Dell Data Guardian

Technical Advisories v2.8

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.

2019 - 07

Rev. A01

Contents

1

Data Guardian Technical Advisories

This document provides information about Data Guardian features and changes in each major release, any issues resolved from a prior release, and any technical advisories in the current release.

Data Guardian provides security, authority, and forensic visibility - all through a single solution. The product is available from Windows, Mac, or iOS and Android mobile devices with cross-platform compatibility. The Data Guardian web portal, if set up by the administrator, allows internal and external users to view or edit encrypted files in a web browser, without installing the Data Guardian client.

Protect - Based on policies, Data Guardian can encrypt data in many file types to protect data at rest, data in motion, and data in use.

- **Basic File Protection** - The enterprise administrator defines non-Office file extensions to protect. A sweep encrypts those file types.
- **Office documents** (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) - Policies determine the level of security:
  - **Opt-in protection** - The user chooses which Office documents to protect.
  - **Forced protection** - A sweep protects all Office documents stored on the local computer, providing a higher level of security.

  If an unauthorized user tries to open the file, only a cover page displays. However, users can grant access to an external user, and the cover page provides information for viewing the encrypted file on a mobile device or the Data Guardian web portal.

  Protected Office documents are supported with Mozy as well as other cloud, email, and NFS storage products.
- **Data Classification (Windows with opt-in mode)** - For users who classify Office documents that contain sensitive information, like credit card numbers, a Data Guardian sweep can encrypt specified classification types to prevent unauthorized access.
- **Outlook email protection (Windows)** - Based on policy, users can protect email attachments or the entire email. If sent to an external person, the internal user can later revoke access of the key so the external user can no longer open it.
- **Cloud protection** - Documents uploaded to the cloud from Android or iOS mobile devices are protected.

Control - This product provides authority and Digital Rights Management (DRM) to the administrator to define access and usage control:

- Enforcement of full access lists/blacklists of email domains and addresses for control over file sharing.
- Management of encryption key expirations and polling periods.

Monitor - To support forensic needs, file monitoring provides detailed data usage visibility. Based on policy, it can include:

- 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.
- A callback beacon can be inserted into each protected Office file if the beacon server is installed as part of the Dell Server Front End.
- Ability to monitor all known IP addresses for cloud service providers and centrally manage encryption keys and data recovery.

Topics:

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.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

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

New Features and Functionality v2.8

Windows v2.8

- For interactive or command line installations, the only option is internal users. If an external user has Data Guardian installed from an earlier version and tries to upgrade, a dialog displays. External users can install Data Guardian on an iOS or Android mobile client or the web portal to view encrypted files.
- Windows 10 supports ISO Version 1903 (May 2019 Update/19H1).
- When Data Guardian's *Email Encryption via Outlook* policy is enabled, the Protect button is still created. However, when a protected email is open, the Outlook workflows in the Quick Access bar and Ribbon, like Move options, are no longer blocked. Data in motion can still be protected but reenabling these workflows results in an improved user experience.
- When a protected email displays the cover page, only internal users can open the protected email. External users cannot view a protected email.

- Data Loss Prevention (DLP) now focuses on Data Guardian's mobile clients and web portal. In Windows, some workflows have been reenabled to improve performance. Therefore, the following policies no longer apply for Windows in Data Guardian v2.8 and higher:
  - Block Print Screen
  - Print Control
  - Export Control
  - Protected Office Document Process Protection
  - Protected Office Clip Board Unauthorized Text
  - On Screen Watermark
  - No red border displays on protected Office documents or protected emails.
- With Access Groups in an on-prem environment, an administrator can set an additional policy to allow the owner of a file to right-click an Outlook email that they protected and sent to users in their access group. The owner of a file can remove an individual's access to that email.

Mac v2.8

- macOS Mojave 10.14.6 is now supported.
- External users can no longer install Data Guardian or upgrade an earlier version to v2.8. External users can install Data Guardian on an iOS or Android mobile client or the web portal to view encrypted files.

Mobile v2.8

- iOS 12.3 is now supported.

Web Portal v2.8

- OneDrive for Business has a *Save to cloud storage provider* option.

Technical Advisories v2.8

All Platforms v2.8

- In an on-prem environment, Data Guardian clients must be able to communicate with the Security Server with the correct protocol, name of the Dell Server, and port, for example https://server.domain.com:8443. Port 8443 is the default. If an enterprise uses a customized port, the administrator must inform users. [DDPCE-14562]

Windows v2.8

- If a user removes the Data Guardian plugin from Outlook, the user may need to uninstall and reinstall Data Guardian to enable the plugins. Administrators should clarify that users should not remove the Data Guardian plugins. [DDPCE-6198]
- If Data Guardian is installed to a non-default location, for example, C:\Data Guardian, the Office plugins are not automatically installed and a dialog states *Publisher cannot be verified*. The installer must select *Install* or *Don't Install*. [DDPCE-13231]
- Recent updates to Adobe Reader DC have modified its signing signature, which is to verify the application. Data Guardian can no longer verify the integrity of the updated Adobe Reader DC, so Adobe Reader DC is blocked from launching to protect sensitive data. Dell is working with Adobe on a permanent resolution. The current workaround is to leverage Adobe Reader 19.10.20098.316574 or earlier. To find previous releases of Adobe Reader DC, see:

  https://supportdownloads.adobe.com/product.jsp?product=10&platform=Windows. [DDPCE-13627]
- Data Guardian has been tested and functions as expected with Windows 10 Defender Exploit Guard, Credential Guard, or with Hypervisor-protected code integrity (HVCI) enabled. [DDPCE-13701, 13702]
- Currently, if email encryption is enabled and a user selects Share on an open, unprotected PDF and then attaches it to Outlook email and sends it as unprotected, the recipient may see an error dialog and not be able to open the PDF. Until resolved, users should attach the unprotected PDF directly in Outlook. [DDPCE-14168]
- For on-prem with Access Groups enabled, when right-clicking an encrypted PDF and selecting *Protected File Access*, the pre-share user interface may not display. To work around this issue, place the encrypted PDF in a cloud storage provider and select **Protected File Access**. [DDPCE-14253]
- When email encryption is enabled and a user selects a [PROTECTED] email from the *Inbox* or *Sent Items* and then selects **Actions > Resend This Message**, the sender must then close the Resend window and is prompted to save the changes. If the sender clicks **No**, the preview pane of the [PROTECTED] email is unprotected and without the cover page. [DDPCE-14476]
- Data Guardian and Microsoft's Azure Information Protection (AIP) are not mutually compatible. If a user protects an Office document with AIP and then uses Data Guardian's right-click or Protected Save As to protect the document an error dialog displays and the user cannot open the protected document. [DDPCE-14491]

Mac v2.8

- No technical advisories.

Mobile v2.8

- Currently, for Android mobile devices with Data Guardian, audit logs are not generating when a user deletes a .xen file or when a user selects File Upload. [DDPCE-12287]
- If an enterprise enables Data Guardian for mobile devices, they must configure their firewall so that users can use the mobile devices on the company network. [DDPCE-14562]

Web Portal v2.8

- Currently, to save or undo changes to a document in OneDrive for Business accessed from the web portal, the user can click the red X in the upper-right to discard changes or click the X on the tab to save changes and close the tab. An Undo button allows the user to undo changes one at a time. [DDPCE-8418, DDPCE-14587]
- As an administrator, when configuring Network Settings for the web portal and using a static IP address, it may take 30 seconds for the IP address to be properly assigned to the web portal. During the Certificate transfer dialog, if the IP address incorrectly displays a previously acquired static IP address, ignore it. Use the configured static address. [DDPCE-12991]
- Currently, users must use the exact web portal URL listed on the cover page. Modifying the form of the URL may redirect to the web portal but could result in unexpected behavior in a browser or cloud storage provider due to cached data. [DDPCE-13846]

New Features and Functionality v2.7

Windows v2.7

- Windows was not released with the other platforms for Data Guardian v2.7.

Mac v2.7

- macOS Mojave 10.14.4 and 10.14.5 are now supported.
- The *Allow File Exclusions* policy, that adds the *Unprotected Documents* folder to users' computers, allows Data Guardian to decrypt file types listed in Basic File Protection as well as Office documents.

Mobile v2.7

- iOS 12.2 is now supported.

Web Portal v2.7

- Based on policy, the Data Guardian web portal can access and open files in OneDrive for Business.

Technical Advisories v2.7

Windows v2.7

- Since Windows was not released with the other platforms for Data Guardian v2.7, any technical advisories are listed in v2.8.

Mac v2.7

- After installing Data Guardian, the sweep agent relaunches other processes, like Explorer, to consume the policies based on the policy poll interval. [DDPCE-13781]

Mobile v2.7

- No technical advisories exist.

Web Portal v2.7

- No technical advisories exist.

New Features and Functionality v2.6

All Platforms v2.6

- In an on-prem environment and if the administrator enables the feature for Access Groups, internal users have a pre-share option for protected Office documents and files encrypted with Basic File Protection. The *Protected File Access* pre-share user interface allows users to select one or more access groups when sharing a protected file. External users who own a file can use the pre-share option.
- In an on-prem environment, when a cover page displays for a protected file, the web portal URL displays so that users can click to access the web portal.

