

Dell Data Guardian

Windows, Mac, Mobile, and Web Administrator Guide
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.

© 2016-2019 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Azure®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

Windows, Mac, Mobile, and Web Administrator Guide

2019 - 07

Rev. A01

Contents

1 Introduction.....	5
Before You Begin.....	5
Contact Dell ProSupport.....	5
2 Requirements.....	6
Dell Server.....	6
Data Guardian for Windows.....	6
Prerequisites.....	6
Hardware.....	7
Operating Systems.....	7
Microsoft Office.....	8
Data Guardian for Mac.....	8
Operating Systems.....	8
Cloud Storage Providers.....	9
Microsoft Office.....	9
Data Guardian for Mobile Application.....	9
Microsoft Office.....	10
Data Guardian for Web.....	10
Cloud Storage Providers.....	11
Microsoft Office.....	11
Web Browsers.....	11
Other Requirements.....	11
Language Support.....	12
3 Configure and Install Data Guardian on Windows.....	13
Data Guardian Client Registry Settings.....	13
Configure an on-prem Server for Data Guardian.....	13
Configure Dell Security Management Server Virtual for Data Guardian.....	14
Configure Dell Security Management Server for Data Guardian.....	14
Disable Microsoft's Exploit Guard or EMET for Managed Applications.....	16
Manage Cloud Storage Protection Provider Profiles.....	16
Allow/Deny Users on Full Access List/Blacklist.....	17
Install Data Guardian.....	17
Pre-existing Folders with Unencrypted Files.....	17
Install Data Guardian Interactively on Windows.....	18
Install Data Guardian with Command Line.....	19
Set GPO on Domain Controller to Enable Entitlements.....	20
Uninstall Data Guardian.....	21
View Reports.....	21
Data Guardian Troubleshooting.....	21
Use the Details Screen.....	21
Use the Enhanced Details Screen.....	22
View Log Files.....	22

Troubleshoot Auto-Activation Issues.....	22
Frequently Asked Questions.....	22
4 Configure and Install Data Guardian on Mac.....	23
Server Tasks.....	23
Prerequisites.....	23
Policies.....	23
Set Up the Security Server to Allow Cloud Client Downloads (On-prem only).....	24
Allow/Deny Users on Full Access List /Blacklist.....	25
Client Tasks.....	26
Prerequisites.....	26
Best Practices.....	26
Install Client.....	26
End User Activation (on-prem).....	28
Uninstall Data Guardian.....	30
5 Configure and Install Data Guardian for the Web Client.....	31
Download the OVA file.....	31
Install Data Guardian for Web.....	31
Open the Management Console.....	33
Data Guardian Basic Terminal Configuration Tasks.....	33
Change Host Name.....	33
Change Network Settings.....	33
Change User Passwords.....	34
Enable SSH.....	34
Start or Stop Services.....	35
Reboot the Appliance.....	35
Shut down the Appliance.....	35
Administrator Tasks.....	35
Set or Change Terminal Language.....	35
Generate a System Snapshot Log.....	35

Introduction

All policy information and their descriptions are found in the AdminHelp.

Before You Begin

- 1 Before you begin, confirm the correct environment for your enterprise and complete any setup:

Hosted Dell Security Center

A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.

See the *Dell Security Center Quick Start Guide* to set up your tenant.

Access the Dell Security Center to set policies.

On-prem Dell Management Server

An on-prem Server located within the enterprise network for managing Dell Data Security software.

Install the Dell Server before deploying clients. Locate the correct guide as shown below, follow the instructions, and then return to this guide. See one of these:

- [Security Management Server Installation and Migration Guide](#)
- [Security Management Server Virtual Quick Start Guide and Installation Guide](#)

From the Dell Server, access the Management Console to set policies.

- 2 Verify that policies are set as desired. Browse through *AdminHelp*, available from the **?** at the top right of the Dell Security Center or Management Console. *AdminHelp* is page-level help designed to help you set and modify policy and understand your options.
- 3 Thoroughly read the [Requirements](#) chapter of this document.
- 4 Deploy clients to users.

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](#).

Requirements

Dell Server

Data Guardian for Windows, Mac, and Mobile requires Security Management Server or Security Management Server Virtual v9.6 or higher. The Data Guardian web client requires Security Management Server or Security Management Server Virtual v9.8 or higher. For the purposes of this document, both Servers are referred to as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Security Management Server Virtual).

Data Guardian for Windows

- IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.
- The user account performing the installation/upgrade/uninstallation must be a local or domain administrator user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or Dell KACE. A non-administrator user that has elevated privileges is not supported.
- Back up all important data before beginning installation/uninstallation.
- Do not make changes to the computer, including inserting or removing external (USB) drives during installation.
- Data Guardian is supported with specific versions of Microsoft Office 2016 and also Microsoft Office 365 Business and Business Premium. It is not supported with Office 365 Business Essentials.
- Data Guardian for Windows is compatible with Workspace ONE. The Data Guardian installer for Workspace ONE and an MSI installation has an .msi extension.
- 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 requires some configuring.
- Ensure that target devices have connectivity to <https://yoursecurityservername.domain.com:8443/cloudweb/register> and <https://yoursecurityservername.domain.com:8443/cloudweb>.
- Before deploying Data Guardian, it is best if the target devices do not yet have cloud storage accounts set up. If users decide to keep their existing accounts, they should ensure that any files that are to remain *unencrypted* are moved out of the sync client before installing Data Guardian.
- Users should be prepared to restart their computer after the client is installed.
- Data Guardian does not interfere with the behavior of sync clients. Therefore, administrators and users should familiarize themselves with how these applications operate prior to deploying Data Guardian. For more information, see Box support at <https://support.box.com/home>, Dropbox support at <https://www.dropbox.com/help>, or OneDrive support at <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.
- Protected Office documents are supported with Mozy, a companion solution to Data Guardian, as well as other cloud, email, and NFS storage products.
- Although Dell Encryption is not required, if used, the Encryption client should be v8.12 or later.
- Data Guardian does not support the Windows System Restore tool or Windows Insider Preview.
- Microsoft's Folder Redirection is not supported with Data Guardian.
- Be sure to periodically check dell.com/support for the most current documentation and Technical Advisories.

