scan protected Office documents to detect some forms of tampering.

If an internal user tampers with a protected Office document:

- Secure Lifecycle 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, Secure Lifecycle restores the cover page when an authorized users saves it again as protected.

External Users and Protected Office Documents

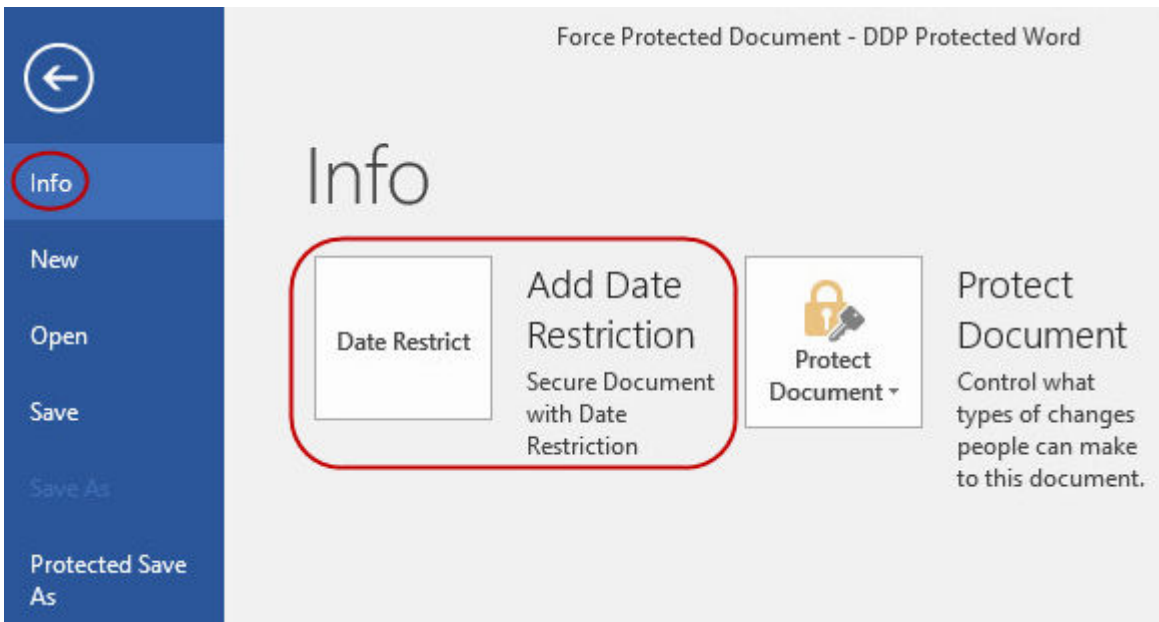
Enhance Security by Adding Date Restrictions

With Secure Lifecycle, you upload a protected Office document to the cloud and share it:

- All internal Secure Lifecycle users can view it.
- Based on policy, external users can view it.

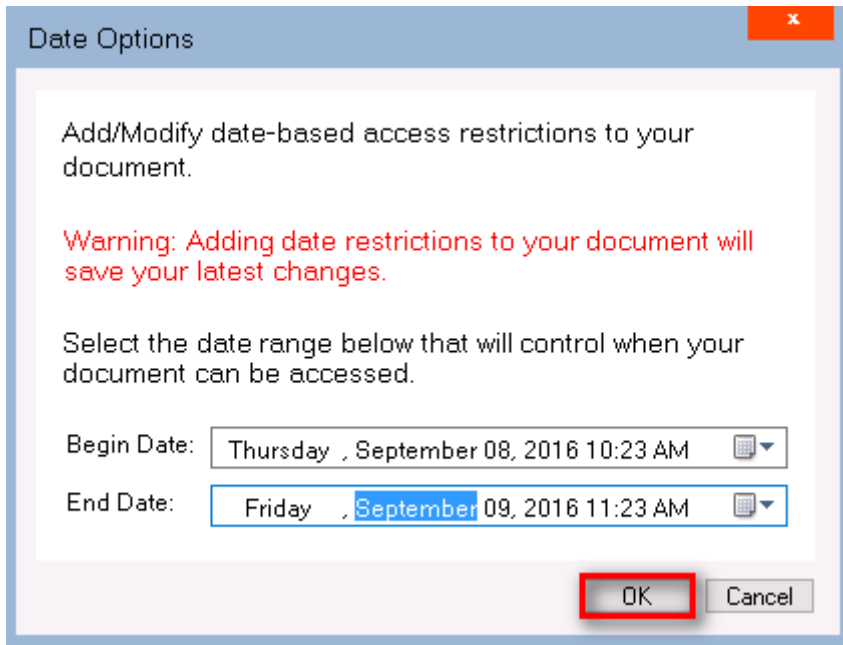
Optionally, for enhanced security with external users, you can add a date restriction to limit the amount of time that an external user can view a protected Office document.