Windows v2.6

- When enabled by Data Classification and Email Classification policies, emails that contain data in the body that meets the classification rules will send an Audit or Encrypt event.
- A policy allows the administrator to create one or more folders to exclude protection of files that would be encrypted through Basic File Protection. This applies to Force Protected or Opt-in mode.
- If an administrator removes file extensions from the *Basic File Protection Configuration* policy, a one-time sweep occurs when the policy is changed.
- A Share audit event occurs for Data Guardian's Access Groups.
- If policy allows the user to protect Outlook email and the encrypted email needs to be recovered, the forensic administrator can drag the encrypted emails directly from Outlook. The administrator can now drag multiple emails. They are not compressed and do not need to be extracted. Encrypted emails are decrypted to a Destination folder, not to individual additional folders.

Mac v2.6

- A policy allows the administrator to create one or more folders to exclude protection of files that would be encrypted through Basic File Protection. This applies to Force Protected or Opt-in mode.
- Decryption for Basic File Protection.

Resolved Technical Advisories v2.6

Windows v2.6

- Occasionally, when an internal user opens a protected Excel file directly from OneDrive, the cover page displays and the file does not open. An error dialog now displays for any encrypted Office document that fails to open: *An error has occurred while opening the file. Please verify that you are trying to open the file from File Explorer. If this issue persists, please contact your administrator*. [DDPCE-11849]

Technical Advisories v2.6

Windows v2.6

- Currently, when configuring a folder where users can exclude files that are being swept and encrypted through the Basic File Protection policy, avoid these environment variables: %USERNAME%, %HOMEPATH%, %USERPROFILE%, %TEMP%, %TMP%. The workaround is to use the KNOWNFOLDERID string to configure the policy. [DDPCE-8221]
- With Data Guardian and TITUS versions prior to 2019.0, if Outlook is opened for several days, an error message may display. To work around this issue, close and reopen Outlook if it has been open for some time. If the error continues, restart your computer. The best practice is to upgrade to TITUS 2019 or later. [DDPCE-11292]
- If the administrator removes a file extension from the Basic File Protection Configuration policy field, the Properties > Dell Data Guardian tab and file overlay icon may be removed during the one-time sweep before the file has finished decrypting. Users may need to wait several minutes for the file to fully decrypt. If any encrypted files with that extension are missed during the one-time sweep, for example, if the file is open or was stored on a file server or other location, the administrator can use the Recovery Tool to decrypt. [DDPCE-13272]
- Currently, Data Guardian may have a compatibility issue with the PhishAlarm plugin used in Microsoft's Outlook for Windows. If Outlook does not open after installing Data Guardian, see https://support.office.com/en-us/article/turn-an-add-in-off-for-outlook-for-windows to disable the PhishAlarm plugin. [DDPCE-13830]

Mac v2.6

- If the administrator removes a file extension from the Basic File Protection Configuration policy field, the *Properties > Dell Data Guardian* tab and file overlay icon may be removed during the one-time sweep before the file has finished decrypting. Users may need to wait several minutes for the file to fully decrypt. If any encrypted files with that extension are missed during the one-time sweep, for example, if the file is open or was stored on a file server or other location, the administrator can use the Recovery Tool to decrypt. [DDPCE-13272]

Mobile v2.6

- No technical advisories exist.

Web Portal v2.6

- No technical advisories exist.

New Features and Functionality v2.5

All Platforms v2.5

- To enhance security for an on-prem environment, administrators can enable a feature for Access Groups in the Management Consoleand apply the feature to User Groups that consist of internal and external users.

  NOTE:

  In the Management Console, the feature name, *Circle of Trust* on the *Services Management* page and *User Groups > Details and Actions*, is changing to *Access Groups* in v2.6. The v2.5 documents reflect that change.

Windows v2.5

- A *File Overlay Icon* policy allows administrators to control the overlay icon.

Mac v2.5

- If the administrator creates a custom port number, users can activate with it.

Mobile v2.5

- Office 2019 is now supported for iOS.
- Chromebook is supported for Android.

Resolved Technical Advisories v2.5

Windows v2.5

- Print screen within Outlook works as expected when the Block Print Screen option is disabled. [DDPCE-10828]
- An issue resulting when an external user tries to open a message from another external user and accepts to request access has been resolved. [DDPCE-12152]
- Resolved an issue with internal communication that would result in logins taking longer than expected. [DDPCE-12231, DDPSUS-2493]

Mac v2.5

- When *Allow MAC Data Guardian Activation* is disabled and a Mac user attempts activate against the specified Dell Server, a message of " Activation for this platform are currently disabled. Please contact the server administrator for more details." now displays. [DDPCE-9939]
- Hidden watermark works as expected for .pdf files when files are encrypted by uploading the file to a configured cloud service provider using Data Guardian. [DDPCE-10666]

Mobile v2.5

- Data Guardian app no longer becomes unresponsive when opening files larger than 4 MB. [DDPCE-9485]
- When using Data Guardian on an Android device, OneDrive can now be unlinked offline. [DDPCE-10656]
-

Technical Advisories v2.5

Windows v2.5

- Currently, if the administrator enables or disables the *File Icon Overlay* policy, users must manually refresh any opened File Explorer to view the correct file overlay behavior. If enabled and the overlay icon does not display for users, the administrator can navigate to the Microsoft Registry, **HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers**. Rename the Data Guardian **OverlayIconExt** key to move it within the top ten registry keys for that folder, for example, by adding spaces to the beginning. [DDPCE-11931, DDPCE-12648]
- Rarely, if you manually activated against a SaaS server, sometime later your computer may not create or open protected documents. The workaround is to right-click the Data Guardian icon in the notification area, press **Ctrl-Shift** and select **Details**, then click **Deactivate**. To reactivate with SaaS credentials, click the Data Guardian icon in the notification area and click **User Activation**. [DDPCE-12752]

Mac v2.5

- For Mac Data Guardian, to avoid security issues with XML eXternal Entity (XXE) Injection attacks, be sure your Mac operating system has libxml2 2.9.4 or higher installed. Typically, this is automatically installed with macOS Sierra 10.12.6 and higher. [DDPCE-12629]
- Mac Data Guardian has security measures, but if the cloud storage provider's login page is compromised, it could cause a redirect to an insecure site where data loss could occur. [DDPCE-12659]
- Be aware that, in some places, the cloud storage providers API involves HTTP Get instead of HTTP Post. [DDPCE-12660]

Mobile v2.5

- No technical advisories exist.

Web Portal v2.5

- No technical advisories exist.

New Features and Functionality v2.4

Windows v2.4

- For Workspace ONE and MSI installations, Visual Studio C++ 2017 Redistributable Package is required.
- Data Guardian v2.4 and higher on Windows is supported in Air Gap environments, but with some limitations. Currently, geolocation data in audit events and embargo files are not supported. Web beacon is supported with additional configuration.
- A red outline border displays for protected Office documents and emails.
- For protected Office documents, the right-click option has changed from *Grant Protected File Access* to *Protected File Access*.
- Currently, Data Guardian's Cloud Encryption protection has been disabled on Windows to prevent compatibility issues with newer functions of cloud service providers. To view files already protected with Cloud Encryption, use Data Guardian's Mobile app, web portal, or Data Guardian with Mac.

Mac v2.4

- For a Hosted solution, if a tenant has been suspended, a message displays when a user closes Explorer.

Mobile v2.4

- Office 2019 is now supported for Android.
- Data Guardian's Mobile app is compatible with Workspace ONE (formerly VMware Airwatch). Single Sign-on is available with Workspace ONE.

Web Portal v2.4

- Web portal has support for Microsoft Hyper-V.

Resolved Technical Advisories v2.4

Windows v2.4

- Protected documents no longer fail to open with Office 2013 when Data Guardian is configured in disconnected mode. [DDPCE-11812, DDPSUS-2468]

Mac v2.4

- An issue resulting when requesting access for multiple shared files to an external user has now been resolved. [DDPCE-11786]

Mobile v2.4

- Adding several images simultaneously to the Data Guardian application works as expected. [DDPCE-9532]
- Office 2019 is now supported for Android. [DDPCE-9753, DDPCE-9754]

Technical Advisories v2.4

Windows v2.4

- Occasionally, if a user selects multiple protected Office documents in File Explorer, right clicks, and selects **Open** from the menu, an error message may display that the file is currently in use. To work around this issue, attempt to reopen the file one at a time. For multiple files, select **File > Open**. [DDPCE-3287]
- For Basic File Protection, the .odt file extension was moved from the certified list to the partially supported list. [DDPCE-11833]
- Currently, Data Guardian's Cloud Encryption protection has been disabled on Windows to prevent compatibility issues with newer functions of cloud service providers. To view files already protected with Cloud Encryption, use Data Guardian's Mobile app, web portal, or Data Guardian with Mac. [DDPCE-12222]

Mac v2.4

- No technical advisories exist.

Mobile v2.4

- No technical advisories exist.