Prerequisites

.exe prerequisites

If not already installed, the installer installs Microsoft Visual C++ 2017 Redistributable Package (x86 and x64).

NOTE:

For Windows 7 and Windows 8.1, the computers should be up-to-date with Windows Updates. For more information, see <https://support.microsoft.com/en-us/help/2919355> and <https://support.microsoft.com/en-us/help/2999226>.

.msi prerequisites

You must install Microsoft Visual Studio C++ 2017 Redistributable Package (x86 and x64).

NOTE:

In addition, if running MSI, you must also install Visual Studio 2010 Tools for Office Runtime (x86 and x64).

General prerequisite

Microsoft .Net 4.5.2 (or later) is required for Data Guardian. All computers shipped from the Dell factory are pre-installed with .Net 4.5.2. However, if you are not installing on Dell hardware or are upgrading Data Guardian on older Dell hardware, you should verify which version of .Net is installed and update the version, if needed, prior to installing Data Guardian to prevent installation/upgrade failures. To verify the version of .Net installed, follow these instructions on the computer targeted for installation: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). To install Microsoft .Net Framework 4.5.2, go to <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

Hardware

Minimum hardware requirements must meet the minimum specifications of the operating system. The following table details supported hardware for the Windows client.

Windows Hardware

- 200 MB free disk space, depending on operating system
- 10/100/1000 or Wi-Fi network interface card
- TCP/IP installed and activated

Operating Systems

The following table details supported operating systems.

Windows Operating Systems (32-bit and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1703 (Creators Update/Redstone 2) through Version 1903 (May 2019 Update/19H1)

NOTE:

The client must be on one of these operating systems, or it will be blocked. If needed, a setting in a registry key allows the administrator to override the block.

For Redstone 4 support, you must upgrade the agent before upgrading the operating system. See <https://www.dell.com/support/article/us/en/04/sln307922>.

NOTE:

Data Guardian is not compatible with Microsoft's Windows Defender Exploit Guard (WDEG) in Redstone 3 and higher or with Enhanced Mitigation Experience Toolkit (EMET) in Redstone 2 and lower.

Windows 7 is not supported with the geolocation policy for Data Guardian audit events.

Data Guardian does not support multiple versions of Office on one computer.

Microsoft Office

Data Guardian supports the following versions of Office. However, you must have just one version of Office installed.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: versions 1705, 1708, and 1803 (Semi-Annual Channel)

Data Guardian for Mac

The following lists supported hardware for the Mac client.

Mac Hardware

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

Operating Systems

The following lists supported operating systems.

Mac Operating Systems

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.6

Cloud Storage Providers

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

Cloud Storage Providers

- Dropbox

- Box

- Google Drive

**NOTE:**

Google Backup and Sync is not supported.

- OneDrive

- OneDrive for Business

Microsoft Office

Data Guardian for Mac supports the following versions of Office.

Microsoft Office

- Office 2013 SP1

- Office 2016

- Office 2019

Data Guardian for Mobile Application

The following lists operating systems supported with Data Guardian for Mobile.

Android Operating Systems

- 5.0—5.1.1 Lollipop

- 6.0—6.0.1 Marshmallow

- 7.0—7.1.2 Nougat

- 8.0—8.1 Oreo

- 9.0 Pie

iOS Operating Systems

- iOS 10.x—10.3.3
- iOS 11.x—11.4.1
- iOS 12.x—12.3

Chromebook Operating System

Chrome OS version M53 or higher is required to run Android applications on Chrome OS. These devices are validated to run Android apps on Chrome OS, but confirm your option with your sales representative:

- <https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps>

Microsoft Office

Data Guardian for Mobile Application can open files created with the following versions of Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Data Guardian for Web

To enable the Data Guardian web client, the administrator sets up a virtual machine that hosts the web client and communicates with the Dell Server v9.8 or later.

The following virtualized environments can be used to deploy the Data Guardian web client.

Virtualized Environments

- **VMware ESXi 6.7**
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended
 - An Operating System is not required
 - See <http://www.vmware.com/resources/compatibility/search.php> for a complete list of supported Host Operating Systems
 - Hardware must conform to minimum VMware requirements
 - 4 GB minimum RAM for dedicated image resource
 - See <http://pubs.vmware.com/vsphere-67/index.jsp> for more information
- **VMware ESXi 5.5**
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended

Virtualized Environments

- An Operating System is not required
 - See <http://www.vmware.com/resources/compatibility/search.php> for a complete list of supported Host Operating Systems
 - Hardware must conform to minimum VMware requirements
 - 4 GB minimum RAM for dedicated image resource
 - See <http://pubs.vmware.com/vsphere-55/index.jsp> for more information
- **Microsoft Hyper-V**
 - 64-bit Processor with Second Level Address Translation (SLAT)
 - 8 GB RAM minimum recommended
 - Hardware must conform to minimum Hyper-V requirements
 - See <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements> for more information.