- 1 Select **File > Info > Date Restrict**.



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

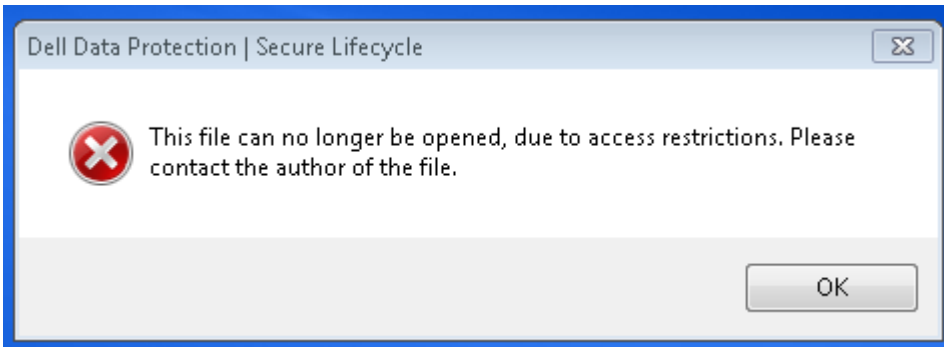
NOTE: The Begin date and time can be future if you want to send the document but prevent the external user from viewing it until the targeted date and time.



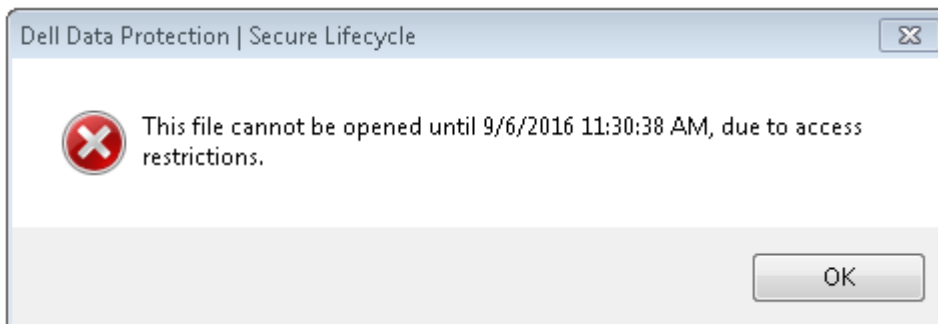
- 3 Click **OK**.
The document will be saved, protected, closed, and then reopened.

- NOTE:** If you modify the dates for an unprotected Office document and then click Cancel, Secure Lifecycle 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 dialog displays stating that the file cannot be opened until that date and time due to access restrictions.



Understand the Secure Lifecycle System Tray Menu Items

Details Screen

The Secure Lifecycle Details screen provides helpful information, for example:

- For technical support, you can provide status or version information.
- To see an unobfuscated filename that is associated with a.xen file, select **Files > File State**.
- To search for a filename, select Copy at the bottom right and paste the contents into a Word file.
- To see who owns a folder, select Folders and scroll to the FOLDER OWNERSHIP column.