Web Portal v2.4

- No technical advisories exist.

New Features and Functionality v2.3

Windows v2.3

- Data Guardian for Windows is compatible with Workspace ONE. For Workspace ONE, the Data Guardian installer has an .msi file.
- The cover page for protected Outlook email has been updated.
- Data Classification has improved detection for phone validations.

Mac v2.3

- macOS Mojave 10.14.3 is now supported.

Mobile v2.3

- The cover page URL has been updated.

Resolved Technical Advisories v2.3

Mac v2.3

- During installation of Data Guardian, "Install for me Only" selection is no longer available for users to select. [DDPCE-10807]

Technical Advisories v2.3

Windows v2.3

- For the Block Print Screen policy to block this option for users, Data Guardian must be installed and run on the client operating system, not a VM or Remote Desktop. [DDPCE-11612]

Mac v2.3

- No technical advisories exist.

Mobile v2.3

- No technical advisories exist.

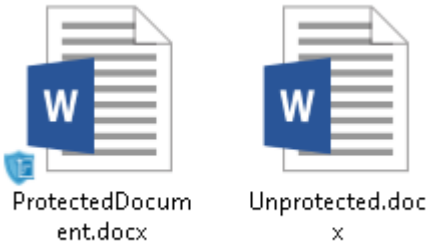
Web Portal v2.3

- Currently, when uploading a PowerPoint or PDF to the web portal, you may not be able to slide to view more than the first page. Either select the page in the left sidebar or use the Previous/Next arrows at the bottom right. [DDPCE-11305]

New Features and Functionality v2.2

Windows v2.2

- Microsoft Office 2019 is now supported.
- Data Guardian now adds an icon to protected documents once they have been encrypted.



Mac v2.2

- Microsoft Office 2019 is now supported.

Web Portal v2.2

- Microsoft Office 2019 is now supported.
- The Basic File Protection policy provides the ability to create new Basic File Protection files from clear text based on the policy.

Resolved Technical Advisories v2.2

Windows v2.2

- Dell Data Guardian no longer prompts for activation for already activated users. [DDPCE-2756]

- PDFs now support Modify Audit Events for protected Office documents. [DDPCE-10452]

Mac v2.2

- Files inside file bundles are no longer encrypted. [DDPCE-10546]
- Files are no longer encrypted in the Unprotected Documents folder. [DDPCE-10686]

Mobile v2.2

- Resolved an issue where pressing the back button on devices running Android operating systems would result in the application closing instead of returning to the home screen for Data Guardian. [DDPCE-10385]

Web Portal v2.2

- [SaaS] An issue resulting with a beacon sent multiple times when transitioning the file between read-only and editable has been resolved. [DDPCE-9533]
- A static IP address is no longer pre-configured on the Data Guardian Web Portal. [DDPCE-11103]

Technical Advisories v2.2

Windows v2.2

- When using Dropbox, overlay icons may not display properly. [DDPCE-11152]
- When recovering Data Guardian protected files, the source and destination locations in the Recovery Tool must be disparate. If the locations defined are the same location, data will not be properly decrypted. [DDPCE-11233]

Mac v2.2

- Users who were blacklisted and subsequently removed from the blacklist are not able to re-activate the Data Guardian app on their devices. To resolve, uninstall and re-install Data Guardian to allow the previously blacklisted user to re-activate. [DDPCE-10937]
- When deleting large amounts of data, Data Guardian may become unresponsive. To work around this issue, simply close and re-open Data Guardian. This issue does not result in any unexpected data loss. [DDPCE-11138]
- When an iOS endpoint has been activated multiple times, the endpoint may display multiple hostnames in the Management Console. For more information, see http://openradar.appspot.com/35746735. [DDPCE-11235]
- An error message of "Policy Error" may display when clicking **About Dell Data Guardian** and cause the application to close. [DDPCE-11829]

Mobile v2.2

- Office 2019 is currently not supported for iOS. [DDPCE-9753, DDPCE-9754]

Web Portal v2.2

- When attempting to open a document within the Data Guardian Web Portal, an error may display with the text "Unauthorized WOPI Host. Please try again later and report to your administrator if the issue persists". To resolve, see KB SLN315062. [DDPCE-11102]

New Features and Functionality v2.1

All Clients

- Data Guardian supports Dell Security Center (SaaS).

Windows v2.1

- Added 12/2018 - Microsoft Windows 10 October 2018 Update is now supported.
- Automatic tenant detection and provisioning is supported. When a user provides an email address and password, the system automatically determines the needed configuration information and sends all the needed data to the client allowing an activation against the intended tenant. If the user exists in more than one tenant, then the system will prompt the user to select one of the available tenants.

Mac v2.1

- macOS Mojave 10.14 and 10.14.1 are now supported.
- Automatic tenant detection and provisioning is supported. When a user provides an email address and password, the system automatically determines the needed configuration information and sends all the needed data to the client allowing an activation against the intended tenant. If the user exists in more than one tenant, then the system will prompt the user to select one of the available tenants.

Mobile v2.1

- Automatic tenant detection and provisioning is supported. When a user provides an email address and password, the system automatically determines the needed configuration information and sends all the needed data to the client allowing an activation against the intended tenant. If the user exists in more than one tenant, then the system will prompt the user to select one of the available tenants.

Web Portal v2.1

- Post Share key request is now supported. When a user attempts to upload or open a protected document without access to it, the user is able to request access with Post Share.

Resolved Technical Advisories v2.1

Windows v2.1

- An audit event is created when printing is blocked after enabling Force Protection. [DDPCE-7218]
- Attached encrypted emails in an encrypted email to an internal user are now supported. [DDPCE-8734, DDPCE-9817]
- Powerpoint works as expected when attempting to overwrite and unprotected powerpoint file with a protected file. [DDPCE-9244]
- To open an unprotected PDF without normal protection mechanism (process blocking, internet access restriction, save restrictions, etc.) being active while a protected PDF is open, close Adobe and re-open only the unprotected PDF. [DDPCE-9514]
- Custom folder locations are currently cached during user login when Dell Data Guardian is installed. If locations for Libraries or other document folders are modified, a reboot or a log off/log on cycle will be required for the affected user. [DDPCE-9556]
- Sent Mail items work as expected with Dell Data Guardian installed. [DDPCE-9772]
- An issue resulting with the removal of a PDF embargo file when an external user saves over a PDF embargo file has now been resolved. [DDPCE-9851]
- Multiple Audit Events are no longer generated when a file meets the criteria of a Classification rule set to Audit only. [DDPCE-9870]

Mac v2.1

- Dell Data Guardian for Mac no longer displays a "spinning wheel" when attempting to load a preview for a protected file with a BMP extension. [DDPCE-8569]
- The right-click Protect option is now available when a user opens Data Guardian for the first time after an installation. [DDPCE-9839]

Technical Advisories v2.1

Windows v2.1

- [SaaS] If Microsoft Office prompts an activation panel , an error message of "An unknown error has occurred" displays when opening an Office document. To avoid this issue, ensure Microsoft Office is activated before Dell Data Guardian is used. [DDPCE-9157]
- Files within Dell Data Guardian may be flagged against various threat prevention applications. For more information on exclusions and a list of files that maybe flagged as unsafe, and a list of suggested exclusions for various Anti-Virus and EDR applications, see https://www.dell.com/support/article/us/en/04/sln305980. [DDPCE-9777]
- When a user opens an encrypted email with a logo, the logo is replaced with the logo from the current user's computer. If the user replies or forwards the encrypted email, then the new message displays the new logo. [DDPCE-9933]
- Emails sent with a protected message following New Items > Email Message Using > More stationery results with a .gif file and a blank stationary for the recipient. A similar issue occurs when a recipient replies to an unprotected message including images and smart shapes with a protected email. [DDPCE-10012]
- When trying to save an Excel file, the Save button may be disabled. To work around this issue, use Save As instead of Save. [DDPCE-10565]
- Depending on policies set by an administrator, an error message for data classification may display at the endpoint. The message is harmless and can be safely dismissed. [DDPCE-10674]

- If a user's authentication token expires before any offline keys have been uploaded to the server, disconnecting, and subsequently reconnecting to the network will force the keys to upload. [DDPCE-10764]

Mac v2.1

- [SaaS] If a user enters an invalid email ID with a domain name that belongs to a configured Tenant, the user will be redirected to Azure to login. [DDPCE-10214]
- When using Google Drive, canceling an in-progress upload and immediately re-uploading the same document creates 2 stored copies of the document. To work around this issue, instead of canceling an upload, allow the file to upload completely and then upload the correct document to overwrite the first document. [DDPCE-10633]
- Added 11/2018 - In rare circumstances, when using Dropbox and attempting to perform multiple file changes, Data Guardian may stop updating, and appear hung. To work around this issue, if the DDG application enters a hung state, re-start the application. [DDPCE-10634]
- The error message that is displayed to the user when Data Guardian is not connected to Internet is not translated to the set locale. [DDPCE-10636]
- Added 02/2019 - When a user edits a protected Office document and saves with a Save As, the file is saved to a temporary folder as a default instead of the local folder. [DDPCE-10662]
- When Data Guardian Audit Data is enabled by policy, a hidden watermark used for tracking purposes is not properly updated or added to a protected document when the file is modified. Audit events involving the protected file's modification or creation are properly logged as expected, though "beacon" data will not be available for that file. [DDPCE-10667]
- When an external user attempts to access embargoed files that are expired or have future embargo dates, an incorrect message is displayed stating that the wrong Dell Server was being contacted for access to the file. The correct message displayed should alert the external user that the embargo date is in the future or has expired. [DDPCE-10669]
- Attempting to access hidden documents on macOS within Dell Data Guardian may erroneously message that the document was generated against a different Dell Security Management Server. [DDPCE-10728]

Mobile v2.1

- Data Guardian for iOS only supports the use of certificates that can be verified by the root certificates that is pre-loaded in the iOS certificate repository.