NOTE:

These minimums represent twenty-five or fewer simultaneous connections to a single web portal.

Cloud Storage Providers

Based on policy settings, Data Guardian's web portal can access these cloud storage providers.

Cloud Storage Providers

- OneDrive for Business

Microsoft Office

Data Guardian for Web can open files created with the following versions of Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Web Browsers

You can use Data Guardian with Internet Explorer, Mozilla Firefox, Google Chrome, and Microsoft Edge.

For Mac, Safari is also supported.

Other Requirements

Currently, Amazon Cognito's multi-factor authentication (MFA) is not supported with any Data Guardian platform.

Language Support

These clients are Multilingual User Interface (MUI) compliant and support the following languages.

Language Support

- EN - English
- ES - Spanish
- FR - French
- IT - Italian
- DE - German
- JA - Japanese
- KO - Korean
- PT-BR - Portuguese, Brazilian
- PT-PT - Portuguese, Portugal (Iberian)

Configure and Install Data Guardian on Windows

Data Guardian Client Registry Settings

This section details all Dell ProSupport approved registry settings for local client computers, regardless of the reason for the registry setting. If a registry setting overlaps two products, it is listed in each category.

These registry changes should be done by administrators only and may not be appropriate or function in all scenarios.

- Logging levels can be increased to aid in troubleshooting. Create or modify the following registry setting.

[HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

"LogVerbosity"=dword:0x1f (31)

By default, the logging level is set to 0xf (15).

Available values:

Off=0x0 (0)

Critical=0x1 (1)

Error=0x3 (3)

Warning=0x7 (7)

Information=0xf (15)

Debug=0x1f (31)

- After installation of Data Guardian, internal users are automatically activated. If necessary, you can modify a registry setting to override auto-activation.

[HKLM\SOFTWARE\Dell\Data Guardian]

DWORD Value: DisableAutomaticActivation=1

NOTE:

You can also confirm the aliases for your domain on the Dell Server. See [Troubleshoot Auto-Activation Issues](#).

Configure an on-prem Server for Data Guardian

Based on policies set by an administrator, Data Guardian protects data, for example:

- Office documents stored locally, shared with other users in various ways, or stored on removable media. These Office documents can be protected: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- See *AdminHelp* to determine additional policies to set.

Inform users which your Data Guardian options your enterprise uses.

Configure Dell Security Management Server Virtual for Data Guardian

To configure the Dell Security Management Server Virtual to support Data Guardian, in the Management Console, configure the Data Guardian policies:

- *Protected Office Documents* - Enterprise level only - You must set this policy to **On** in order to use other Data Guardian policies.
- See *AdminHelp* to determine additional policies to set.

Configure Dell Security Management Server for Data Guardian

To configure Dell Security Management Server to support Data Guardian, in the Management Console, configure the Data Guardian policies:

- *Protected Office Documents* - Enterprise level only - You must set this policy to **On** in order to use other Data Guardian policies.
- See *AdminHelp* to determine additional policies to set.

Then [Configure the Security Management Server to Allow Data Guardian Downloads](#).

Configure Security Management Server to Allow Data Guardian Downloads

This section details the steps needed to allow users to download Data Guardian for Windows client from your Security Management Server.

- 1 On the Security Management Server, navigate to `<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources` and open `messages.properties` with a text editor.
- 2 Ensure that the entries are as follows:
`download.deviceWin.mode=remote`

`download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe`

`download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe`
- 3 Edit the entries to the following
`download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe`

`download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe`
- 4 Save and close the file.
- 5 Go to `<Security Server install dir>` and create a new folder under it named Download (Security Server\Download).
- 6 Within the Download folder, create another new folder and name it cloudweb (Security Server\Download\cloudweb).
- 7 Add the 64-bit and the 32-bit setup files for Data Guardian to the cloudweb folder and, optionally, rename them, for example, to `DataGuardian64.exe` and `DataGuardian32.exe`, respectively.
These are user-defined but must match the file names in the versions.xml file.
- 8 Restart the Security Server for the changes to take effect.

Configure the Security Management Server for Automatic Download of the Windows Data Guardian Client (Optional)

For automatic downloads, the versions.xml file and binaries must be in the same location. The location must be accessible by the client, so it could be IIS or you could use the **Security Server\Download\cloudweb** folder you created. If using the cloudweb folder, follow this sample configuration.

- 1 Navigate to the **Security Server\Download\cloudweb** folder. (See [step 6](#) in [Configure the Security Server to Allow Data Guardian Client Downloads.](#))
- 2 Create a folder under it named DataGuardianUpdate.

NOTE:

DataGuardianUpdate is used in this example, but you can choose any name.

- 3 Place the updated executables in the DataGuardianUpdate folder.
- 4 Create a *versions.xml* file in the DataGuardianUpdate folder.
- 5 Open *versions.xml* with a text editor and verify the file name path is correct for your environment.

