Dell Data Protection | Secure Lifecycle

Technical Advisories 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.

Secure Lifecycle Technical Advisories

2017 - 02

Rev. A01

Contents

1

Technical Advisories

This document provides information about Secure Lifecycle features and changes in each major release, any issues resolved from a prior release, and any technical advisories in the current release. Secure Lifecycle provides data security, wherever it goes - data at rest, data in motion and data in use - through encryption. Data Loss Prevention (DLP) ensures no data is lost in motion or in flight, while Digital Rights Management (DRM) defines access and usage control. Additionally, file monitoring provides detailed data usage visibility to support forensics needs. Secure Lifecycle provides security, authority, visibility, and cross-platform compatibility - all through a single solution - with the following features:

- Auditing and reporting on file activity, files synced, files accessed by whom, where and when, and compliance reporting.
- Geolocation with map visualization as well as multiple filtering options for audit events.
- Enforcement of full access lists/blacklists of email domains and addresses for control over file sharing.
- Enforcement of policies for access to cloud services, folders, and applications.
- Management of key expirations and polling periods.
- Ability of administrators to monitor all known IP addresses for cloud service providers and match them with the application process to centrally manage encryption, encryption keys, data recovery, policies and forensics.

Secure Lifecycle Protected Office mode offers enhanced security on Office documents (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) for internal users.

- Files remain encrypted for unauthorized users, for example, when files are attached in email, moved in a web browser or File Explorer, or stored on removable media.
- A callback beacon can be inserted into every protected Office file, when the beacon server is installed as part of the Dell Server Front End/Proxy Mode installation.
- Protected Office documents are supported with Mozy, our companion solution, as well as other cloud, email, and nfs storage products.

New Features and Functionality v1.1

- Secure Lifecycle now offers the following:
  - Audit events logs can now be exported from the Dell Server to SIEM.
  - Protected Office Mode now protects macro-enabled Office documents (.docm, .pptm, .xlsm).
  - File sharing is improved with introduction of the Full Access List, which replaces the Whitelist and Graylist, in the Dell Server Remote Management Console.
  - Internal users now auto-activate after installation.
  - When Office documents or macro-enabled documents are created on an Android or iOS client that is not connected to the Dell Server, keys are generated offline and then uploaded to the Dell Server the next time the device is online.
  - New geofencing policies for Android and iOS clients allow administrators to restrict protected Office document and .xen file access to a specified region. Regions currently include the United States and Canada.

Resolved Technical Advisories v1.1

Secure Lifecycle

- Encryption sweep performance is improved. [DDPCE-4183]
- An issue is resolved that previously prevented the Save As function in Google Drive to overwrite a protected file with an unprotected update to the file. [DDPCE-4275]

Secure Lifecycle Mobile Application

- The bookmark feature now functions as expected on iOS and Android operating systems. [DDPCE-4124, DDPCE-4160]

Technical Advisories v1.1

Secure Lifecycle

- When a protected macro-enabled document is opened in Excel, the macro cannot be edited from the **Macros** menu. To work around this issue, use **Alt+F11** to open the macro editor. [DDPCE-4418]
- On rare occasion, Secure Lifecycle may display an error when opening or saving protected files. To work around this issue if it occurs, follow these steps:

  a From the Windows Start menu, select **Run**, then enter `services.msc`.

  b Delete the following files from the **C:\Program Files\Dell\Dell Data Protection\Secure Lifecycle** folder:

  XendowData.xdb

  XendowSys.xdb

  xendow.xtc

  c Restart the computer.

