Users Quick Reference to get started with Dell Data Protection | Secure Lifecycle v1.1

This Quick Reference provides a brief introduction of the product and tips for getting started.

- Internal users, see **Internal Users – Install on Windows**.
- External users, see **Register as an External User**.

Purpose of Secure Lifecycle

Provides additional security for:

- Data that is stored in a cloud-based file sharing system
- Sensitive Office documents (**.docx, .pptx, .xlsx, .docm, .pptm, .xlsm**) that are stored locally, shared with other users in various ways, or stored on removable media

Options with Secure Lifecycle

You may have one or both of these options:

- **Cloud Encryption only** – Data stored in the cloud is encrypted as .xen files. Unauthorized users cannot view the data. On the client computer with Secure Lifecycle, a virtual drive (DDP|SL) displays the content in cleartext.
- **Protected Office Documents only** – two options exist:
  - **Opt-in** mode – you can determine which Office documents to protect.
  - **Force-Protected** mode – higher level of security.
  - For both options, Office documents that are protected retain the usual file extension, not a .xen extension.
- **Cloud Encryption** and **Protected Office**
  - Office documents that are protected retain the usual file extension in the cloud but display only a cover page if opened.
  - Non-Office files have a .xen extension in the cloud.

All Users - Before you begin

You must know:

- Which options you have and the level of security on Office documents
- Additional policies that impact security
- Fully qualified host name of the Dell Server – Required to install the product.
- Cloud storage provider to use – if the enterprise has a preferred provider.

Internal Users – Install on Windows

You must be a local administrator on the computer to install Secure Lifecycle.
See the *Secure Lifecycle User Guide*:

- **Chapter 3** – *Cloud Encryption* with or without *Protected Office Documents*
- **Chapter 4** - *Protected Office Documents* only

Before you install Secure Lifecycle:

- If you already have a cloud storage provider installed and have folders or files synced to the cloud, see **Chapter 3**.
- For Cloud Encryption, see the online help for your cloud storage provider before you deploy this product.

After you install:

- In the system tray, confirm that the Secure Lifecycle icon has a green checkmark.
- If Cloud Encryption is enabled for your enterprise, you must log in to your cloud sync client for File Explorer to display the DDP|SL virtual drive.

Important – Before you use Secure Lifecycle:

- If you plan to protect existing Office documents, make backups. A Secure Lifecycle Recovery tool exists for the administrator to recover and decrypt files, but Dell recommends making a backup.

Reminders/Tips for Protected Office

To determine which options you have:

- For *Protected Office Documents*, see Chapter 3 or 4 > *Observe File Menu Options to Determine the Level of Security for Office Documents*.
  Note: If you have *Protected Office* only, no DDP|SL virtual drive displays in File Explorer.
- If you save an Office document to protected mode and then open it in the cloud or on a device that does not have Secure Lifecycle, it is protected. Only a cover page displays. An unauthorized user cannot view your data.

Reminders/Tips for Cloud Encryption

- Chapter 3 has information on each cloud sync client that relates specifically to Secure Lifecycle. See the online help for your cloud storage provider for information related to a provider.
- When you log in to your cloud sync client, the virtual drive (DDP|SL) adds a cloud sync folder. Add files and sub-folders to the cloud sync folder, **not** at the root of the virtual drive.
- If you have both *Cloud Encryption* and *Force-Protected* mode, if you right-click on the virtual drive to create a new Office document, the document is protected as a .xen file but a sweep will not automatically make it a *Protected Document*. You must manually select **Protected Save As** from the File menu. You can drag protected Office documents to the virtual drive.
- With Opt-in mode (but not Force-Protected mode), a *Secure Documents* folder as added at 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 delete the folder, it is recreated.

Share with External Users

An internal user can share secure files with an external user. To grant access to external users, see the *Secure Lifecycle User Guide*.

Register as an External User

The first time that an external user receives a secure file, the Dell Enterprise Server sends an Account Verification email. The user must register and install Secure Lifecycle to view the file. The external user must be a local administrator on the computer:

1. In the Account Verification email, 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**. (You must reset a random password.)
5. At the Reset Password Page, enter and confirm your password, and then click **Register**. You will receive an email.
6. In your email, open an account activation email and click the link within.
   In the email, note the Server name.
7. Click **Return to Login** and enter the same email address and password you used to register. Click **Login**.
8. Download and install Secure Lifecycle.
9. Under Windows, click Download (32-bit) or Download (64-bit), depending on your computer's operating system.
10. Download the setup file to a directory on your computer.
11. Double-click the setup file to launch the installer and follow the wizard's instructions. **Note**:
    In the *Server Name* field, enter the name from the activation email you received.
    In the *Management Type* window, select **External Use**.
12. After you click **Finish**, click **Yes** to restart.

To activate as an external user:

1. Log in to Windows.
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**. A green check displays on the Secure Lifecycle system tray icon.