  Useful Certificate Information

Use of certificates on iOS	https://support.apple.com/en-us/HT204477
Manually add certificates	https://developer.apple.com/library/archive/qa/qa1948/_index.html
Trusted root certificates	https://support.apple.com/en-us/HT204132
Deploying certificates	https://www.apple.com/hk/en/ipad/business/docs/iOS_6_Certificates_Sep12.pdf

  [DDPCE-9733]
- An unregistered external user will get an account locked error message, rather than an authentication failure error message when using Data Guardian on a mobile device. [DDPCE-10103]
- User name and email address may not display on the Menu screen and Setting screens on iOS devices if the app is closed unexpectedly at the PIN screen. To work around this issue, the app must remain open during the initial pin setup. [DDPCE-10164]
- When the device display for Data Guardian is set to the largest font size, some text may not fully display on the device screen. [DDPCE-10188]
- When swapping user accounts on Data Guardian mobile, the previous user account may show in the menu, and may display if on-screen watermark is enabled for either of the mobile users. [DDPCE-10632]
- When using Data Guardian on an Android device, OneDrive cannot be unlinked offline. To work around the issue, re-connect the device and then unlink OneDrive. [DDPCE-10565]
- Occasionally, blacklisted users that have been recently removed from the blacklist in the External User Management page within the Dell Security Management Server may be required to uninstall and re-install the Dell Data Guardian mobile application. [DDPCE-10684]
- When a user attempts to save a file after logging in to a hosted environment and then disconnecting the network before entering their pin, a message "Error in saving file" displays and file does not save. To work around this issue, the user must login online at least once for a hosted environment after setting up the pin to create files in offline mode. [DDPCE-10221]
- Added 11/2018 - Devices running Android 9.X (Pie) may not immediately send audit events or beacon events from these devices due to battery optimization settings introduced in this operating system release. When Dell Data Guardian and Microsoft Office applications are removed from battery optimization or once the device connects to power, these event are sent successfully. [DDPCE-11165, DDPCE-11256]

Web Portal v2.1

- No technical advisories exist.

New Features and Functionality v2.0.1

Windows v2.0.1

- Added 09/28/2018 - Data protection for email is now available. In this initial release, a preview of Data Loss Prevention (DLP) is included with future releases continuing to add further improvements. As always, data in motion is protected, including protected Office documents, files protected by Basic File Protection, and emails protected by Data Guardian.

  Some actions are disabled or blocked to minimize DLP when an encrypted email is open:

  - Outlook's Quick Steps
  - Move, Move to Folder, and additional Folder actions
  - Next and Previous arrows
  - Forward
  - Some right-click options

  These actions are controlled to minimize DLP when an encrypted email is open:

  - Copy/Paste
  - Print and Export of data
  - Some right-click options
  - Draft folder and Autosave

Resolved Technical Advisories v2.0.1

Windows v2.0.1

- A cover page no longer displays for a protected email when access has been granted. [DDPCE-9578]
- Emails sent to an external user from the draft folder no longer require external user to request access to the file with Post Share. [DDPCE-9823]

Technical Advisories v2.0.1

Windows v2.0.1

- The copy/paste feature is currently blocked when a user attempts to copy/paste from one protected email to another protected email. [DDPCE-9012]
- In some cases, after a protected email has been sent and added to the sent folder in Outlook, the protected email is unable to open or be forwarded. [DDPCE-9706]
- In rare occurrences, the "ProtectEmail" message attachment displays in the Outlook preview window. To read a protected email, double-click the email, not the attachment, to open the pop-up window and read the email. Deleting the attachment results in the removal of protected email content. [DDPCE-9763]

Mac v2.0.1

- No technical advisories exist.

Mobile v2.0.1

- No technical advisories exist.

Web Portal v2.0.1

- No technical advisories exist.

New Features and Functionality v2.0

Windows v2.0

- Dell IP Data Classification: allows administrators to choose which files should be encrypted based on content.
  - In Windows for Office documents and PDFs, the *Data Classification Rules* policy allows administrators to select rules that enforce encryption on sensitive data.
  - The Classification rules can be set at the Enterprise, Endpoint Groups, or Endpoints populations.
  - The *Data Classification Rules* policy allows administrators to modify:
    - Classification Name and Priority - The policy lists sample classification names with default priorities that administrators can modify:
    - - *Restricted* - priority 3 , the highest
      - *Internal Use* - priority 2
      - *Public* - priority 1 , the lowest. The lowest priority displays (default) after the classification name, and no rules or actions apply.
    - Actions:
      - **Encrypt** - If administrator selects the **Encrypt** check box for a non-default classification, the system encrypts the files.
      - **Audit** - By default when the **Classification** policy is enabled, the Audit action applies to all files matching the non default classification level .
    - Rules: For configured rules, the system will sweep and detect them when a user saves the file.
    - Elements: Options for configuring a rule, such as Credit Card number, US Name, Social Security Number, or Tags.
-

Mac v2.0

- Added 01/2019 - The Basic File Protection policy provides the ability to select specific extensions and own processes outside of protected office documents to encrypt any file for motion with the same Digital Rights Management (DRM) capabilities currently offered with protected office documents.

Mobile v2.0

- Added 01/2019 - The Basic File Protection policy provides the ability to select specific extensions and own processes outside of protected office documents to encrypt any file for motion with the same Digital Rights Management (DRM) capabilities currently offered with protected office documents.

Web Portal v2.0

- Added 01/2019 - The Basic File Protection policy provides the ability to select specific extensions and own processes outside of protected office documents to encrypt any file for motion with the same Digital Rights Management (DRM) capabilities currently offered with protected office documents.

Resolved Technical Advisories v2.0

Windows v2.0

- A pop-up message displays when Data Guardian blocks the snipping tool after opening a protected PDF. [DDPCE 7361, DDPCE-7385]
- Files are no longer converted to temporary files after saving a protected document over a file with the same file name. [DDPCE-7398]
- Documents that are decrypted through an exclusion folder are now properly identified during the audit event. [DDPCE-8152]
- Data Guardian protected files no longer generated multiple keys per file. [DDPCE-8168]
- Data Guardian icons no longer disappear or become unresponsive after upgrading to Windows 10, 1803, update. [DDPCE-8181]
- Block PrintScreen engages as expected when the Dropbox sync client is installed and configured to save screenshots to Dropbox. [DDPCE-8247]
- A toaster is now generated when PrintScreen is blocked and File Protection is enabled. [DDPCE-8276]
- An issue resulting with protected documents being removed from the network after making changes to a protected PDF has been resolved. [DDPCE-8333]
- Resolved an issue that resulted in performance degredation over time with Dell Data Guardian. [DDPCE-8495]
- Data Guardian is now able to protect documents that may exceed the default maximum file path. [DDPCE-8551]

Mac v2.0

- Uploading files to OneDrive no longer becomes unresponsive with user account almost full. [DDPCE-8266]

Mobile v2.0

- Search filters are working as expected on the Content Security Policy screen when a user opens Data Guardian on an iOS. [DDPCE-7325]

Web Portal v2.0

- The viewer and Editor menus are localized to Japanese language. [DDPCE-6644]
- Users are able to open encrypted files not encrypted by Data Guardian when logged in and browsing for secured PDF files. [DDPCE-7332]

Technical Advisories v2.0

Windows v2.0

- When connected remotely to a machine with a paused installation of Data Guardian, the copy/paste features become unresponsive on the host machine. To work around this issue, disconnect from the remote machine. [DDPCE-5931]
- With Basic File Protection enabled to encrypt mp3, mp4, and wav files, an error message displays "File not supported" when attempting to open these files on a computer with Windows April 2018 Update. [DDPCE-8979]
- Added 11/2018 - Data Guardian is unable to open tampered Office files with the exception of Word files. To work around this issue, the recovery application can be used to open the tampered files. [DDPCE-9107]
- Added 11/2018 - Currently, Data Classification is unable to verify unprotected Office documents (.docx, .docm, .xlsx, .xlsm, .pptx, .pptm, .pdf) over 2GB. [DDPCE-9331]
- During the removal of Dell Data Guardian from programs and features a 'Modify' option is present. This presents a menu of options for various components for Dell Data Guardian. Currently no action can be taken per-component. It is suggested to back out of this screen and either 'Repair' or 'Remove' Data Guardian. [DDPCE-9528]
- In some cases, a reboot may be required when background sweeps has been enabled and memory allocation reaches close to capacity. After a reboot, the memory usage is expected to return to a normal state. [DDPCE-9711]
- Added 11/2018 - After clicking Protect and saving the email using Ctrl + S keys, the email gets saved into drafts but remains unprotected. To work around this issue, open the email from the draft folder and click Protect to send the encrypted email. [DDPCE-9767]
- Files may not be accessible for an external user when the remote Dell Security Management Server is not accessible and a Dell Data Guardian protected document has been created and sent. To work around this issue, ensure the remote server is accessible when attempting to open a Protected Office Document and a request to access the document is displayed. [DDPCE-9837]
- Removable disks are automatically swept and encrypted by Basic File Protection and Data Classification. To work around this issue, turn Basic File Protection and Data Classification off when inserting an external drive. [DDPCE-9977]

