Dell Data Guardian for Mac

Technical Advisories v1.2

Notes, cautions, and warnings

ⓘ | **NOTE: A NOTE indicates important information that helps you make better use of your product.**

△ | **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

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

Technical Advisories

2017 - 05

Rev. A02

Contents

Dell Data Guardian for Mac Technical Advisories

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

Data Guardian for both Mac and Windows can open files encrypted by the other.

Data Guardian for Mac is comprised of the following:

- Data Guardian:
  - **Cloud Encryption** - protects data in cloud-based file sharing systems as .xen files.
  - **Protected Office Documents** - protects Office documents (.docx, .pptx, and .xlsx) and macro-enabled documents (.docm, .pptm, and .xlsm) in the cloud and on disk, displaying the original filename and extension. If protected, the files can only be opened with a Data Guardian 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*, accessible from the Remote Management Console.

    A word about Data Guardian for Mac: Data Guardian 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 Data Guardian Activation* policy to Not Selected to prevent Data Guardian from activating on Macs.
- Dell Security Server - a component of the Dell Server that manages Data Guardian 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 product.

Additionally, online support for Dell 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.

New Features and Functionality v1.2

- Dell Secure Lifecycle has been rebranded to Dell Data Guardian.
- Amended 05/2017: Apple released macOS Sierra 10.12.5 on 05/15/17 and is now supported.
- macOS Sierra 10.12.4 is now supported.
- External users with Data Guardian installed and activated on Windows, Mac, or a mobile device can now directly and immediately request file access from internal users. Administrators can grant or deny access through the Dell Remote Management Console when internal users are unavailable.

- Additional protection is available for protected Office documents through the Print Control policy, which allows the administrator to control whether a document can be printed and, if printed, contain a watermark with the name, domain, and computer ID of the user who prints it.
- 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.
- Internal users can now allow access to protected files sent to external users through Outlook in one easy step before the email is sent.
- A new context menu option allows users to quickly protect an unprotected Office document by simply right-clicking the file.
- A new Dell Data Guardian tab is available in File Properties of a protected Office document, with the file's Key ID and access and embargo data.
- A new audit event tracks when an external user requests access to a file.

Dell Data Guardian for Mac Technical Advisories v1.2

- A OneDrive for Business user cannot access an encrypted (.xen) file from an internal account when the file is uploaded to the cloud with an external account and the Server policy, Obfuscate Filenames, is set to Guid. [DDPCE-5079]
- An error may occur when attempting to bulk upload a large number of OneDrive for Business files. To work around this error if it occurs, upload fewer files at one time. [DDPCE-5244]
- Adding multiple folders to Google Drive may result in duplicated, rather than incremented, folder names. To work around this issue, rename folders as they are added. [DDPCE-5264]
- Google Drive Sign in to link to Dell Data Guardian fails when the user is not signed in to a Google account. [DDPCE-5348]
- Downloading a Google Drive file that is larger than 500 MB may result in a timeout error. [DDPCE-5351]

New Features and Functionality v1.1

- macOS Sierra 10.12.3 is now supported.
- 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.

Resolved Technical Advisories v1.1

- An Upload Error no longer occurs when the user attempts to replace an encrypted file. [DDPCE-4330]
- PDFs can now be deleted and renamed without having to close and restart Secure Lifecycle. [DDPCE-4393]
- Protected Office files now open and display the protected Office watermark as expected. [DDPCE-4427]
- Audit events are now reported to the Dell Server as expected. [DDPCE-4450]
- Secure Lifecycle no longer becomes unresponsive when Cloud Encryption is disabled on the Dell Server while Secure Lifecycle is running. [DDPCE-4456]
- An issue is resolved that occasionally prevented connection with OneDrive. [DDPCE-4463]
- Files can now be successfully renamed in Box. [DDPCE-4464]
- An issue is resolved that caused Secure Lifecycle to become unresponsive after the user deleted files from Box and then attempted to open a file. [DDPCE-4496]

Secure Lifecycle for Mac Technical Advisories v1.0

- Added 4/2017 - If a user drags the Secure Lifecycle application to the trash, credentials such as email and Dell Server name may remain in the key chain. If the user reinstalls with a different Server, to work around this issue, click **Change Server** and enter the new Server information when Secure Lifecycle is launched. [DDPCE-1121]
- Bulk uploads to Box occasionally fail with a timeout error. To work around this issue, reduce the upload size. [DDPCE-3308]
- Added 4/2017 - Downloading a OneDrive file that is larger than 500 MB may result in a timeout error. [DDPCE-3311]
- With Dropbox, if a user copies bulk data, the progress bar may remain and not indicate that it has copied all folders and files even when it has. The user can confirm that folders and files have been copied and then close the dialog. [DDPCE-3700]
- The buttons in the Select a Destination installer dialog are disabled. To work around this issue click either option, **Install for all users of this computer** or **Install for me only**, to enable them. [DDPCE-3795]

- When the Enable Callback Beacon policy is Selected and a callback beacon is inserted into protected Office 2011 and online Office versions' .pptx files, some files are not reported on the Dell Server as beacon events. These beacon events are reported when files are opened from Office 2016 or Office 365. [DDPCE-4341, DDPCE 4336]
- Added 4/2017 - After upgrade from Cloud Edition to Secure Lifecycle, the user's cloud storage provider may be unlinked from Secure Lifecycle. To work around this issue, relink the cloud storage provider to Secure Lifecycle. [DDPCE-4351]