To access the Details screen:

Click the **Secure Lifecycle** system tray icon, and then click **Details...**

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

Service Status: Status of the Secure Lifecycle 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

External user - a user outside of this domain address

Registration Email: For Internal users, this is the domain email address. For External users, this is the email under which they registered.

Server URL: DDP EE Server/VE Server that communicates with this client.

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

Policy Version: Policy version generated by the DDP EE Server/VE Server.

The **Files** area of the Details screen displays the following information:

Name: Name of the file

Cloud: Lists the obfuscated filename or whether the file is *Unprotected*.

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 folder (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: *True or False*.

Browser Created: *True or False*.



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

NOTE:

Log files can be also be found at `C:\ProgramData\Dell\Dell Data Protection\Secure Lifecycle`.

The **Folders** area of the Details screen displays the following information:

Name: Name of the folder

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

Sync Client: The last sync client to sync that folder (See [Cloud Sync Clients](#).)

Folder Ownership: This value indicates the owner of the folder. Value is determined by the Key ID.

Override: Options are *None* and *Pre-existing*. Pre-existing files are not protected. Also, if you have access to Folder Management and unprotected some files, this column indicates that they are not protected.

Obfuscation Type: If your enterprise manages your cloud storage, this is a policy set on each folder indicating what type of .xen files will be created in the cloud. This is a policy set by your administrator. If your administrator selects *Extension only*, the actual filename with the ".xen" extension will be displayed. If your administrator selects *Guid*, a scrambled filename with the ".xen" extension will display. This is a policy setting that takes effect on new folders only. The default is *Extension only*.

Manage Folders Menu

Some managers or administrators may need to temporarily troubleshoot folders shared by more than one user. You can request permission from your administrator for the Manage Folders option. Typically, this is a temporary option.

Locate Log Files

For troubleshooting, your administrator may request log files.

To locate log files:

- 1 Navigate to
- 2 Select **Xendow.Service.log**.

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

Check for Policy Updates

If your administrator modifies a policy and notifies you of a policy update, go to the Windows system tray, click the **Dell Data Protection | Secure Lifecycle** 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.

Upgrade Secure Lifecycle

The best practice is to uninstall your previous version and then install the current version. See [Uninstall Secure Lifecycle](#).

Provide Feedback to Dell


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



To access the form, click the Secure Lifecycle icon in the system tray, and select **Send Feedback**.

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

Possible Issues With Activating - Protected Office

If you have installed Secure Lifecycle, but the Secure Lifecycle icon in the the system tray does not have a green checkmark , be aware of the following:

- Secure Lifecycle 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 Secure Lifecycle.
- Contact your system administrator about having your computer configured to manually activate. See [Activate Secure Lifecycle](#).

Activate Secure Lifecycle

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

- Log in to Windows.
In the system tray, a shield icon with an orange exclamation point displays.
- Click the **Secure Lifecycle** icon in the system tray and select **User Activation**.
- Enter your domain email address and domain password, and click **Activate**.
If you are an internal user (with a domain email address), ignore the Register button. Only external users need to register.

After activation is complete, a green check displays on the Secure Lifecycle system tray icon .

- Confirm your user mode status. Click the system tray icon and select **Details**.
- At the top, confirm User Mode:

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

External: A user with a non-domain email address. For more information, see [Using Secure Lifecycle as an External User](#).

Using Secure Lifecycle Mobile with iOS or Android

This section describes basic information on using Secure Lifecycle Mobile with iOS or Android devices. When your administrator sets a policy to enable Secure Lifecycle, files are encrypted and secure in the cloud. However, you can use the Secure Lifecycle Mobile app to view them on your mobile device.

Prerequisite

Before you use the Secure Lifecycle app, you need the name of your enterprise's Dell Data Protection Server, such as server.domain.com. This information is supplied by your administrator.

Get Started with Secure Lifecycle Mobile

Follow this sequence as you use Secure Lifecycle Mobile.

