Dell Data Protection | Secure Lifecycle for Mac

Administrator Guide v1.0

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.

Secure Lifecycle for Mac Administrator Guide

2016 - 12

Rev. A01

Contents

1

Secure Lifecycle for Mac Introduction

This guide provides the information needed to administer the cloud client software for Mac.

Overview

Dell Data Protection | Secure Lifecycle for Mac protects data in cloud-based file sharing systems. Mac OS X computers using Secure Lifecycle can view, modify, and encrypt files on cloud-based file sharing systems for secure storage.

Secure Lifecycle for both Mac and Windows can open files encrypted by the other.

Secure Lifecycle for Mac is comprised of the following:

- Secure Lifecycle:
  - **Cloud Encryption** - protects data in cloud-based file sharing systems as .xen files.
  - **Protected Office Documents** - protects Office documents (Word, PowerPoint, or Excel) in the cloud, displaying the original filename and extension. If protected, the files can only be opened with a Secure Lifecycle client. If opened elsewhere, a cover page displays indicating that the document is protected and explains how an authorized user can request access to the encrypted file.

    You can set policies for Cloud Encryption only or both policy groups. For more information, see *Admin Help*.

    A word about Secure Lifecycle for Mac: Secure Lifecycle for Mac is designed for sharing files within cloud encryption providers. However, if "Protected Office Documents" policies are enabled for Macs, all file auditing and traceability is lost if the file is saved by the end user to the local Mac. If strict file auditing and traceability is needed in your organization, set the *Allow Mac Secure Lifecycle Activation* policy to "Not Selected" to prevent Secure Lifecycle from activating on Macs.
- Dell Security Server - a component of the Dell Server that manages Secure Lifecycle for Mac. The Security Server ensures data is secure in the cloud, no matter with whom it is shared. The Security Server also protects internal devices from passing on sensitive data.
- Remote Management Console - provides centralized security policy administration, integrates with existing enterprise directories, and creates reports.

  These Dell components interoperate seamlessly to provide a secure environment without detracting from the user experience.

Contact Dell ProSupport

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

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

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

Secure Lifecycle for Mac Requirements

Client hardware and software requirements are provided in this chapter. Ensure that the deployment environments meet the requirements before continuing with deployment tasks.

NOTE: IPv6 is not supported.

Encryption Client

Although the Encryption client is not required, Secure Lifecycle for Mac can be used with the Dell Enterprise Server v9.5 or later.

Mac Client Hardware

The following lists supported hardware for the Mac client.

Mac Hardware

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

Operating Systems

The following lists supported operating systems.

Mac Operating Systems

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

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 Storage Providers

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

Cloud Storage Providers

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Secure Lifecycle Installation Tasks

Prerequisites

Before performing these tasks, confirm the following:

- Install the Dell Server and its components. See one of these:
  - *Enterprise Server Installation and Migration Guide*
  - *Virtual Edition Quick Start Guide and Installation Guide*
- In the Remote Management Console, assign an appropriate Dell Administrator Role.

Policies

By default, Secure Lifecycle encrypts users' files and sends audit events to the DDP EE Server/VE Server. 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).

If you want audit events to include geolocation data, you must enable Wifi. For more information on geolocation and audit events, see *AdminHelp*.

To change default behavior for each supported cloud storage provider, set the *Cloud Storage Protection Providers* policy. If your enterprise prefers a specific cloud storage provider, set this policy to **Block** for other providers. For information about policies, see the *AdminHelp*, which is accessible from the Dell Server's Remote Management Console.

NOTE: This policy's Bypass option is for Windows. If you select Bypass for Mac, it displays as Allow to the end user.

Dell Enterprise Server Tasks

Set Up the Security Server to Allow Cloud Client Downloads

DDP Enterprise Server

1 On the DDP Enterprise Server, go to <Security Server install dir>\webapps\cloudweb\brand\dell\resources\

2 Open the **messages.properties** file with a text editor.

3 Ensure that the entries are as follows.

For **local** installation:

download.deviceWin.mode=local

download.deviceMac.local.filename=DDPSL-Explorer-0.x.x.xxxx.dmg

For **remote** installation:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

4 Save and close the files.

5 Go to <Security Server install dir> and create a folder named Download (Security Server\Download).
6 Within the Download folder, create a CloudWeb folder (Security Server\Download\CloudWeb).
7 Add the Secure Lifecycle installers to that folder.

Virtual Edition: Manually Install a Different Cloud Client Version

No action is needed to allow users to download the latest SecureLifecycle installer. The latest installer is preinstalled on the VE Security Server.

To manually install a different Secure Lifecycle installer version on the VE Security Server, update the message.properties file.