Sample:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version: File version of the updated executables

setup.exe file name: The setup name of the executables is user-defined but must match the setup name in the messages.properties file. (See [step 3](#) in [Configure the Security Server to Allow Data Guardian Client Downloads.](#))

- 6 Save and close the file.
- 7 Add the binaries to this folder.
- 8 If using IIS, restart IIS.
- 9 As a Dell administrator, log in to the Management Console.
- 10 In the left pane, click **Populations > Enterprise**, and the Security Policies tab displays.
- 11 In the Data Guardian technology group, click **Cloud Encryption > Show advanced settings**.
- 12 Scroll to the *Software Update Server URL* policy and enter **https://<YOUR HOST URL > /DataGuardianUpdate**.

NOTE:

DataGuardianUpdate is only an example to match the example above.

- 13 Click **Save** to store the policy modification in the queue to commit.
- 14 Click **Management > Commit**.
- 15 Enter a comment and click **Commit Policies**.

Re-image a Computer with Data Guardian Installed

If a computer needs to be re-imaged and has Data Guardian installed, ask the user if they have worked offline and created any protected Office documents while offline. If so, offline keys were generated for those documents and those keys have not been escrowed to the Dell Server.

- 1 For information on recovering Data Guardian offline-generated keys that were not escrowed to the Dell Server, see the *Recovery Guide*.
- 2 Check for an offline keys folder before a re-image of the computer.

When the first escrow keys are created, a Data Guardian folder is added to C:\Program Files\Dell. Navigate to the Data Guardian > OfflineKeys folder. If no OfflineKeys folder exists, check the user's My Documents folder.

Disable Microsoft's Exploit Guard or EMET for Managed Applications

In Windows 10, the following may be enabled or built into the operating system:

- Redstone 3 and higher - Windows Defender Exploit Guard (WDEG)
- Redstone 2 and lower - Enhanced Mitigation Experience Toolkit (EMET)

If these features are enabled or built into the operating system, you must configure the settings to disable these managed applications:

- winword.exe
- powerpnt.exe
- excel.exe
- acord32.exe

If you do not disable these, you may see the DLP as an exploit.

Windows Defender Exploit Guard (WDEG)

To disable the managed applications:

- 1 On the target computer, *search* for and open *Windows Defender Security Center*.
- 2 Click **App & browser control**.
- 3 Scroll to the bottom of the screen and click **Exploit protection settings**.
- 4 Select **Program settings**.
- 5 Click **+** to add each managed application listed above.
- 6 In the Properties for each managed application, select the *Override* check box for any option that is set to *On* and then toggle the option to **Off**.



NOTE:

If a managed application is open and a dialog states you must restart the .exe, restart it after completing these steps.

- 7 Click **Apply**.
 - 8 Click **Yes**.
- In Program settings, the managed application lists the overrides based on the options you changed.

Enhanced Mitigation Experience Toolkit (EMET)

To disable the managed applications:

- 1 Navigate to *Application Configuration*.
- 2 In the *ROP Caller Check* and *Export Address Table Address Filter (EAF)* options, clear the check boxes for the managed applications listed above.

Manage Cloud Storage Protection Provider Profiles

Data Guardian encrypts users' files and sends audit events to the Dell Server. To change the behavior for each supported cloud storage provider, set each provider to one of these values:

Value	Description
Protect	Allow the provider/connection, encrypt the files, and send audit events about file/folder activity.
Block	Block all access to the provider/connection.
Allow	Allow the provider/connection to pass through without encrypting, but audit file/folder activity.
Bypass	Bypass the protection of the provider/connection without encrypting or auditing. When this value is set, the cloud storage provider folder does not display in the Data Guardian virtual drive on the client computer.

For more information, see the *AdminHelp*, which is accessible from the Management Console.

Allow/Deny Users on Full Access List/Blacklist

You can determine which external users can register with the Dell Server or Hosted Dell Security Center to use Data Guardian. For adequate security, be sure to carefully set up and manage these lists.

- An internal user is within the domain.
- An external user is a non-domain user, either a person from another organization with whom an internal user wants to share business-sensitive documents or an internal user who wants to access their computer from a non-domain device.

To allow a user who is not in the organization's domain to register to use Data Guardian:

- 1 In the left pane of the Management Console or Dell Security Center, click **Management > External User Management**.
- 2 Click **Add**.
- 3 Select Registration Access Type:

Blacklist - Blocks registration for a user or a domain. User cannot open a protected Office document or protected file.

Full Access List - Grants registration and all file access for a user or domain. If a user or domain is also on the blacklist, no access is granted.

- 4 In the Enter Domain/Email field, enter either the user's domain to set access for the entire domain, or email address to set access only for that user.



NOTE:

For external mobile users in a hosted environment, the email must be in lowercase.

- 5 Click **Add**.

For more information on using full access list/blacklist, see *AdminHelp*, which is accessible from the Management Console or Dell Security Center.

Install Data Guardian

There are two methods to install Data Guardian:

- [Install Data Guardian Interactively](#)
- [Install Data Guardian with Command Line](#)

Pre-existing Folders with Unencrypted Files

When deploying Data Guardian, it is best if the target devices do not yet have a cloud storage provider account set up.

If a cloud storage provider account is set up with folders that are synced to the local computer before Data Guardian installation:

- Pre-existing files and folders that sync up to the cloud remain in cleartext
- Files you add to those pre-existing folders remain in cleartext
- Files that sync down from the cloud are encrypted

Install Data Guardian Interactively on Windows

You must be a local administrator to install Data Guardian. If users will install the product, inform them of the location of the installation media.