Task	Description	See this section
Install Secure Lifecycle	Determine the following:	Administrator installed: Tap the Secure Lifecycle app and log in.
	Administrator already installed	User installs: See one of these:
	User must install	Install on an iOS device Install on an Android device
Access your cloud storage provider account	On the device, navigate to the Home page of the Secure Lifecycle app and tap your cloud storage provider.	See one of these: Access your Cloud Storage Provider account for iOS Access your Cloud Storage Provider account for Android

The Secure Lifecycle Mobile app lists the cloud sync client used with your company and allows you to download it.

NOTE:

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

To protect your data in the cloud, Secure Lifecycle encrypts it. Therefore, the Secure Lifecycle app must be installed on your mobile device to view encrypted files.

- Protected Office files (.docx, .pptx, .xlsx) retain their file extension.
- Non-Office files in the cloud have a .xen extension.

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

On mobile devices, you can:



- Create folders
- Upload and download files

NOTE: With Secure Lifecycle, 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 Secure Lifecycle Home screen, not a cloud sync client app. When you tap a file, Secure Lifecycle automatically decrypts it and displays it in cleartext within the app. However, in the cloud, the file remains secure as a .xen file.

- Add a file to Favorites
 - For iOS, see the navigation drawer. For Android, press and hold the filename.
- Delete folders and files
- Accept a shared folder from an internal user

NOTE: If an internal user shares a folder with you through Secure Lifecycle, 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.

- Share a document with an external user (if the policy is enabled for external viewers) - For iOS, see [View Secure Lifecycle Cloud Storage policies for your iOS device](#).
- Edit .docx and .ppt Office files.

NOTE: Currently, .csv and .csv.xen files cannot be edited on mobile devices.

Protected Office Documents When Offline

When you 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 Secure Lifecycle 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.

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 work. If the geofencing feature is enabled by your administrator and location services are set to Off, file access is denied.

Use a PIN

Your administrator may set a policy requiring a PIN.

Secure Lifecycle on an iOS device

Install on an iOS device

- 1 On your device, tap **App Store** and search for **Secure Lifecycle Mobile**.
- 2 Select and install the **Secure Lifecycle** app.
- 3 For the Server field at the login screen, enter the hostname of your company's Dell Data Protection Server, such as server.domain.com.
- 4 Enter your user name and password.
- 5 Tap **Login**.

Access your Cloud Storage Provider account for iOS

After you log in to Secure Lifecycle, a Secure Lifecycle policy determines which cloud storage providers display on the Home screen. Your administrator may designate a specific cloud storage provider for use within the enterprise.

The navigation drawer has additional options.

To access an account:



- 1 On the Secure Lifecycle Home page, tap the cloud storage provider.
- 2 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.

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 Secure Lifecycle navigation drawer and tap **Settings**.
- 2 Tap **Unlink**.

View Secure Lifecycle Cloud Storage policies for your iOS device

- 1 In the Secure Lifecycle navigation drawer, tap **Settings**.
- 2 Tap **Policy**.

The list may include:

- Revision - number of policies that have been revised
- Obfuscate Filenames - default is set to **No**
- Cloud sync client - policy should be set to **Encrypt**
- External Viewers - if set to **Yes**, the sharing policy is enabled. When you open a document in the app, a menu option allows you to share the file.

Uninstall the Secure Lifecycle app

- 1 In the iOS Apps drawer, tap and hold the **Secure Lifecycle** icon.
- 2 Tap **x**.
- 3 Tap **Delete**.

Troubleshooting iOS and Secure Lifecycle

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 Secure Lifecycle. If the device has sufficient memory, close the file and reopen it.

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 Secure Lifecycle app.

Secure Lifecycle on an Android device

Install on an Android device

- 1 On your device, access **Google Play** and search for **Secure Lifecycle Mobile**.
- 2 Select and install the **Secure Lifecycle** app.
- 3 For the Server field at the login screen, enter the name of your company's Dell Data Protection Server, such as server.domain.com.
- 4 Enter your user name and password.
- 5 Tap **Login**.

Your account is now activated.