  [DDPCE-4420]
- When an internal user attempts to grant protected file access to an unprotected file, an error displays rather than a message that the file is unprotected and, therefore, does not need to be shared. [DDPCE-4461]
- After upgrade from Cloud Edition v2.0, issues may occur with certificates and systray application functionality. To work around these issues, follow instructions in *Cloud Edition User Guide* to uninstall Cloud Edition, and then install Secure Lifecycle. [DDPCE-4474]
- A date-protected Word file stored in a mapped drive does not show the date-protection period in **File** > **Info** when the file is opened from the mapped drive. [DDPCE-4566]
- If auto-activation fails, disable auto-activation on the client computer. To disable auto-activation, create the following registry key:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Secure Lifecycle]

  "DisableAutomaticActivation" =dword:00000001

  To re-enable auto-activation, delete the registry key.

  [DDPCE-4573]
- On a computer running Windows 10 and Office 2016, the **Protected Save As** menu item is disabled after setting a date restriction and saving an Excel file. [DDPCE-4587]

New Features and Functionality v1.0

Technical Advisories v1.0

Secure Lifecycle

- When Folder Management is enabled, the Dropbox option remains in Folder Management after Dropbox is uninstalled. [DDPCE-417]
- Files cannot be downloaded directly from a cloud storage provider's website. To work around this issue, open files in the Secure Lifecycle virtual drive on the client computer. [DDPCE-1511]
- When a new folder is created in the Secure Lifecycle virtual drive and a new file is added to it, the help file specified in the Help File Name and Help File Contents policies is not added to the folder. [DDPCE-1824]

- When a user with a personal Dropbox account joins a Dropbox for Business team, the user must restart the computer in order for Secure Lifecycle to protect all Dropbox files. [DDPCE-1854]
- If a cloud profile is removed from the Cloud Storage Protection Providers policy, files can be uploaded in cleartext. Cloud profiles are included in the policy value by default and must remain there. [DDPCE-1888]
- If Google Drive is installed before Secure Lifecycle activation, files can be uploaded in cleartext until activation. Dell recommends that sync clients are not installed prior to Secure Lifecycle activation. [DDPCE-1951]
- If the Obfuscate Filenames policy is changed, only new folders and their contents are named based on the policy change. Existing folders and their contents are named based on the Obfuscate Filenames policy value at the time the folder is created. [DDPCE-1956]
- When the Dropbox Encrypt Personal Folders policy is Not Selected, a folder that is cut and pasted from a personal Dropbox folder to a Dropbox for Business folder is not encrypted. [DDPCE-1957]
- When a file is downloaded to a computer and decrypted, a copy of the file with a .xen extension remains. The copy of the .xen file can be deleted. [DDPCE-2297]
- A protected Word or Excel file can be inserted into an unprotected non-Office file (.txt or .csv) if the non-Office file is opened with Word or Excel and the user inserts it as an object. Embedded Office files are not supported with protected Office mode. [DDPCE-2591, DDPCE-2647]
- When accessing Dropbox files after uninstalling Secure Lifecycle, an error displays that says Dropbox refers to a location that is unavailable. To work around this issue, repair or reinstall Dropbox after uninstalling Secure Lifecycle. [DDPCE-2666]
- When a OneDrive file is uploaded from a computer without Secure Lifecycle installed, a placeholder file (.plh) is created in the Secure Lifecycle virtual drive. Attempting to open the file results in a File Access Denied error. To work around this issue, simply delete the .plh file. [DDPCE-2702]
- Syncing a file that is copied and modified outside the sync folder then pasted back into the sync folder occasionally requires more time than syncing other files. [DDPCE-2717]
- If the sync client is not installed on the computer, protected Office documents cannot be opened in the Office application by selecting the Open in Protected View option and entering the file name. [DDPCE-2818]
- If the administrator installs Secure Lifecycle, the user must be logged in when the administrator enters the administrative user name and password. If the user is not logged in, the Secure Lifecycle directories are placed in the administrator's User folder. The user gets an unknown error and cannot open protected Office files. [DDPCE-2992]
- Added 2/2017 - After two or more Excel copy/cut and paste operations in rapid succession on a computer running either Windows 7 or Office 2010, Secure Lifecycle becomes unresponsive. With other OSs and Office versions, Excel occasionally returns an error, but Secure Lifecycle continues to function as expected. [DDPCE-3246]
- With Secure Lifecycle and protected Office documents, users can have multiple PowerPoint or Word documents open. However, if a user selects multiple protected PowerPoint or Word documents in Windows Explorer, right-clicks, and selects **Open** from the menu, an error message may display or some files may fail to open. If this occurs, open the documents one at a time or, for multiple documents, select **File > Open**. [DDPCE-3287]
- Some files may remain after deleting multiple Google Drive files from the Secure Lifecycle virtual drive. To work around this issue, delete the files in the browser or from the command line. [DDPCE-3366]
- When running protected Office mode, saving an existing Word file does not convert it to a protected Office file. To work around this issue, select **File > Save As** and rename the file. [DDPCE-3448]
- New files in pre-existing sync client folders are encrypted rather than remaining unencrypted as expected when Secure Lifecycle is installed and the Force Protected File Only policy is Selected. [DDPCE-3594]
- When the Enable Time to Live and Embargo Control policy is Selected, a previously unprotected file is protected even if the user cancels after selecting to Date Restrict/embargo the file and does not save edits. [DDPCE-3692]
- Audit events are not uploaded to the Dell Server if the user removes the audit certificate from the Windows store. To work around this issue, restart the computer to regenerate the audit certificate. This is possible since the certificate remains in memory although it has been removed. Ensure that certificates are not purged through Group Policy. [DDPCE-3820]
- Added 2/2017 - After canceling an operation to add a date restriction to a file, the Secure Lifecycle window is unresponsive for a short time. [DDPCE-3845]
- Secure Lifecycle protects the Clipboard when a user copies from a protected Office document and pastes to an unprotected location. This impacts **Open > Recent** if a user selects a recent Office file and right clicks to select **Copy path to clipboard**. Currently, for Office 2013 and 2016, if a user has a protected Office document open or if the enterprise has policies set for Force-Protected mode, the user cannot paste any path in the list to an unprotected location. The user must manually type the path or paste it into a protected Office document. [DDPCE-4130]