Before you begin

Depending on the environment and Data Guardian product, determine which of these you need:

Hosted Dell Security Center

If your hosted environment is multi-tenant, you will need an Installation ID.

On-prem Dell Management Server

Be sure you know the name of the Dell Server.

Install Data Guardian

Be prepared to restart the computer after Data Guardian is installed.

- 1 To download the Data Guardian installer, go to the location specified by your administrator.
- 2 Based on your operating system, select either the 32-bit or 64-bit installer, and copy it to the local computer. Here are sample installer names:
 - Hosted Dell Security Center - installer names have an .exe extension
 - on-prem - installer names have:
 - .exe extension
 - .msi extension for Workspace ONE and an MSI installation
- 3 Double-click the file to launch the installer.
- 4 If you get a Security Warning, click **Run**.
- 5 Select a language and click **OK**.
- 6 If prompted to install Microsoft Visual C++ 2015 Redistributable Package or Microsoft .NET Framework 4.5.2 Client Profile, click **OK**.
- 7 At the Welcome screen, click **Next**.
- 8 Read the license agreement, accept the terms, and click **Next**.
- 9 At the Destination Folder screen, click **Next** to install in the default location of `C:\Program Files\Dell\Data Guardian\`. Do not install Data Guardian in the `C:\Users` or `C:\Windows` folders or at the root of any drive.
- 10 Select one of these:

Hosted Dell Security Center

A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.

- a Select **Hosted Dell Security Center**.
- b Optionally, if your enterprise is multi-tenant, enter an Installation ID.

On-prem Dell Management Server

An on-prem Server located within the enterprise network for managing Dell Data Security software.

- a Select **On-prem Dell Management Server**.
- b In the *Dell Management Server Name*: field, enter the Dell Server Name that this computer will communicate with, such as `server.domain.com`. You do not need to include `www` or `http(s)`. This information is supplied by your administrator.

NOTE:

If your enterprise is multi-tenant and you do not enter an Installation ID, you can enter it when you activate or the administrator can add it to the Registry later.


- c Click **Continue**.
- d Continue with [step 11](#).

NOTE:

Do not clear the *Enable SSL Trust Verification* check box unless your administrator instructs you to do so.

- c Click **Next**.
- d In the Confirm Dell Management Server Information screen, confirm that the Dell Server URL address is correct. The installer adds www or http(s) and the port. Click **Next**.
- e Continue with [step 11](#).

- 11 Click **Install** to begin the installation.
A status window displays the installation progress.
- 12 Click **Finish** when the Installation Complete screen displays.
- 13 Click **Yes** to restart.
Installation of Data Guardian is complete.

- 14 Users must confirm activation. The Data Guardian notification area icon should have a green check mark .

NOTE:

Depending on the way Data Guardian is deployed within the enterprise, activation may not be immediate. However, if activation does not occur, the user must manually activate.

Install Data Guardian with Command Line

- Command line switches and parameters are case-sensitive.
- Be sure to enclose a value that contains one or more special characters, such as a blank space in the command line, in escaped quotation marks.
- The following table details the switches available for the installation.

Switch (.exe only)	Meaning
/V	Pass variables to the .msi inside the setup.exe. The content must always be enclosed in plain-text quotes.
/S	Silent mode

Option	Meaning
/QB	Progress dialog with Cancel button, prompts for restart
/QB!	Progress dialog without Cancel button, prompts for restart
/QN	No user interface

- The following table details the parameters available for the installation. Choose the correct option for your environment.

Parameters for Hosted Dell Security Center	Parameters for Dell Server (On-prem) - .exe or .msi (for Workspace ONE)
SAAS=1	SERVER=<ServerName> (FQDN of the Dell Server for activation)
INSTALL_ID=<Installation ID for that tenant> (For a multi-tenant environment.)	ENTERPRISE=1 (Internal User)

Parameters for Hosted Dell Security Center

ENABLESSLTRUST=0 (Disable SSL trust validation)

REBOOT=SUPPRESS (Null allows for automatic reboots, SUPPRESS disables reboot)

Parameters for Dell Server (On-prem) - .exe or .msi (for Workspace ONE)

ENABLESSLTRUST=0 (Disable SSL trust validation)

REBOOT=SUPPRESS (Null allows for automatic reboots, SUPPRESS disables reboot)

Example Command Line for on-prem

- The following example installs Data Guardian silently, for an internal user, with no SSL trust validation, logs stored to C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library\Logs\install.log" ENABLESSLTRUST=0"
```

Example Command Line for Hosted Dell Security Center

- The following example installs Data Guardian silently, in a SaaS environment, for an internal user, with no SSL trust validation, logs stored to C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS SAAS=1 /L*V "c:\Library\Logs\install.log" ENABLESSLTRUST=0"
```

Example Command Line for .msi

- The following example installs Data Guardian in an .msi environment, for an internal user, with no SSL trust validation, logs stored to C:\Library\Logs\Install.log.

```
"Dell Data Guardian.msi" /QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library\Logs\install.log" ENABLESSLTRUST=0
```

User must reboot after a Location change

After Data Guardian has been installed, if you use Microsoft's *Folder Redirection*, *Group Policy*, *Windows Registry*, or other option to modify the location of a local folder or library that Data Guardian would sweep, client-side caching occurs. For example, a user might modify the Documents folder's *Properties* > *Location* to a network drive. Therefore, after a Location change, the user must reboot before logging in to Data Guardian. The following may be impacted:

- Opt-in mode** - If you or a user modify the location of the *Documents* or *Secure Documents* folder, the user must reboot or manually protect a file through right-click or *Save As*.
- Force-protected mode** - If you or a user modify the location of the *Documents* or *Unprotected* folder, the user must reboot or manually protect a file through *Save As Protected*.