Access your Cloud Storage Provider account for Android

After you log in to Secure Lifecycle, a Secure Lifecycle policy determines which cloud storage providers display. Your administrator may designate a specific cloud storage provider to use within the enterprise and block the others.



To access an account:

- 1 On the Secure Lifecycle Home page, tap the cloud storage provider.
- 2 Do one of these by following the online screens:
 - 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.

- 3 After you access your account, open the navigation drawer and tap **Settings**. When you grant access to a cloud storage provider, a check mark displays in the check box.

NOTE:

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.

NOTE: For OneDrive and Dropbox, if you are unable to share a file from Applications and the file shares a link with the Secure Lifecycle app, then share the file from the File Browser app on the device.

Uninstall the Secure Lifecycle app

- 1 In the Android Apps drawer, tap **Settings**.
- 2 In **Settings**, tap **Apps**.
- 3 Press the **Secure Lifecycle** icon.
- 4 Drag the icon to the Uninstall option.
- 5 Click **OK**.

Security Considerations with Secure Lifecycle and Sync Clients

Secure Lifecycle encrypts folders and files to make data secure. As Secure Lifecycle 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 Data Protection EE Server/VE Server. Therefore, the files are not encrypted. For Android and iOS devices with Secure Lifecycle, access to these Google Docs is blocked. It differs slightly for each platform:

- Android
- iOS - A message is displayed.

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.

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 Secure Lifecycle 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.



Using Secure Lifecycle as an External User

An external user who has a non-domain email address can also use Secure Lifecycle. Here are some examples.

- You have installed and activated Secure Lifecycle 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 Secure Lifecycle on a computer or 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.

For external users, see [Server Requirements](#). Also, the domain or user must not be on the enterprise's blacklist.

NOTE: External users who were registered with Secure Lifecycle 1.0 will be migrated if the enterprise upgrades.

Internal User Tasks

To share secure files with an external user, you must:

- Make one or more secure files available to the external user.
 - Protected Office documents - Grant access to one or more secure files through:
 - Local folder or network drive
 - Email
 - Removable media
 - Network share
 - Non-Office .xen files - Create a folder to share on the sync client and add files.
- Grant the external user access to one or more files.

If you plan to share non-Office .xen files, you must add them to a sync client folder and then grant access. For protected Office files, you must grant access. The steps may vary depending on the method you use or the sync client used.

Share a folder on the sync client to share .xen files

- 1 In Windows Explorer, access your sync client, create a folder, and upload a file to share with an external user. See [View Folders and Files on the Local Computer and in the Cloud](#).

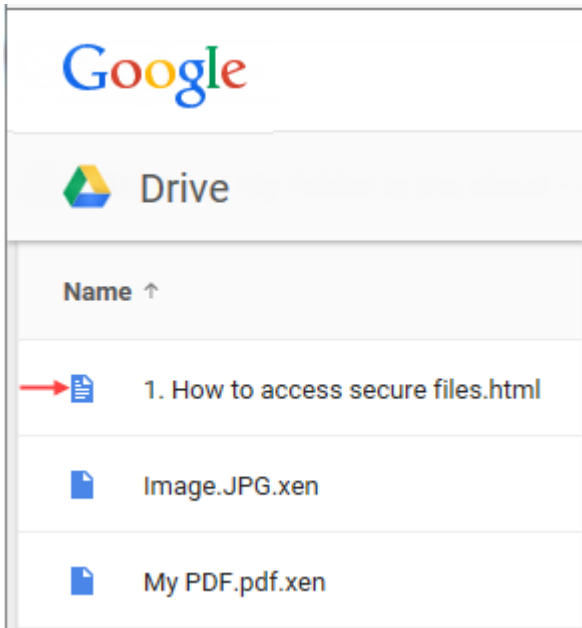
Protected Office documents can be on the DDP|SL virtual drive, in the Secure Documents folder, or on the desktop.

NOTE: With protected Office files, you cannot select a folder.