1 Go to:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Open the **messages.properties** file with a text editor.
For **local** installation:

```
download.deviceWin.mode=local

download.deviceMac.local.filename=DDPSL-Explorer-0.x.x.xxxx.dmg
```

For **remote** installation:

```
download.deviceWin.mode=remote

download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

3 Save and close the files.
4 Copy the files to /opt/dell/server/security-server/download/cloudweb.
5 Add the Secure Lifecycle installers to that folder.

Allow/Deny Users on Whitelist /Blacklist

The whitelist and blacklist entries determine which users can register with the Dell Server to use Secure Lifecycle.

Whitelist

The whitelist allows specific users or groups of users to register with the Dell Server and to use Secure Lifecycle.

External users must be placed on the whitelist to allow registration. See the following examples to allow users to register:

User Type	Enter
All organization.com email addresses	`<Allow>*@organization.com</Allow>`
All users	`<Allow>*<Allow>`
A specific user	`<Allow>jdoe@organization.com</Allow>`
All Gmail users	`<Allow>*@gmail.com</Allow>`

NOTE: If you have used a wildcard in the whitelist and want to use the blacklist, you must remove the wildcard.

Blacklist

The blacklist prevents specific users or groups of users from registering with the Dell Server and using Secure Lifecycle. Users whose email addresses are entered in the blacklist receive a message stating that they cannot register for Secure Lifecycle.

NOTE: If a user is already registered, this list does not prevent them from using Secure Lifecycle.

You can use the blacklist to exclude specific users who are members of approved groups on the whitelist. Additionally, using the wild card (*), you can place entire domains on the blacklist, which will prevent anyone with an email address in that domain from registering. See the following examples to prevent a user or group from registering with the Dell Server:

User Type	Enter
All organization.com email addresses	`<deny>*@organization.com</deny>`
A specific user and that email address	`<deny>jdoe@organization.com</deny>`
All Gmail users	`<deny>*@gmail.com</deny>`

To modify the whitelist/blacklist, follow these instructions:

1 Open the Security Server configuration folder.
Enterprise Edition: **<Security Server install dir>\conf**.

Virtual Edition: **/opt/dell/server/security-server/conf/**

2 With a text editor, open **registration-access.xml**

3 Allow or deny users based on the above information and the following example:
<?xml version="1.0" encoding="UTF-8"?>

```
 <access>
  <whitelist>
    <allow>user1@organization.com</allow>
    <allow>*@organization.com</allow>
    -->
    <allow>*</allow>
  </whitelist>
  <blacklist>
    <!--All addresses not specifically allowed are denied.
    <deny> </deny>
    -->
  </blacklist>
 </access>
```

```
<?xml version="1.0" encoding="UTF-8">
  <access>
   <whitelist>
      <allow>user1@organization.com</allow>
      <allow>*@organization.com</allow>
      -->
      <allow>*</allow>
   </whitelist>
   <blacklist>
      <!--All addresses not specifically allowed are denied.
      <deny> </deny>
      -->
```