Mac v2.0

- When uploading files with invalid characters to OneDrive, a completion message of "Upload is Successful" or "Upload failed" fails to display. The file count during the upload is also inaccurate. [DDPCE-9241]

Mobile v2.0

- Added 11/2018 - Filtering workflows for files will be disparate for iOS and Android. [DDPCE-9060]
- Once a Protected Office Document has been saved with a *Save As* , the audit trails shows a new file has been created instead of an overwritten file. The audit trails should only show new protected files have been created. [DDPCE-9073]
- Currently, linking Dropbox Personal and Dropbox Business with the same user credentials are not supported. [DDPCE-9161]
- After entering an incorrect password with the correct email in the Data Guardian app, the login screen continuous to reload and becomes unresponsive. To work around this issue, ensure the credentials provided to Dell Data Guardian are correct for the desired user account. [DDPCE-9228]
- When an external user logs into the Data Guardian app, a tenant screen displays before the PIN screen instead of only the PIN screen displaying. The tenant screen requires the user to click Submit before the user is redirected to the PIN screen. [DDPCE-9758]
- When a user sets the preferred language by navigating to **Setting > Language & Region** to a language not supported by Data Guardian, the default is the previous supported language instead of defaulting to English. [DDPCE-9786]
- In rare occurrences, an error messages of "Null" displays when attempting to unzip a file that has been zipped multiple times. [DDPCE-9792]

- OneDrive for Business may not properly bind initially due to a rare communication issue with OneDrive. To resolve, attempt to add the OneDrive for Business account again. [DDPCE-10320]

Web Portal v2.0

- No technical advisories exist.

New Features and Functionality v1.6/v1.3

All Clients

Windows v1.6

- Data Guardian agents detect and encrypt files based on Titus Classification. Files identified with certain classification based on Titus will automatically encrypt as a protected office document. Based on Data Guardian policy, administrators can determine which Titus classifications will be encrypted automatically.
- The Basic File Protection policy provides the ability to select specific extensions and own processes outside of protected office documents to encrypt any file for motion with the same Digital Rights Management (DRM) capabilities currently offered with protected office documents.

Mac v1.6

- macOS Sierra v10.13.3 is now supported.
- Read-only is supported for Basic File Protection.

Mobile v1.6

- Read-only is supported for Basic File Protection.

Web Portal v1.3

- Read-only is supported for Basic File Protection.

Resolved Technical Advisories v1.6

Windows v1.6

- Excel protected Office documents can now successfully be opened, edited, and saved to a shared network location or a mapped network drive. [DDPCE-7701]
- Protected Office documents that are store on authenticated network shares now open as expected. [DDPCE-7718]
- A decrypted file now opens as expected immediately after using the recovery tool. [DDPCE-7720]

Mobile v1.6

- When using the iOS application, the issue of copying files between sync folders when the date is out-of-range for embargoed files is resolved. [DDPCE-4303]

Technical Advisories v1.6/v1.3

Windows v1.6

- With Force Protection enabled, and saving a Data Guardian protected file directly into the Unprotected Documents folder, the file will be protected. [DDPCE-7953]
- In some cases, Excel becomes unresponsive while opening a Protected Office Document when the latest office updates are not installed. The current workaround is to manually apply updates for Office. To change the default settings for updates to make them automatic, the user can navigate to Windows Update settings and select "Give me updates for other Microsoft products when I update Windows" under advanced options. Depending on the office edition that is installed, it may be possible to check for updates directly in the office app. Office standard does not have that option but Office Professional does. [DDPCE-8200]
- When Dell Data Guardian is enabled and blocking copy+paste or print-screen options, this may incorrectly trigger within a remote desktop connection session. For more information on disabling clipboard to prevent any issues with data ex-filtration through Remote

Desktop, the user can disable Clipboard within the Remote Desktop Connection based on Microsoft's documentation here:https://msdn.microsoft.com/en-us/library/aa380804(v=vs.85).aspx. [DDPCE-8250]

- In some cases, when using the recovery tool to recover large number of files pointed to a network location, the recovery tool fails to recover all the files. [DDPCE-8277]

Mac v1.6

- Currently, when linking Google drive to Data Guardian, users are required to submit user credentials more than one time. [DDPCE-7791]
- Currently, file counts are showing discrepancies between original file count and after uploading files to Data Guardian linked with OneDrive. [DDPCE-8253]
- When attempting to create a folder in finder with Dell Data Guardian for Mac installed, in certain circumstances the folder creation process may present an error and the folder will not be created. re-attempting to create the folder will resolve. [DDPCE-8273]

Mobile v1.6

- Currently, the playback feature for embedded videos is not supported on a PPTX file while using the Data Guardian application for Android or iOS. [DDPCE-8271, DDPCE-8285]

Web Portal v1.3

- Added 02/2019 - In rare occurrences, the download button may disappear when opening files in the web portal. To work around this issue, refresh the page and then close and reopen the document. [DDPCE-6047]
- When a user attempts to download a file after uploading the file with a custom cover page image to the web portal, an error message of "Download failed. An error occurred while downloading the file, please contact your system administrator" displays. The file is unable to download. To work around this issue, modify the cover-page image and re-protect the document. [DDPCE-8259]

New Features and Functionality v1.5.1/v1.2.1

Mobile Application v1.5.1

- IPv6 is now supported with Android and iOs.

Web Portal v1.2.1

- Web Portal v1.2.1 has been updated with the latest patches for the Specter Vulnerability.

Resolved Technical Advisories v1.5.1

All Clients

- No resolved technical advisories.

Technical Advisories v1.5.1/v1.2.1

All Clients

- No technical advisories.

New Features and Functionality v1.5/v1.2

Windows v1.5

- IPV6 is now supported for Windows.
- Post Sharing Encrypted PDFs is enabled using Adobe Acrobat Reader DC.
- The Print Control policy has been enabled for Office plug-in, and it displays a pop-up message when printing is blocked.
- The Data Guardian cover page is shown when a file is opened in protected view.

- Administrators can now define applications that can be blocked from running while protected office documents are opened, such as the Snipping Tool built into Windows 10.
- A durable device identifier has been created. This will be used in future releases of the Dell Servers for device identification and management.

Mac v1.5

- IPV6 is now supported for Mac.
- If protected office document encryption is on, then Data Guardian will sweep the files. If Force Protect is also on, Data Guardian sweeps the home folder of all users of the Mac. When Force Protect is off, Data Guardian ensures that a Secure Documents folder exists in the user's Documents folder, and will then sweep that folder.

Web Portal v1.2

- The Hidden Watermark Audit Trail within protected office documents and protected PDF files is now supported.
- Audit Trail can be enabled or disabled by policy.
- File name is now visible in the browser tab.
- Web portal supports opening a password-protected .pdf file.
- A pop-up notification occurs when an application process is terminated or blocked due to a protected document being open.

Resolved Technical Advisories v1.5

Windows v1.5

- An issue that allowed users to print an unprotected PDF out of a protected document using a shell extension right-click option has been resolved. [DDPCE-6389]
- Word documents now open properly after upgrading the operating system to Windows 10 Creators Update. [DDPCE-7493]
- An issue causing a long delay in sweep time when a PDF is printed from Word with Force Protected Office turned on has been resolved. [DDPCE-6806]
- An issue resulting with the in-pod audit listing the Windows login ID instead of the activated email address after an external domain user edited a PDF has been resolved. [DDPCE-6881]

Mac v1.5

- Errors no longer display when attempting to bulk upload a large number of OneDrive for Business files. [DDPCE-5244]

Mobile v1.5

- The issue of the application becoming unresponsive when a large number of PowerPoint files with images and videos are added to the sync client folder is resolved. [DDPCE-3632]
- An issue that resulted in an incorrect file path to be displayed in audit logs for a document created with the Android application on Google Drive or OneDrive for Business has been resolved. [DDPCE-4022]
- An issue that allowed users to print an unprotected PDF out of a protected document using right-click has been resolved. [DDPCE-6389]

Web Portal v1.2

- When logging in to the web portal, a failed authentication attempt followed by a successful authentication attempt now results in the user being routed to the correct destination. [DDPCE-6318]
- The web portal now supports opening a password-protected .pdf file. [DDPCE-6896]