Set GPO on Domain Controller to Enable Entitlements

- If your clients will be entitled from Dell Digital Delivery, follow these instructions to set the GPO on the domain controller to enable entitlements (this may not be the same server running the Dell Server).
- The workstation must be a member of the OU where the GPO is applied.
- Ensure that outbound port 443 is available to communicate with the Dell Server. If port 443 is blocked (for any reason), the entitlement feature does not function.

- On the Domain Controller to manage the clients, click **Start > Administrative Tools > Group Policy Management**.
- Right-click the OU where the policy should be applied and select **Create a GPO in this domain**, and **Link it here**.
- Enter a name for the new GPO, select (none) for Source Starter GPO, and click **OK**.
- Right-click the GPO that was created and select **Edit**.
- The Group Policy Management Editor loads. Access **Computer Configuration > Preferences > Windows Settings > Registry**.
- Right-click the Registry and select **New > Registry Item**. Complete the following.

Action: Create

Hive: HKEY_LOCAL_MACHINE

Key Path: SOFTWARE\Dell\Dell Data Protection

Value name: Server

Value type: REG_SZ

Value data: <IP address of the Dell Server>

- 7 Click **OK**.
- 8 Log out and then back into the workstation, or run **gpupdate /force** to apply the group policy.

Uninstall Data Guardian

- If a user has a local administrator account, they can uninstall Data Guardian. See the *Data Guardian User Guide* for information. This section describes the administrator process for uninstalling Data Guardian.

IMPORTANT:

When Data Guardian is uninstalled from a users' computer, their folders and files in the cloud are encrypted and unreadable. If this user leaves the company and no other user shares that folder or file, the data is unreadable, but secure (to view the files, re-install Data Guardian).

Protected Office documents remain encrypted if you uninstall Data Guardian. To decrypt, see the *Recovery Guide > Data Guardian Recovery*.

Command Line Uninstallation

- Once extracted from the master installer, the Data Guardian client installer can be located at **C:\Dell\DataGuardian_XXbit_setup.exe**.
- The following example silently uninstalls the Data Guardian client.

```
setup.exe /x /s /v" /qn"
```

Reboot the computer when prompted.

View Reports

Information about your Data Guardian environment is available in the Dell Security Center or Management Console. Select **Reporting > Audit Events** for audit events related to cloud sync client folders and protected Office documents.

For compliance and monitoring purposes of device detail, Shield detail, or audit events, see **Reporting > Manage Reports**.

For more information, see *AdminHelp*, which is accessible through the Dell Security Center or Management Console.

Data Guardian Troubleshooting

Use the Details Screen

You can use the *Details* screen for troubleshooting or support issues. For example:

- If a user creates a folder but it's not encrypting, select **Details > Files > Folder State** to check the state.
- If a user requests support, you can instruct them to set up the Enhanced Details screen and select the **Details > Policy** tab. This tab lists which policies are being enforced.
- View logs for troubleshooting.

Use the Enhanced Details Screen

- While pressing **<Ctrl><Shift>**, click the Data Guardian notification area icon, and then select **Details**.
- In addition to Files and Folders, the following display:

Security: Lists the key, key type, and state. This pane temporarily lists some protected Office files until they are sent to the Dell Server - the length of time depends on the polling interval.

Audit: Lists modules, user ID, and event type. Information is in queue in this audit log and then sent to the Dell Server at specified intervals. The administrator can view **Audit Events** from the left pane of the Dell Security Center or Management Console for auditing.

Policy: Lists the policy names and values.

View Log Files

- Click **View Log** from the bottom-left corner of the Details screen.

Log files can be also be found at **C:\ProgramData\Dell\Data Guardian**.

Protected Office document logs files are located in the Custom.xml folder.

Troubleshoot Auto-Activation Issues

If Data Guardian does not auto-activate for several users, you can change the [Data Guardian Client Registry Settings](#). You should also check the aliases on the Dell Server:

- 1 In the Dell Security Center or Management Console, navigate to **Populations > Domains** and select a domain and any sub-domains.
- 2 On the Domain Detail page, select the **Settings** tab.
- 3 In the *Alias* field, confirm that all aliases are correct.

Frequently Asked Questions

Question

Answer

Solution

Configure and Install Data Guardian on Mac

Data Guardian for Mac is designed for sharing files within cloud encryption providers. However, if Protected Office Documents policies are enabled for Macs, all file auditing and traceability is lost if the file is saved by the user to the local Mac. If strict file auditing and traceability is needed in your organization, set the *Allow Mac Data Guardian Activation* policy to **Not Selected** to prevent Data Guardian from activating on Macs.

Server Tasks

Prerequisites

Before performing these tasks, confirm the correct environment for your enterprise and complete any setup:

Hosted Dell Security Center

A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.

See the *Dell Security Center Quick Start Guide* to set up your tenant.

Assign an appropriate Dell administrator role from the Administrators page in the Dell Security Center.

On-prem Dell Management Server

An on-prem Server located within the enterprise network for managing Dell Data Security software.