```
    </blacklist>
  </access>
```

4 Save and close the file.

Remote Wipe a Dropbox for Business Team Member Account

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

Prerequisites

NOTE: Before you perform this procedure, you must back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.

Only a Dropbox for Business Administrator can remote wipe a Dropbox for Business account.

The end user must have activated Secure Lifecycle and connected to Dropbox for Business.

Register in Remote Management Console

Only one Dropbox for Business Administrator needs to register.

1 In the Remote Management Console's left pane, select **Management** > **Dropbox Management**.
2 On the Dropbox for Business page, click **Register**.
The browser opens to the Dropbox for Business site.
3 If prompted, log in to Dropbox with your Dropbox for Business Administrator account.
4 To allow access to Secure Lifecycle, click **Allow**.
A confirmation page displays to indicate Dropbox authorization is granted to the DDP Enterprise Server - VE.
5 In the Remote Management Console, return to **Management** > **Dropbox Management** and click **Refresh**.
The administrator name displays.

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

Remote Wipe a Team Member Account

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

1 In the Remote Management Console, select **Populations** > **Users** in the left pane.
2 Search for the specified user.
3 Access the **User Detail** page.
4 In the Command column, click **Remote Wipe**.
The remote wipe is performed.

NOTE: Before you select Remote Wipe, you must back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.

5 At the confirmation for Remote Wipe, click **Yes**.
The User Detail page lists the date the remote wipe is performed.
6 In your Dropbox for Business Administrator Console Members page, refresh the list of Team Members.
The user is removed from the list. You can select the **Removed Members** tab to view which users have been removed.

Client Tasks

Prerequisites

- Ensure that target devices have connectivity to:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Ensure that the user performing the installation has a local Administrator account for installing.
- If installing using the command line, ensure that you have the fully qualified domain name of the Dell Security Server that users will activate against.

Best Practices

During deployment, be sure to follow IT best practices. This includes, but is not limited to:

- Controlled test environments for initial tests
- Staggered deployments to users

Install Client

At this point, users who were added to the whitelist can register at: https://yoursecurityservername.domain.com:8443/cloudweb/register.

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