A *Protected Document Access Sharing* page opens with a column displaying the selected files.

- 2 On the sync client website, confirm that the folder and file were created and encrypted.

When you add a .xen file to a new folder on the DDP|SL virtual drive, Secure Lifecycle adds a document, *How to access secure files.html*, to the folder on the website. This file is used only when sharing the folder with an external user.



- 3 On the sync client website, right-click the folder you created and click **Share**.
A window opens, allowing you to enter the email account for an external user. The steps vary depending on the sync client used. For links to information about your sync client, see [Work with the cloud sync client on the DDP|SL virtual drive](#).
- 4 [Grant access](#) to the individual files within that folder that you want to share.

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 secure file and select **Grant Protected File Access**. You can select a single or multiple files up to 50.
- 2 In the *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, inform the external user that they will receive an email from you with instructions that allow them to register with a Dell Server, download and activate Dell Data Protection | Secure Lifecycle, and then view shared protected files.

External User Tasks

To open and view a Secure Lifecycle document, the external user must:

- Register with Secure Lifecycle
- Install Secure Lifecycle - the external user must have administrator rights on their computer
- If the internal user shares a folder through a sync client, the external user must have a sync client account. See [Install a Cloud Sync Client](#) and then [Work with the cloud sync client on the DDP|SL virtual drive](#).

Register Secure Lifecycle

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

To register Secure Lifecycle:

- 1 In the Account Verification email from the Dell Enterprise Server, click the hyperlink.



- 2 Continue to the webpage.
- 3 At the Confirmation page, click **Continue to Login**.
- 4 At the Login page, click **Forgot Password**.

NOTE: The Dell Server has assigned a random password, which you must reset.

- 5 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.
- 6 Open the account activation email and click the link.
The email also lists the Server name to use when you install Secure Lifecycle.
- 7 On the Login page, enter the email address and password you used to register.
- 8 Click **Login**.
A Secure Lifecycle Download page opens.
- 9 Download and Install Secure Lifecycle.
A Download page opens with options for Windows, iOS, Android, and Mac OS X. These steps describe installing Secure Lifecycle on Windows. See also [User Tasks - Protected Office without Cloud Encryption](#).

NOTE: The Download page also lists the Server Name that you will need in these steps.

- 10 Under Windows, click **Download (32-bit)** or **Download (64-bit)**, depending on your computer's operating system.
- 11 Download the setup file to a directory on your computer.
- 12 Double-click the setup file to launch the installer.
- 13 Select a language and click **OK**.
- 14 If prompted to install Microsoft Visual C++ 2010 Redistributable Package, click **OK**.
- 15 At the Welcome screen, click **Next**.
- 16 Read the license agreement, accept the terms, and click **Next**.
- 17 At the Destination Folder screen, click **Next** to install in the default location of `C:\Program Files\Dell\Dell Data Protection\Secure Lifecycle\`.
- 18 In the *Server Name*: field, enter the Server Name that this computer will communicate with. This name is in the activation email you received or at the top of the Download page.
- 19 Click **Next**.
- 20 In the Confirm Activation Server screen, confirm that the Server URL address is correct. The installer adds `www` or `http(s)` and the port. Click **Next**.
- 21 In the Management Type window, select this option:
 - External Use - A user with a non-enterprise domain email address.
- 22 Click **Install** to begin the installation.
A status window displays the installation progress.
- 23 Click **Finish** when the Installation Complete screen displays.
- 24 Click **Yes** to restart.
Installation of Secure Lifecycle is complete.
- 25 See [Activate Secure Lifecycle](#).

Activate Secure Lifecycle

After Secure Lifecycle is installed and the computer reboots, follow these steps to activate:

- 1 Log in to Windows.
In the system tray, a cloud icon with an orange exclamation point displays.
- 2 When a dialog displays in the system tray, click **Click here to Activate**.
If you do not see the dialog, click the **Secure Lifecycle** icon in the system tray and select **User Activation**.
- 3 Enter your email address and password you used to register, and click **Activate**.