Install the Dell Server and its components. See one of these:

- *Security Management Server Installation and Migration Guide*
- *Security Management Server Virtual Quick Start Guide and Installation Guide*

NOTE:

For the purposes of this document, Security Management Server/Security Management Server Virtual are both cited as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Security Management Server Virtual).

Assign an appropriate Dell administrator role from the Administrators page in the Management Console.

Policies

For information about policies, see the *AdminHelp*, which is accessible from the Dell Security Center or Management Console.

By default, Data Guardian encrypts users' files and sends audit events to the Dell Security Center or Dell Server.

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

To change default behavior for each supported cloud storage provider, set the *Cloud Storage Protection Providers* policy. If your enterprise prefers a specific cloud storage provider, set this policy to **Block** for other providers.

NOTE:

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

Set Up the Security Server to Allow Cloud Client Downloads (On-prem only)

Before performing these tasks, confirm the following:

- Install the Dell Server and its components. See one of these:
 - *Security Management Server Installation and Migration Guide*
 - *Security Management Server Virtual Quick Start Guide and Installation Guide*
- Assign an appropriate Dell administrator role from the Administrators page in the Management Console.

Security Management Server

- 1 On the Security Management Server, go to <Security Server install dir>\webapps\cloudweb\brand\dell\resources\
- 2 Open the **messages.properties** file with a text editor.
- 3 Ensure that the entries are as follows.

For **local** installation:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

For **remote** installation:

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

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

- 4 Save and close the files.
- 5 Go to <Security Server install dir> and create a folder named Download (Security Server\Download).
- 6 Within the Download folder, create a CloudWeb folder (Security Server\Download\CloudWeb).
- 7 Add the Dell Data Guardian installers to that folder.

Security Management Server Virtual: Manually Install a Different Cloud Client Version

No action is needed to allow users to download the latest Dell Data Guardian installer. The latest installer is preinstalled on the Security Server of Security Management Server Virtual.

To manually install a different Data Guardian installer version on the Security Server of Security Management Server Virtual, update the message.properties file.

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

For **local** installation:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

For **remote** installation:

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

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

- 3 Save and close the files.

- 4 Copy the files to /opt/dell/server/security-server/download/cloudweb.
- 5 Add the Data Guardian installers to that folder.

Allow/Deny Users on Full Access List /Blacklist

The full access list and blacklist entries determine which users can register with the Dell Server to use Data Guardian.

Full Access List

The full access list allows specific users or groups of users to register with the Dell Server and to use Data Guardian.

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

User Type	Enter
All organization.com email addresses	organization.com
A specific user	jdoe@organization.com
All Gmail users	gmail.com

Blacklist

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

NOTE:

If a user is already registered, this list does **not** prevent them from using Data Guardian.

You can use the blacklist to exclude specific users who are members of approved groups on the full access list. Additionally, you can place entire domains on the blacklist, which prevents anyone with an email address in that domain from registering. See the following examples to prevent a user or group from registering with the Dell Server:

User Type	Enter
All organization.com email addresses	organization.com
A specific user and that email address	jdoe@organization.com
All Gmail users	gmail.com

To modify the full access list /blacklist, follow these instructions:

- 1 In the left pane of the Dell Security Center or Management Console, click **Management > External User Management**.
- 2 Click **Add**.
- 3 Select Registration Access Type:

Blacklist - Blocks registration for a user or a domain. User cannot open a protected Office document or .xen file.

Full Access List - Grants registration and all file access for a user or domain. If a user or domain is also on the blacklist, no access is granted.

- 4 In the Enter Domain/Email field, enter either the user's domain to set access for the entire domain, or email address to set access only for that user.

5 Click **Add**.

For more information on using full access list/blacklist, see *AdminHelp*, which is accessible from the Dell Security Center or Dell Server Management Console.

An external user can request access from an internal user for the key to a protected file. If the internal user is not available, an administrator can approve or deny access.

- 1 Select **Management > Key Request Management**.
- 2 For more information, select **?** (Help).

Client Tasks

Prerequisites

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

Best Practices

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

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

Install Client

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

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

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

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

Upgrade From Previous Versions of Cloud Edition

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

NOTE:

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

Install Options

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

- [Interactive Installation](#) - This is the easiest method to install Data Guardian for Mac. However, use this method only if you plan to install the client on one computer at a time.
- or
- [Command Line Installation](#) - For this advanced installation method, administrators must be experienced with command line syntax. This method can be used for a scripted installation, using batch files, or any other push technology available to your organization.
 - During a sweep after installation, if a dialog states that you have a failure related to a valid certificate, see [Troubleshooting](#).

Interactive Installation

- 1 For Data Guardian Client, locate the Installer in **Dell-Data-Guardian-Mac-0.x.x.xxx.dmg**.
- 2 Use the **.pkg** file inside Dell-Data-Guardian-0.x.x.xxx.dmg to install or upgrade. You can use a scripted installation, batch files, or any other push technology available to your organization.
- 3 Double-click the **Dell-Data-Guardian-x.x.x** package.
- 4 Click **Continue**.
- 5 On the Introduction window, click **Continue**.
- 6 On the Software License Agreement window, click **Continue**.
- 7 Click **Agree** to continue.
- 8 On the Configuration Type window, select one of these:

Hosted Dell Security Center

A hosted Software as a Service (SaaS) solution for managing Dell Data Security software.

- a Select **Hosted Dell Security Center**.
- b Click **Continue**.
- c Continue with [step 9](#).