Technical Advisories v1.5/v1.2

Windows v1.5

- Added 05/2018 - If a user double-clicks files in the virtual drive intermittently, it may result in an error. To work around this issue, copy the file to a local directory before opening. [DDPCE-7233]
- Currently, if you open a protected PDF from Dropbox, another protected PDF from Dropbox will not open. To work around this issue, copy the protected PDF file from the virtual drive to a local directory before opening another protected pdf. [DDPCE-7326]

- Added 3/2018-Currently, if you try saving an unprotected PDF with the same name as a previously deleted PDF, you will receive an error message "A device attached to the system is not functioning" when Data Guardian is active. The workaround is to choose a different file name. [DDPCE-7397]
- OneDrive's Files On-Demand feature is not supported with Data Guardian. If Files On-Demand is selected in OneDrive and Data Guardian's Cloud Encryption is enabled, the error message "Location is not available" displays upon file save. To resolve the issue, deselect Files On-Demand on the OneDrive settings tab. [DDPCE-7350]
- In Global Settings, the Custom Support Dialog policy, that provides users with IT support information, should allow a maximum of 10,000 characters, which can be four lines with a maximum of 2500 characters each. The text cannot contain line feeds, hard returns, or similar characters unless they are escaped. If an administrator enters an invalid character (non-JSON format), this may cause Data Guardian clients to stop activating. For user experience on Windows devices, a maximum of 2000 characters is recommended. [DDPCE-7393]
- Added 3/2018 - Currently, if you try saving an unprotected PDF with the same name as a previously deleted PDF, you will receive an error message "A device attached to the system is not functioning" when Data Guardian is active. The workaround is to choose a different file name. [DDPCE-7397]
- In rare circumstances, the Data Guardian injection client prevents a user from completing an uninstall by displaying a "Files in Use" message. Click Ignore for the uninstallation to proceed as expected. [DDPCE-7696]

Mac v1.5

- In Global Settings, the Custom Support Dialog policy, that provides users with IT support information, should allow a maximum of 10,000 characters, which can be four lines with a maximum of 2500 characters each. The text cannot contain line feeds, hard returns, or similar characters unless they are escaped. If an administrator enters an invalid character (non-JSON format), this may cause Data Guardian clients to stop activating. For user experience on a Mac, a maximum of 1000 characters is recommended. [DDPCE-7393]
- Added 05/2018 - Uploads of large number of files may intermittently fail when pushing to CSPS. [DDPCE-7458, DDPCE-7466]
- Added 05/2018 - Currently, when user logs off from Server and logs into system, a blank Data Guardian screen displays. To work around this issue, the user must relaunch Data Guardian. [DDPCE-7468]
- If an administrator sets the Custom Support Dialog policy and the client receives the policy, it still could take up to 120 seconds before the information displays. [DDPCE-7507]
- Added 05/2018 - When a user opens a .xen file after making changes and saving it, an error message of "This file type is unsupported, Corporate security policy" displays. To work around this issue, retry the operation. [DDPCE-7509]
- Added 05/2018 - When user logs into Google drive after disconnecting any previous google accounts on the browser, an error message of "The HTTP listener was cancelled programmatically." displays. To work around this issue, open the browser and log into drive from there. [DDPCE-7518]
- Files in the trash folder are swept for encryption if Force Protect is enabled. [DDPCE-7565]
- A corrupted file in a folder will stop a folder upload from completing and results in an error message "Fatal Upload Error". [DDPCE-7596]
- Opening and editing multiple files at the same time may result in an error message "This file type is unsupported". To workaround this issue, edit one file at a time. [DDPCE-7597]
- When Data Guardian is restarted, Google drive becomes unlinked automatically. [DDPCE-7703]
- When a password protected file is uploaded, an error message of "Fatal upload error" displays. [DDPCE-7704]

Mobile v1.5

- In Global Settings, the Custom Support Dialog policy, that provides users with IT support information, should allow a maximum of 10,000 characters, which can be four lines with a maximum of 2500 characters each. The text cannot contain line feeds, hard returns, or similar characters unless they are escaped. If an administrator enters an invalid character (non-JSON format), this may cause Data Guardian clients to stop activating. For user experience on Mobile devices, a maximum of 1000 characters is recommended. [DDPCE-7393]

Web Portal v1.2

- No technical advisories exist.

New Features and Functionality v1.4/v1.1

All Clients v1.4/v1.1

- For Windows, Mac, and Mobile, the Hidden Audit Trail policy for protected Office documents enables or disables the ability for user information to be captured in the file metadata. This supports the General Data Protection Regulation (GDPR) for privacy laws in Europe with the option to disable audit data, geolocation, and in-file audit tracking watermark. With Windows, to view data that is collected using the Hidden Audit Trail, an administrator can use the Data Guardian recovery tool to decrypt the file, which creates an Audit Trail folder with a log of each decrypted file that has hidden audit trail information.

Windows v1.4

- Protected .pdf files can be opened and edited with Adobe Acrobat Reader DC.

  NOTE: The following are not supported: Adobe Acrobat Standard DC, Adobe Acrobat Pro DC, and Adobe Acrobat DC.
- As part of the Acrobat Reader DC functionality, users can add annotations to a protected .pdf file or complete a form. When the file is saved, a new protected .pdf file is created that includes the changes.
- To enhance security, when one protected .pdf file is open with Acrobat Reader DC, Internet access is blocked until Acrobat Reader DC is closed.
- Network IO is disabled for Acrobat Reader DC, so users cannot open a protected .pdf file from the network. Users can open a protected .pdf file with Word from the network.
- The Export policy can be applied to protected .pdf files opened with Acrobat Reader DC. If the Export policy is set to Blocked or Watermark and a user selects **File > Save as Other > Text**, the Save is blocked.
- Copying from a protected .pdf is blocked.
- To enhance security, if a protected PDF is open, a user cannot email from that instance.
- Data Guardian is supported with specific versions of Microsoft Office 2016, either stand-alone or as part of Microsoft Office 365 Business or Business Premium. It is not supported with Office 365 Business Essentials.

Mac v1.4

- Users can open protected Office documents from local storage in addition to documents in the cloud. However, it will only convert unprotected Office files by copying them to the cloud.

Mobile v1.4

- If attempts to modify a protected PDF are made, a hidden watermark provides security administrators with an audit trail.

Web Portal v1.1

- Protected PDFs are now supported.
- The timeout period has been extended when uploading large files. At a specified time, the user is prompted to extend the session. The user also has the option to cancel the upload.
- Audit events are now supported as well as a policy to disable audit events and geolocation. If disabled, no audit or geolocation data is collected
- On-screen watermark with the user's registered email address is now supported. Based on policy, Data Guardian can apply an on-screen watermark to protected Office documents and PDFs. If a user prints or shares the document, the watermark persists.
- If the edit policy is enabled, .pptx and .pptm files can be edited and saved.

Resolved Technical Advisories v1.4

Windows v1.4

- Files can now be downloaded from a cloud storage provider's website as expected. [DDPCE-1511]
- Bulk uploads to Box no longer fail. [DDPCE-3308]
- Localization is now complete for Dropbox when using the Android application. [DDPCE-3643]
- An embargoed document is now automatically saved over an existing document so a user cannot cancel with the Save As option. [DDPCE-3692]
- With Dropbox, if a user copies bulk data, the progress bar now properly displays and indicates that the copy was successful. [DDPCE-3700]
- The issue of the Android application being occasionally unable to provision a sync client in Settings is resolved. [DDPCE-4045]
- When an internal user attempts to email a protected Office document to a blacklisted external user, the message now properly states that the protected file cannot be shared due to blacklisting. [DDPCE-5226]
- Copy/paste functionality now works as expected in protected Excel documents. [DDPCE-5861, DDPCE-5920]
- The issue of dragging and dropping a sheet from a protected Excel document to an unprotected Excel document is resolved. [DDPCE-6014]
- Copying and pasting an image multiple times in Excel no longer results in an error, and the image is pasted as expected. [DDPCE-6052]
- A protected Word or Excel document is no longer hidden behind open windows when opened. [DDPCE-6097]

Web Portal v1.1

- The Settings page is now localized as expected. [DDPCE-6260, DDPCE-6518]