Installing the Mac client is optional for administrators, as end users will typically install the Mac client themselves (after registration) from https://yoursecurityservername.domain.com:8443/cloudweb.

However, you can install the Mac client if your organization requires you to do so. Install the Secure Lifecycle client through the user interface or by command line using any push technology available to your organization. Registration and Activation by the end user are both still required.

Upgrade From Previous Versions of Cloud Edition

If an enterprise has a previous version of Cloud Edition and upgrades to Secure Lifecycle, the previous version of Cloud Edition is removed.

NOTE: If the enterprise upgrades from Cloud Edition to Secure Lifecycle, users must authenticate and re-link Secure Lifecycle with their cloud storage provider. For more information on authentication, see the online Secure Lifecycle Help.

Install Options

To install/upgrade the client, select one of the following:

- Interactive Installation - This is the easiest method to install Secure Lifecycle for Mac. However, use this method only if you plan to install the client on one computer at a time.

  or
- Command Line Installation - For this advanced installation method, administrators must be experienced with command line syntax. This method can be used for a scripted installation, using batch files, or any other push technology available to your organization.

Interactive Installation

1 For Secure Lifecycle Client, locate the Installer in **DDPSL-Explorer-0.x.x.xxxx.dmg.**

2 Use the **.pkg** file inside DDPSL-Explorer-0.x.x.xxxx.dmg to install or upgrade. You can use a scripted installation, batch files, or any other push technology available to your organization.

3 Double-click the **DDPSL-Explorer-x.x.x** package.

4 Click **Continue**.

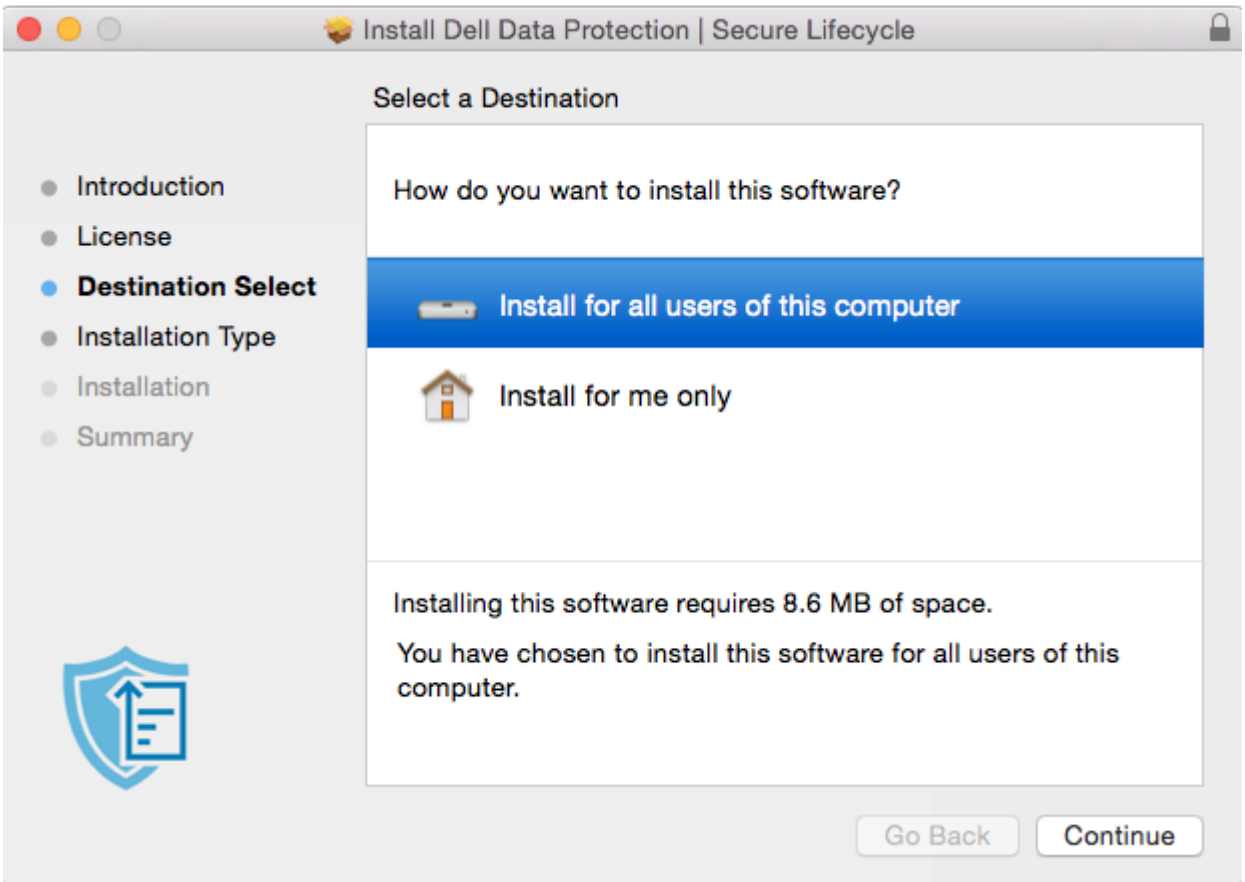
5 On the Introduction window, click **Continue**.

6 On the Software License Agreement window, click **Continue**.

7 Click **Agree** to continue.

8 On the Installation Type window, do one of these:

- Click **Install**, then go to step 9.
- On the Destination Select window, select an option below, click **Continue Installation**, then go to step 9.
  - Install for all users of this computer
  - Install for me only



9 In the dialog, enter your user name and password and click **Install Software**.

10 On the Summary window, click **Close**.

11 See End User Activation.

NOTE: If the enterprise upgrades from Cloud Edition to Secure Lifecycle, users must authenticate and re-link Secure Lifecycle with their cloud storage provider. For more information on authentication, see the online Secure Lifecycle Help.

Command Line Installation

1 Mount the .dmg.

2 Perform a command line installation of the package using the installer command:

```
sudo installer -pkg/Volumes/DDP\ Secure\ Lifecycle"DDPSL-Explorer\ 0.x.x.xxxx.pkg" -target /
```

3 Instruct end users to activate Secure Lifecycle. See End User Activation.

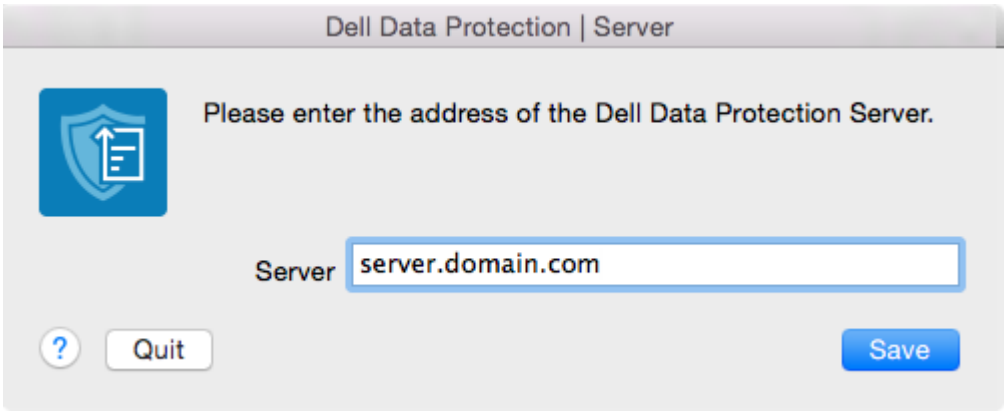
Secure Lifecycle Activation and User Experience

End User Activation

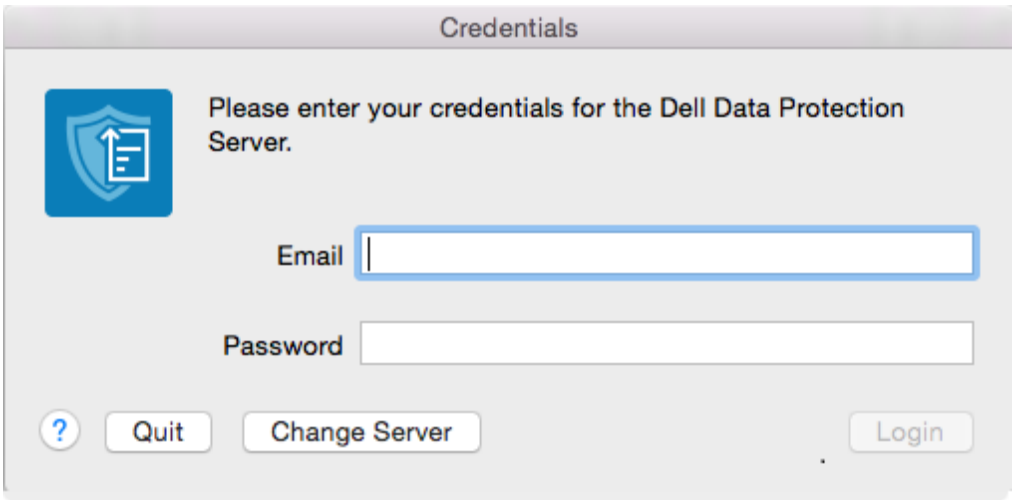
After you open Secure Lifecycle on the Mac for the first time, follow these steps:

1 In Finder, select **Applications**, and double-click **Secure Lifecycle**.

2 When the Dell Data Protection | Server window opens, enter the DDP Server address and click **Save**.



The Credentials window opens.

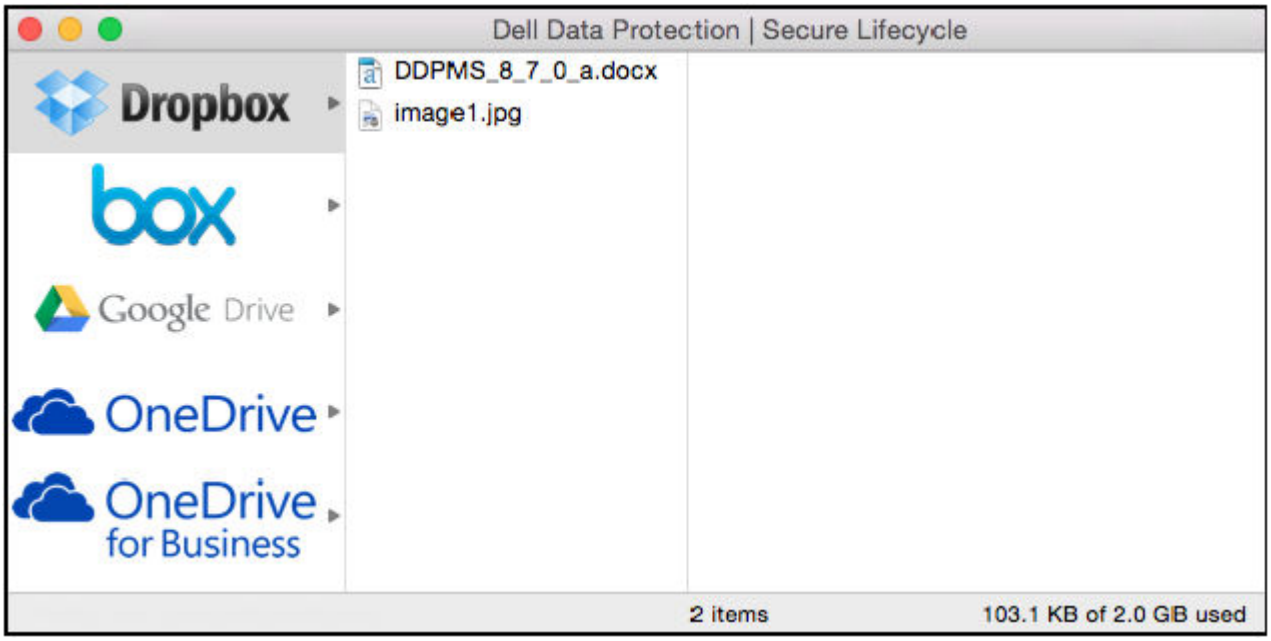


3 Enter your domain email address and domain password.

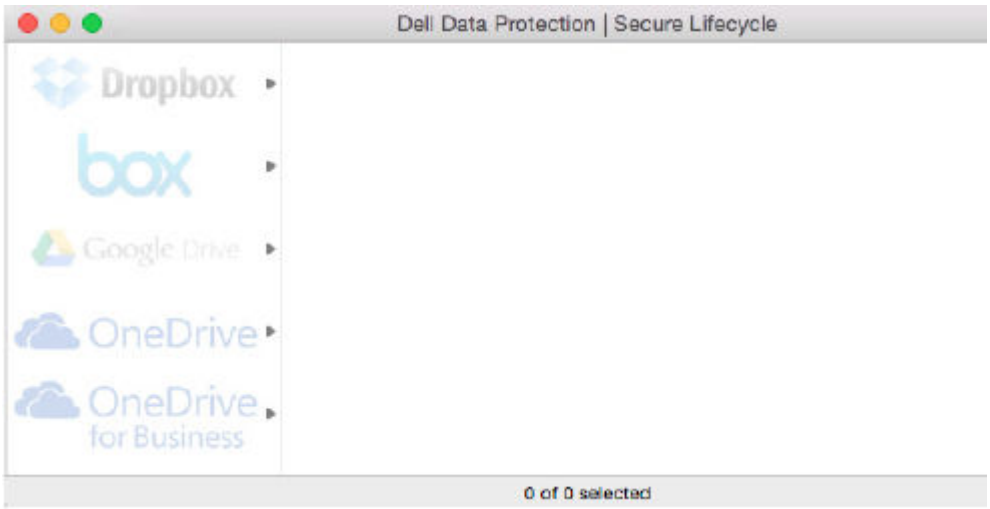
4 Click **Login** to activate Secure Lifecycle.

When the Dell Data Protection| Secure Lifecycle application opens and activation is successful, the cloud storage provider name is activated in the left pane.

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



If activation is not successful or if the authentication for the Secure Lifecycle application is revoked or expires, the cloud storage provider name is grayed out.



5 In the left pane, select the cloud storage provider.

A window opens, prompting for your credentials.

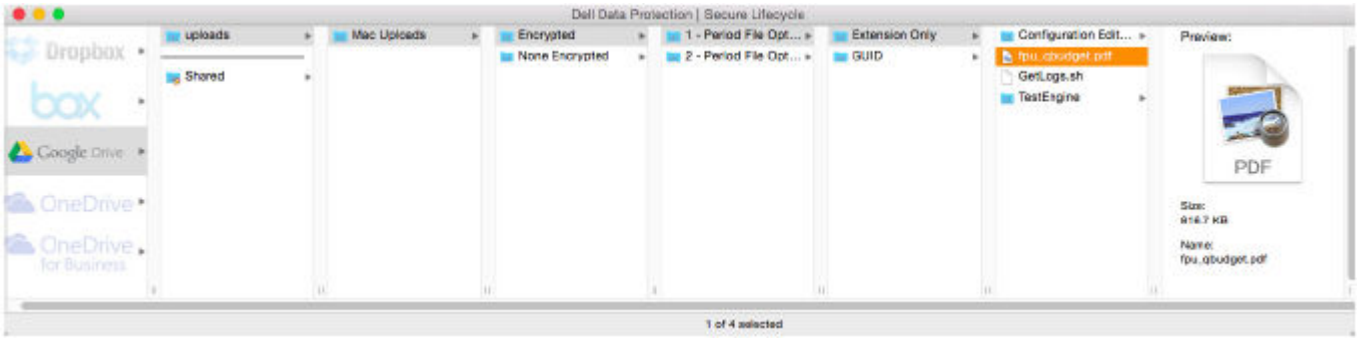
6 For more information on authentication, see the online Secure Lifecycle Help.

User Interface

The Secure Lifecycle interface is similar to the OS X Finder *View as Columns* interface. Each column represents a folder on the selected cloud storage provider.

NOTE: The title bar may vary depending on your operating system.

To encrypt and decrypt files, you must use the Dell Data Protection | Secure Lifecycle interface, not the cloud storage provider website.



You can perform these tasks in the Secure Lifecycle window:

- **File** > **New Folder** - To create new folders.

  NOTE: Google Drive and OneDrive automatically add a Shared folder. However, data sharing in OneDrive for Business is not supported.

- Context menu - Select one or more folders or files in the main window. Then, Control-click (or right-click) and select a menu option:
  - **Download**
  - **Rename** - When you rename a file in the Secure Lifecycle interface, Secure Lifecycle syncs the change on the cloud storage provider website. Do not rename a .xen file on the cloud storage provider website. It will not sync.
  - **Delete**

    NOTE: Google Drive with Secure Lifecycle does not have a Remove option (removes to trash). It has Delete only, to be consistent with other Secure Lifecycle functionality.