Secure Lifecycle Mobile Application

- When a large number of PowerPoint (.pptx) files with images and videos are added to the sync client folder after the application has been continuously open and in the foreground, a timeout may occur and the application becomes unresponsive. [DDPCE-3632]
- A few Dropbox items are not translated in the Android application. [DDPCE-3643]
- Files can still be made available offline although an Android device is suspended. [DDPCE-3652]

- Shared folders are not visible in the iOS application for Google Drive or OneDrive or in the Android application for OneDrive. [DDPCE-3755, DDPCE-3756, DDPCE-3757]
- In the iOS application, more than one file instance (offline and online) is created if a protected Office document is edited and saved multiple times while the network connection is intermittently interrupted. [DDPCE-3937]
- An incorrect file path displays in Audit Logs for a document created with the Android application on Google Drive or OneDrive for Business. To work around this issue, use the file name rather than the path for audit data. [DDPCE-4022]
- On rare occasion, the Android application is unable to provision a sync client in **Settings**. To work around this issue, retry provisioning. [DDPCE-4045]
- Occasionally, the iOS application may become unresponsive when a file is synced over a slow network connection. [DDPCE-4163]
- The file path in Audit Logs is an empty value for a document created with the iOS application. To work around this issue, use the file name rather than the path for audit data. [DDPCE-4239]
- In the iOS application, out-of-range Date Restricted/embargoed files can be copied from one sync folder to another. [DDPCE-4303]

2

Software and Hardware Compatibility

Secure Lifecycle is tested with third-party software and hardware as needed. Dell reports problems found during testing to other vendors, where appropriate.

Hacks and Utilities

- Hacks or utilities that alter device manufacturer performance specifications are not supported. For example, the AfterBurner hack adjusts the clock speed of a device processor, affecting the results of certain math operations. Because some of these math operations are required for encryption and decryption, using this hack could lead to data corruption.