Technical Advisories v1.4/v1.1

Windows v1.4

- Occasionally, in Excel, if a user selects **File > New > New workbook** and then selects **File > Open** to select a file from the network or in Protected view, Excel will not open. To work around this issue, close the workbook before opening from the network or in Protected View. [DDPCE-6411]
- When using Excel 2010, users can drag and drop a protected Excel document to an unprotected one. Users should be made aware that sensitive content should not be transferred in this way. [DDPCE-6426]
- Added 05/2018 - In some cases, when a user uploads files to a website in Firefox, "NoEntId" is added to the filenames and is unable to upload. To workaround this issue, use the sync client or shut down the browser and upload the file again. [DDPCE-6798]
- Currently, when accessing .pdf files from a network location in Acrobat Reader DC, the files must first be copied to a local folder. [DDPCE-6810]
- Currently, if you download a zipped folder of protected documents from the Internet, that folder may be marked as read-only, and a dialog displays that the file appears to be corrupted. To work around this issue, clear read-only from those folders, subfolders, and files and in the file's Properties, click Unblock. [DDPCE-6815]
- Currently, within Acrobat Reader DC, a user can navigate to the VDisk virtual drive and then to Dropbox. The user may get an access error when opening a protected PDF file. To work around this issue, copy the file to a local drive. [DDPCE-6820]
- Added 05/2018 - Occasionally, in Acrobat, when a user makes changes to a protected document and attempts to save over the existing file, a message of " The document could not be saved. Cannot save to this filename. Please save the document with a different name or in a different folder." displays and the file is converted to a temporary file. To work around this issue, save the file to a new file name. [DDPCE-6823]
- Added 05/2018- When a user downloads .xen files from Dropbox while using Internet Explorer, the files downloaded are not decrypted. As a work-around, downloading from Firefox and Chrome will cause files to be saved in the downloads folder and properly decrypted. [DDPCE-6832]
- Added 05/2018 - In rare circumstances, when an external user opens files edited by an internal user and saves in a virtual drive, the files fail to open. The application launches as expected. [DDPCE-6869]
- When installing Data Guardian on Windows 10 32-bit, a crash may occur due to the Intel Graphics Controller. To work around this issue, uninstall the Intel HD graphic video driver and then download the Intel HD graphic video driver from the Drivers section of the specific platform on dell.com/support. [DDPCE-6905]
- Added 05/2018 - Creating or renaming folders in sync clients using virtual drive results in an error message of "Cannot read from source file or disk". To work around this issue, folder can be created using the command line or creating folders through an online browser access. [DDPCE-6918]
- Currently, with Google Drive, protected Office documents do not decrypt when opened from a browser outside the Cloud Explorer. To work around this issue, open the files using Cloud Explorer. [DDPCE-6943]
- Added 05/2018 - In rare circumstances, when a user opens a protected file after making changes and saving it, the file becomes unprotected if user tries to make another change immediately and saves again. To work around this issue, the user needs to wait more time before reopening the protected file. [DDPCE-7082]

Mac v1.4

- With Data Guardian SDK 2.0, Dropbox cloud storage provider is not supported with Yosemite or previous operating systems.
- Added 05/2018- In rare occurrences, when user tries to upload .xen files using the Data Guardian with selected cloud service, the .xen files fail to convert to protected office documents. [DDPCE-6884]

Mobile v1.4

- Added 05/2018 - In rare circumstances, when a user logs into Data Guardian while using BOX as the cloud service provider, the login screen displays instead of the PIN screen . To work around this issue, user can tap anywhere on the login screen for the PIN screen to display. [DDPCE-6378]

Web Portal v1.1

- With Firefox, if a user edits an uploaded file after logging out of the web portal, a corrupted file may be downloaded. The viewer displays a message for the end user to log in again if making changes. The user can delete the corrupted file. [DDPCE-5702]

New Features and Functionality v1.3.1/v1.0

Mac v1.3.1

- iOS 11.x is now supported.
- The Data Guardian Dropbox SDK was upgraded to 2.0 to support the new Dropbox API.

Mobile v1.3.1

- iOS 11.x is now supported.
- For iOS and Android, the Data Guardian Dropbox SDK was upgraded to 2.0 to support the new Dropbox API.

New Features and Functionality v1.3/v1.0

All Clients v1.3/v1.0

- An administrator can revoke Data Guardian encryption keys for individual files that were shared with an external user, on either the External User Management page or the Audit Events page of the Management Console, and can now blacklist an external user from the Audit Events page.
- The Remote Wipe command to remove a Dropbox for Business user has been deprecated. Administrators may use the Dropbox for Business function to remove users.
- The Enterprise Server and Virtual Edition are rebranded to Security Management Server and Security Management Server Virtual, but when no distinction is needed are referred to as Dell Server.

Windows v1.3

- PDF files used with Office are now supported.
  - Internal and external users can select the *Save as type* option to create a protected .pdf file from an Office document.
  - Currently, a protected .pdf file can only be opened from Microsoft Word.
  - A hidden watermark provides security administrators with an audit trail, in case a user attempts to modify a protected PDF.
- Based on policy, Data Guardian can apply an watermark to protected Office documents and PDFs. If a user prints or shares the document, the watermark persists. The watermark identifies the user.
- The virtual drive has been renamed and displays as DDG VDisk in Data Guardian's Cloud Encryption.

Mac v1.3

- macOS Sierra v10.12.6 is now supported.
- PDF files used with Office are now supported.
  - Users can drag a .pdf file from the Finder to a cloud provider in Data Guardian to protect the file.
  - Mac users drag the protected .pdf file to the desktop from Data Guardian.
  - A hidden watermark provides security administrators with an audit trail if a user attempts to modify a protected PDF.

Mobile v1.3

- PDF files used with Office are now supported.
  - Internal and external users can select the *Save as type* option to create a protected .pdf file from an Office document.
  - Users can open a protected .pdf file from the native editor supported by the Data Guardian application.

Web Portal v1.0

- The web portal is now supported with Dell Servers v9.8 or later.
  - Based on policy, internal and external users can view and edit protected office documents and .xen files, with Print Control, Block Copy, and Embargo features, without installing the full Data Guardian client on their computers.
  - The administrator runs a quick installation to set up a virtual machine that hosts the web client and communicates with the Dell Server.

Resolved Technical Advisories v1.3

All Clients v1.3

- An external user no longer must reactivate Data Guardian after being removed from the Full Access List. [DDPS-5021]

Windows v1.3

- The print watermark is no longer obscured in a protected Word document when a white image is added and moved behind the text. [DDPCE-2239]
- The proper error message is now received when attempting to copy data from a protected office document to a new unprotected office document. [DDPCE-2618]
- An issue is now resolved that caused PowerPoint to become unstable when copying/cutting and pasting content into an unprotected PowerPoint file in Force-Protected mode. [DDPCE-2639]
- Excel copy/cut/paste operations made in rapid succession now work as expected. [DDPCE-3246]
- In protected Office mode, saving an existing Word file now properly converts the file to a protected Office file. [DDPCE-3448]
- The watermark now properly displays in a protected Word document when the Print Control policy is set to Watermark. [DDPCE-3617]
- The **Protected Save As** menu item is no longer disabled after setting a date restriction and saving an Excel file with Windows 10 and Office 2016. [DDPCE-4587]
- A Word error no longer displays before the protected clipboard message when attempting to paste from a protected Excel document into an unprotected Word document. [DDPCE-4811]
- An Outlook .msg file is now shared, and the share dialog displays when the user double-clicks the file and selects **Send**. [DDPCE-5076]
- The issue of adding a camera image directly into a protected Excel document was closed as not reproducible. [DDPCE-5279]
- Two instances of a protected file are no longer created when an external user creates a protected PowerPoint file. [DDPCE-5380]
- Data Guardian uninstallation is now blocked when Word, Excel, PowerPoint, or Outlook is open. [DDPCE-5382]
- Protected documents are now created as expected using Gallery templates with PowerPoint 2016 in Force-Protect mode. [DDPCE-5441]
- An issue is resolved that caused occasional failure of external user encryption key requests. [DDPCE-5559]
- The log error message that describes activation failure when the Dell Server version cannot be retrieved now directs the administrator to check the Dell Server connectivity and SSL/TLS trust settings, rather than showing activation failure due to incorrect Dell Server version. [DDPCE-5610]
- Data Guardian functionality is no longer interrupted when the computer is not connected to the Internet. [DDPCE-5614]

Mac v1.3

- An issue is resolved that resulted in an intermittent invalid file error when a protected office document was opened. [DDPCE-5053]
- Audit events are now generated for .xen files with macOS Sierra 10.12.5. [DDPCE-5224]
- An external user can now access a file that is modified by the internal user who approved the external user's file access request. [DDPCE-5508, DDPCE-5510]
- Data Guardian no longer occasionally becomes unresponsive when a file that is already encrypted is uploaded. [DDPCE-5863]
- A tamper error no longer displays after the cover page of an encrypted file is modified, and the cover page is repaired as expected. [DDPCE-5928]
- The Detected Tampering event now displays in audit events when files are tampered with. [DDPCE-5946]

Mobile v1.3

- The Iberian Portuguese interface now displays as expected in iOS 10.3. [DDPCE-5360]

Technical Advisories v1.3/v1.0

All Clients v1.3/v1.0

- Data Guardian is not supported with Google's Back Up and Sync feature. [DDPCE-6203]