- **Unlink** - To unlink Mac Secure Lifecycle from a cloud storage provider, select the provider in the left pane, Control-click (or right-click), then select Unlink from the menu.

Additional information on files and folders:

- To add files and folders to folders shown in the Secure Lifecycle user interface, drag them from the OS X Finder or other applications that support drag and drop. Files will be encrypted based on current policy.
- To decrypt and open files in applications, double-click the file in the Secure Lifecycle window. If the file is modified in an external application, the modified file will then be encrypted and uploaded as a new revision on the cloud storage provider.
- To make an unencrypted local copy, drag a file or folder from the Secure Lifecycle window into Finder.
- Secure Lifecycle's *Cloud Encryption* 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 Secure Lifecycle interface.
- Extended attributes are not copied to the cloud.

Avoid Check Out option on website

Secure Lifecycle does not protect or encrypt files used with the *Open & Check Out* option on the OneDrive for Business website or any cloud storage provider website. If a file is open and checked out, do not use the Open command on the Secure Lifecycle interface as automatic upload will be blocked.

When protecting your files with Secure Lifecycle, use the Secure Lifecycle interface to work with files.

If you want to work on a file with special properties from a cloud storage provider website:

1 On the Secure Lifecycle interface, Control-click (or right-click) a file and select **Download**.
2 Select and edit the file.
3 Through Secure Lifecycle interface, upload the file.

Application Preferences

To launch Preferences:

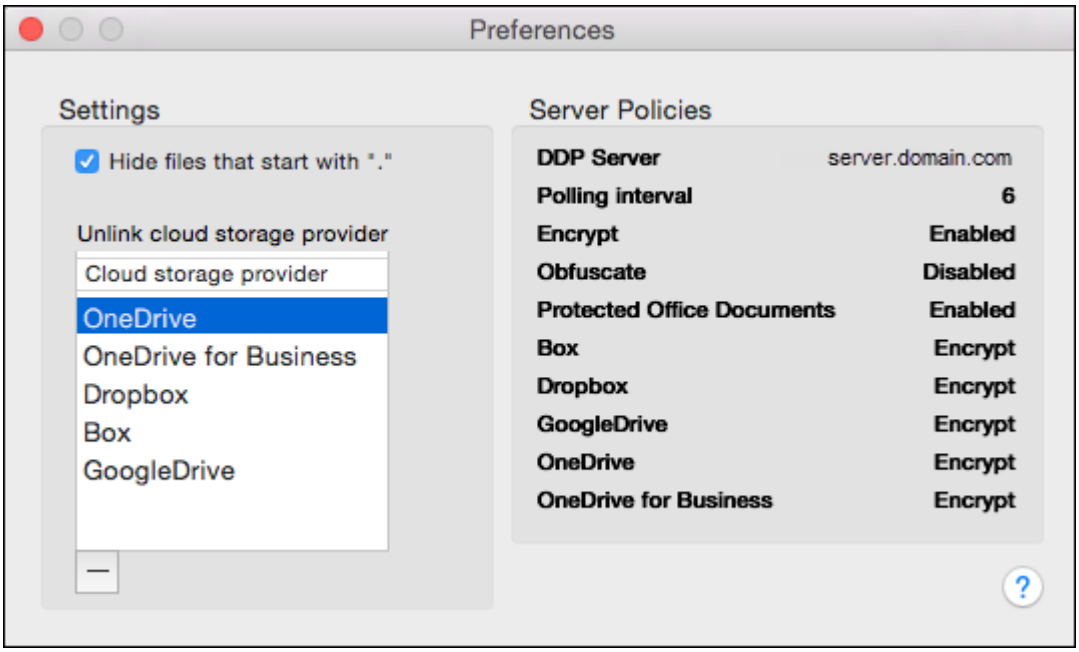
1 Launch Secure Lifecycle.
2 From the Secure Lifecycle menu bar, select **Preferences**.

NOTE: This information is also available from the Help icon.

You can modify these settings:

- Hide files that start with "." - By default, the box is checked, hiding the files. To see the hidden files, clear the check box.

  NOTE: Generally, files prefixed with a dot separator are hidden in the OS X Finder.



- **Unlink cloud storage provider** - Lists cloud storage providers authenticated by Secure Lifecycle. To remove a cloud storage provider from Secure Lifecycle, select the provider name, and click the minus (-) button at the bottom left of the Preferences window.

Server Policies - The DDP Server administrator sets the following policies that control how Secure Lifecycle manages files and folders:

- **DDP Server** - Lists the server URL.
- **Polling Interval** - Lists the interval in minutes that the client software polls for policy updates.
- **Encrypt** - Master encryption policy that allows encryption of folders and files on the cloud storage website.
- **Extension Only** or **Obfuscate**

  Extension Only (default policy setting) displays the filename on the website.

  If an enterprise requires additional protection for files, set this policy to Obfuscate to hide the filenames on the cloud website as GUID names.

  NOTE: If the policy is first set to Extension Only and users have files on the cloud website and then the policy is changed to Obfuscate, names of pre-existing files on the website will not be obfuscated. To obfuscate pre-existing filenames, the user must download and then re-upload the files through the Secure Lifecycle interface. Or, if the user edits a file, it will upload with an obfuscated filename.

- **Cloud Storage Protection Providers** - A provider name displays based on policy settings. Options are **Box**/ **Dropbox**/ **Google Drive** / **OneDrive OneDrive for Business**.

Enable or disable encryption of files uploaded to that cloud storage provider. One of the following displays:

- **Encrypt** - Files sent to the cloud are encrypted.
- **Allow** - The user can access files in the cloud but files sent to a cloud storage provider website are not encrypted.
- **Blocked** - The cloud storage provider is unavailable and at this time means that cloud storage provider name is not displayed in the main window.

- **Protected Office Documents** - protects Office documents (Word, PowerPoint, or Excel) in the cloud but displays the file extension, not a .xen extension.

  If this policy is enabled, Office documents (Word, PowerPoint, or Excel) in the cloud display the file extension, not a .xen extension. However, the file cannot be opened in the cloud or if downloaded. If opened, only a cover page displays, stating that the document is protected. If you have installed Secure Lifecycle but not authenticated, the cover page will indicate that.

Security and Other Considerations for Secure Lifecycle and Cloud Sync Clients

Google Drive

Secure Lifecycle's *Cloud Encryption* encrypts folders and files in the cloud to protect data. Be aware of these considerations.

- Corporate security policy, set to Protect, prohibits use of Google Docs with Secure Lifecycle. If set to Allow, you can edit them. 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. Google Docs that you create display in your Google Docs cloud storage provider folders.