After activation is complete, a green check displays on the Secure Lifecycle system tray icon



- 4 Confirm your user mode status. Click the system tray icon and select **Details**.

At the top, User Mode is:

External: A user with a non-domain email address.

If you already installed and logged in to a sync client, the DDP|SL virtual drive displays in Windows Explorer.

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 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



Uninstall Sync Client or Secure Lifecycle

If your administrator installed Secure Lifecycle, only your administrator can uninstall the product. An external user who has been invited to share a folder and has administrator rights on an external computer may also uninstall Secure Lifecycle from that external computer.

Uninstall a Cloud Sync Client

If you uninstall your cloud sync client but still have Secure Lifecycle on your computer, you can still view your files in cleartext on the DDP|SL virtual drive.

However, if you reinstall the same cloud sync client, you need a new key to open them on the DDP|SL virtual drive and will have to download your files from the sync client website.

Uninstall Secure Lifecycle

You must be a local administrator on the computer to uninstall Secure Lifecycle.

Copy Files to Your Local Drive

If you uninstall Secure Lifecycle from your computer or device, files on the sync client 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 from the DDP|SL virtual drive to your local drive.

These files, copied from the DDP|SL virtual drive, will display in cleartext. The folders and files on the sync client website will be encrypted, even if you download them. To view them, you must reinstall Secure Lifecycle.

Uninstall Secure Lifecycle

- 1 Use the Windows Control Panel to uninstall the program.
- 2 Select Dell Data Protection | Secure Lifecycle and click **Change** on the top menu.
- 3 Click **Next** when the Welcome screen displays.
- 4 Select **Remove** and click **Next**.
- 5 A warning displays to confirm if you want to uninstall Dell Data Protection | Secure Lifecycle. 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 Click **Finish** when the Completed screen displays.
- 9 Click **Yes** to restart.

Uninstallation of Dell Data Protection | Secure Lifecycle is complete.

Frequently Asked Questions

Miscellaneous FAQs

Question

I moved the cloud provider's sync folder to Program Files, and now I cannot decrypt the files that are being downloaded to my sync folder from the cloud.

Answer

By design, the Program Files folder or other excluded folders are unprotected, based on policy. Secure Lifecycle will not decrypt any files downloaded to this folder or its subfolders.

Solution

Unlink or uninstall the sync client and move the sync folder back to its default location or to an alternate managed location.

NOTE:

For a list of managed and unmanaged locations, contact your administrator.

Question

I had some archived .xen files, and I copied them to my desktop. Some of them decrypted, but others did not.

Answer

During a sync, Secure Lifecycle is designed to decrypt directly to the virtual drive or decrypt when downloading through a web browser. For files that have been copied from another location, use Windows Explorer and move the .xen file into the virtual drive to be decrypted.

Solution

Move the .xen files into the virtual drive folder to have them uploaded into the cloud. Then, they will be decrypted locally.

Question

I renamed my computer. Now, I am not getting any policy updates, and I am not encrypting into the cloud.

Answer

Currently, the Server only recognizes the endpoint against which you originally activated. If you change the endpoint name, the Server will not recognize the location for sending the policy and Secure Lifecycle will not perform as expected.

Solution

1 Stop syncing files to the local computer.

NOTE: If you do not stop syncing before uninstalling, valuable data may become unprotected in the cloud or possibly deleted.

2 Uninstall Secure Lifecycle and then reinstall. You must have Administrator rights to uninstall.

Question



On suspended Windows devices, when I try to upload files into the cloud, nothing happens. When I close the windows that were already opened, an error message states, Access Denied.

Answer

The error message is not from Secure Lifecycle. You can access the files locally but will not get future updates to the files.

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 Secure Lifecycle. Confirm that the Secure Lifecycle icon in the system tray has a green checkmark, indicating that it is activated.

Solution

Determine if you need to install or activate Secure Lifecycle. See [Install Secure Lifecycle](#) 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* checkbox is cleared.
- 6 Click **OK**.