Windows v1.3

- Save is not enabled in a new protected PowerPoint file until after the file is saved for the first time. To work around this issue, use **File** > **Save**. [DDPCE-5511]
- An error related with *\Users\...\Dropbox\.dropbox.cache* may occur with Dropbox for Business, with an error in the log that is similar to: *Err CBFSPortalFolder [6084] - Initialize - Folder 'C:\Users\SCTest21\Dropbox (Dell Official Team)\.dropbox.cache', Unable to find database record for folder*. To work around this issue, add the `\Users\...\Dropbox\.dropbox.cache` folder to the Excluded folders policy. [DDPCE-5573]
- The right-click menu is not available in a protected Excel or PowerPoint document. To work around this issue, use the menu at the top of the application window. [DDPCE-5822]
- Clicking Quick Print in a protected Excel document results in an error, and the document does not print although the print progress dialog displays. [DDPCE-5921]
- When the Print Control policy is changed while a protected office document is open, the updated policy is not applied to Quick Print until the document is closed and then reopened. [DDPCE-5976]
- After the cover page of a protected PDF is tampered with, the cover page, rather than the protected content, occasionally displays. [DDPCE-5984]
- Attempting to create a protected office document fails on a computer that has been suspended then is unsuspended in the Management Console. [DDPCE-6040]
- A protected PDF does not open from the right-click menu. To work around this issue, open Word then select **File** > **Open**. [DDPCE-6048]
- The on-screen watermark is not visible when the Ease of Access option, High Contrast, is enabled. [DDPCE-6084]
- Added 09/2017 - Currently, with .xlsx or .pptx files, the Recovery Tool may fail to extract audit trail author information. To work around this issue, an administrator can zip the file and use a zip viewing tool, then open CustomXml > item1.xml in a text editor, and view the authors tag. However, if a user has attempted to remove themselves or add someone to the authors list, the Recovery Tool will indicate that the file has been tampered with. [DDPCE-6160]
- The Recovery Tool does not include network paths or mapped network drives in the Browse for Folder dialog. To work around this issue, type or paste the location into the field. [DDPCE-6224]

Mac v1.3

- Added 05/2018 - Data Guardian is launched by default for unencrypted docx, pptx, pdf, etc, files. [DDPCE-6554]

Mobile v1.3

- No Technical Advisories exist.

Web Portal v1.0

- When attempting to upload an unsupported file format, the error message is dismissed by clicking OK, but the browser does not close as expected. To work around this issue, close the browser manually after clicking **OK.** [DDPCE-5797]
- Added 8/2017 - If a user clicks **Back** on the browser while uploading a file to the web portal, the user is redirected to the download page. Navigating back to the web client home page resolves this issue. [DDPCE-5922]
- Added 8/2017 - After configuring the Data Guardian virtual machine, configuration options cannot be changed. The SSL certificate, Dell Server FQDN, and other settings cannot be changed once deployed. To change these values, an administrator must deploy a new virtual machine. [DDPCE-6300]
- Added 8/2017 - Changing the Data Guardian virtual machine hostname will cause the VM to cease to function after reboot due to a mis-match of the certificate and the assigned certificate alias. [DDPCE-6315]
- Added 8/2017 - When configuring a new web portal, the same hostname cannot be used for the Data Guardian virtual machine and the Dell Server. [DDPCE-6317]
- Added 8/2017 - When downloading a large file through the web portal, encryption and download progress may not be visible to the end user. During this period, the user is unable to edit the document. [DDPCE-6319]

New Features and Functionality v1.2

All Clients v1.2

- Secure Lifecycle is rebranded to Dell Data Guardian.
-

Windows v1.2

- New audit events supported with Windows clients track when an internal user is blocked from copying protected content and when an external user requests access to a file.
- 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.
- 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.

Mac v1.2

- 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 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.

Mobile v1.2

- New Data Guardian Mobile policies provide geolocation and geofencing capabilities.
- Data Guardian Mobile is now integrated with Airwatch.
- Embargo is now available with Data Guardian Mobile.

Windows Resolved Technical Advisories v1.2

Windows v1.2

- User experience is improved with additional error-handling dialogs.
- After Data Guardian uninstallation, the user is no longer redirected to the Data Guardian virtual drive when accessing a Dropbox file from the Favorites folder. [DDPCE-2666]
- The issue of a short period of unresponsiveness after canceling an operation to add a date restriction to a file, has been closed as not reproducible. [DDPCE-3845]
- The issue of embargo dates not displaying when an embargoed Office document is saved to a network drive has been closed as not reproducible. [DDPCE-4058]
- When creating a document on the iOS application, the file path in the audit logs are now populated. [DDPCE-4239]
- The issue of occasional errors displaying when opening or saving protected files is resolved. [DDPCE-4420]
- An external user that is blacklisted and later whitelisted is no longer required to uninstall then reinstall to gain access to encryption keys. [DDPCE-4458]
- Date-protected Word files stored in a mapped drive now properly display the date protection period as expected. [DDPCE-4566]
- Google Drive sign in to link to Data Guardian no longer fails when the user is not signed in to a Google account. [DDPCE-5348]

Technical Advisories v1.2

Windows v1.2

- For Office 2010 and 2013, if a user selects **Attach File** in Outlook for a protected Office document, the user must select **Insert** not Insert as Text. As a protected document, the Office file's cover page displays a warning that the document is protected. For Office 2016, a user can select **Insert as Text**, but the file content is not protected. [DDPCE-4611]
- Dropbox Smart Sync is disabled when Data Guardian is installed. [DDPCE-4743]
- When emailing a protected file to an external user, the internal user must attach the file in an Outlook message for the encryption key to be shared. If the internal user right-clicks a file in Windows Explorer and selects **Send To > Mail recipient** or sends a protected file using a browser-based email, the encryption keys will not be shared. The internal user can still grant access, or the external user can request access. [DDPCE-4880]
- An external user cannot access a protected Office document from within a forwarded email. To work around this issue, the internal user must attach a protected Office document to a new email rather than forwarding it to the external user. [DDPCE-4936]
- A file cannot be macro-enabled after it is embargoed. To work around this issue, select **Protected Save As** and **Macro Enabled Document**, and then reset the embargo Date Restriction. [DDPCE-4946]
- Dropbox Sign in to link to Dell Data Guardian fails in non-English user interfaces. [DDPCE-5030]
- When an internal user forwards an email with an attached protected Office document or resends an email with a protected Office document that differs from the original, file sharing is not always successful. [DDPCE-5058]
- When a user right-clicks a new Office file, the **Protect** option displays even if the file has no content. [DDPCE-5065]
- Data Guardian properties do not display when a protected Office document is open. To work around this issue, close the document then right-click and select **Properties > Dell Data Guardian** to view Data Guardian properties. [DDPCE-5070]
- Log in/Log out audit events do not display in the Dell Server Remote Management Console. This data is available in the Dell Server through logs or audit data export to SIEM.

Mobile v1.2

- No Technical Advisories exist

Mac 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 Obfuscate Filenames policy is set to Guid. [DDPCE-5079]
- 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]
- 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

Windows v1.1

- 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 Management Console.
- Internal users now auto-activate after installation.

Mac 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.

Mobile v1.1

- When Office documents or macro-enabled documents are created on an Android or iOS client that is not connected to the Dell Server, encryption 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

Windows v1.1

- 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]
- As per Office native behavior, a protected macro-enabled document cannot be edited from the macros menu. [DDPCE-4418]

Mac v1.1

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

Mobile v1.1

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

Technical Advisories v1.1

Windows v1.1

- 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]
- 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]
- Added 4/2017 - A protected office document cannot be opened from a File Explorer search result when running Office 2016 on Windows 7. [DDPCE-4577]

Technical Advisories v1.0

Windows v1.0

- As expected, Dropbox remains an option in the virtual drive's Folder Management after Dropbox is uninstalled (if Folder Management is enabled). To prevent Dropbox from displaying in the virtual drive, manually remove it. [DDPCE-417]

- 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 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 disabled, 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]
- Added 4/2017 - Occasionally, due to Office Clipboard cache, protected content remains in the cache and can be copied to new unprotected office documents although Force-Protected mode is enabled. [DDPCE-2646]
- 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 credentials. 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 05/2018- For office applications, the most recent protected file saved does not show up in the recent list on the Start Screen. [DDPCE-3096]
- 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]
- 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]
- 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]
- 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**. 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]
- Added 4/2017 - When a Dropbox and OneDrive user attempts to delete all folders from the virtual drive, files are deleted but the folders remain. To work around this issue, delete the folders in the cloud storage provider's website. [DDPCE-4224]
- Added 4/2017 - Encrypted (.xen) files cannot be opened directly from a cloud storage provider folder in File Explorer. To work around this issue, open files in the Data Guardian virtual drive. Protected office documents are not affected by this issue. [DDPCE-4260]
- Amended 7/2017 - When user right-clicks a protected Word document in File Explorer and selects **Print**, Word may become unresponsive or only the cover page is watermarked even though the Print Control policy is set to *Watermark*. To work around this issue, use another print option, such as **File > Print**. [DDPCE-4261]

Mobile v1.0

- 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]

- Occasionally, the iOS application may become unresponsive when a file is synced over a slow network connection. [DDPCE-4163]

Mac 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 Dell Server, to work around this issue, click **Change Server** and enter the new Dell Server information when Secure Lifecycle is launched. [DDPCE-1121]
- Added 4/2017 - Downloading a OneDrive file that is larger than 500 MB may result in a timeout error. [DDPCE-3311]
- 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 enabled 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. Beacon events are reported successfully 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]

2

Software and Hardware Compatibility

Data Guardian 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.