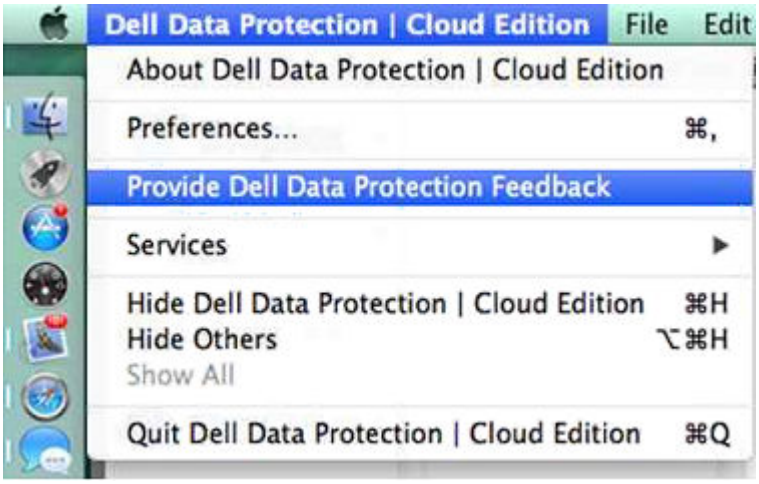
  However, if you open the folder, a dialog warns you that Secure Lifecycle cannot encrypt that document.

OneDrive for Business

Data sharing in OneDrive for Business is not supported.

Feedback About This Product

If enabled by policy, users can provide feedback about Secure Lifecycle. The feedback form is available from the menu bar > **Provide Dell Data Protection Feedback**.


Dell Data Protection | Cloud Edition
File
Edit
About Dell Data Protection | Cloud Edition
Preferences... ⌘,
Provide Dell Data Protection Feedback
Services
Hide Dell Data Protection | Cloud Edition ⌘H
Hide Others ⌥⌘H
Show All
Quit Dell Data Protection | Cloud Edition ⌘Q

5

Secure Lifecycle Uninstallation Tasks

This section describes the administrator process for uninstalling Secure Lifecycle. If an end user has a local Administrator account, they can uninstall Secure Lifecycle for Mac themselves.

Prerequisites

You must have a local Administrator account to perform the uninstallation.

Uninstall Secure Lifecycle

Do one of these to remove Secure Lifecycle:

Finder

1 While pressing the <option> key, select **Go** from the menu bar.
2 Open the **~/Library/Application Support/Dell** folder.
3 Remove the **SecureLifecycle** folder.
4 From **Go** in the menu bar, open the Applications folder and remove the **Secure Lifecycle** application.

Terminal

You may have Secure Lifecycle in one or both of the following locations.

1 Use one or both of these commands:
   - rm -R ~/Applications/Secure\ Lifecycle.app
   - rm -R ~/Library/Application Support/Dell/SecureLifecycle
2 Remove the **SecureLifecycle** folder.

6

Glossary

Activate(d) - Activation occurs when the computer has been registered with the Dell Server and has received at least an initial set of policies.

Dell Enterprise Server - The Dell Enterprise Server is made up of a collection of components. When referring to the Server-side of the product as a whole, it is collectively known as the Dell Enterprise Server.

Remote Management Console - The Remote Management Console is the administrative console for the entire enterprise deployment. The Remote Management Console is one component of the Dell Enterprise Server.

Security Server - a component of the Dell Server that manages Secure Lifecycle. The Security Server ensures data is secure in the cloud, no matter with whom it is shared. The Security Server also protects internal devices from passing on sensitive data.

External Users - Users outside the organization's domain address.