On-prem Dell Management Server

An on-prem Server located within the enterprise network for managing Dell Data Security software.

- a Select **On-prem Dell Management Server**.
- b In the *Dell Management Server Name*: field, enter the Dell Server Name that this computer will communicate with, such as server.domain.com. You do not need to include www or http(s). This information is supplied by your administrator.
- c Click **Continue**.
- d Continue with [step 9](#).

- 9 On the Installation Type window, do one of these:
 - Click **Install**, then go to step 10.
 - Click **Change Install Location**.
 - 1 On the Destination Select window, select all users. Currently, this is the only option.
 - 2 Click **Continue**.
 - 3 Click **Install**, then go to step 10.
- 10 In the dialog, enter your user name and password and click **Install Software**.
- 11 On the Summary window, click **Close**.
- 12 When prompted, either keep the .pkg file or move it to *Trash*.
- 13 Do one of these:

Hosted Dell Security Center

The Credentials window automatically opens after you install. If your enterprise is multi-tenant, you will need an Installation ID.

- 1 In the Credentials window, enter your login account email and click **Continue**.
- 2 Do one of these:
 - If your enterprise is multi-tenant, enter an Installation ID, click **Continue**, and continue with [step 3](#).

On-prem Dell Management Server

- 1 Close the .dmg window to open Finder.
- 2 See [End User Activation](#).

NOTE:

If an error displays, check your credentials. If you notice an incorrect email address or Installation ID, click **Restart Initialization** to re-enter your Credentials.

- For single tenants, continue with [step 3](#).
- 3 At the Microsoft window, enter your password and click **Sign in**.
 - 4 In the Azure window, enter your password.

NOTE:

If an error displays, check your credentials. If you notice an incorrect email address or Installation ID, click **Restart Initialization** to re-enter your Credentials.

- 5 The Dell Data Guardian interface opens. See [Dell Data Guardian application](#).

NOTE:

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

Command Line Installation

- 1 Mount the .dmg.
- 2 Perform a command line installation of the package using the installer command:


```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```
- 3 Instruct users to activate Data Guardian. See [End User Activation](#).

Troubleshooting

During a sweep after installation, if a dialog states that a user has a failure related to self-signed certificate:

- 1 Log in to the **Management Console**.
- 2 If a dialog states that the website has a certificate that is not valid, click **visit this website**.
- 3 At the confirmation, click **Visit Website**.
- 4 Enter the user name and password of the currently logged-in user of that computer, and click **Update Settings**. This adds the certificate to the *Keychains > login* list.
- 5 On the Mac, navigate to **Finder > Applications > Utilities**, and launch the **Keychain Access** application.
- 6 On the left in *Keychains*, select **login** and copy the certificate.
- 7 Paste the certificate to **Keychains > System**.
- 8 When prompted for credentials, enter your administrator user name and password.

End User Activation (on-prem)

Activation for On-prem Dell Management Server

With on-prem, after you open Dell Data Guardian for the first time, you must log in to activate:

- 1 In Finder, select **Applications**, and double-click **Dell Data Guardian**.
- 2 When the Credentials window opens, enter the Dell Server address, for example, company.server.com). This information is supplied by your administrator. By default, the port number is 8443. If your enterprise modifies the default port to a custom port number, your administrator will inform you.



NOTE:

Do not select the SSL Errors check box unless your administrator instructs you to do so.

- 3 Enter your email address and password.
- 4 Click **Login** to activate Data Guardian.
- 5 See *Dell Data Guardian application* below.

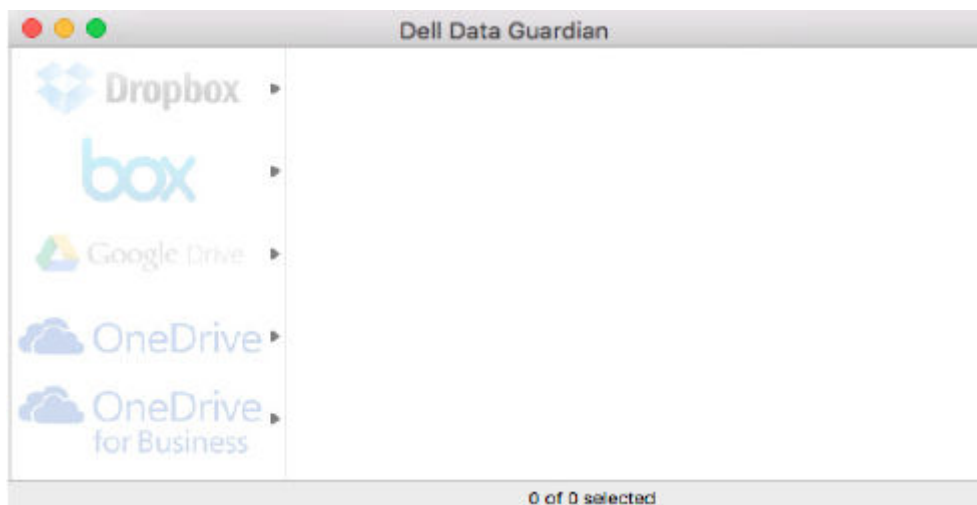
For more information on authentication, see the online Dell Data Guardian Help.

Dell Data Guardian application

When the Dell Data Guardian application opens and activation is successful, the faded cloud storage provider name displays in the left pane.

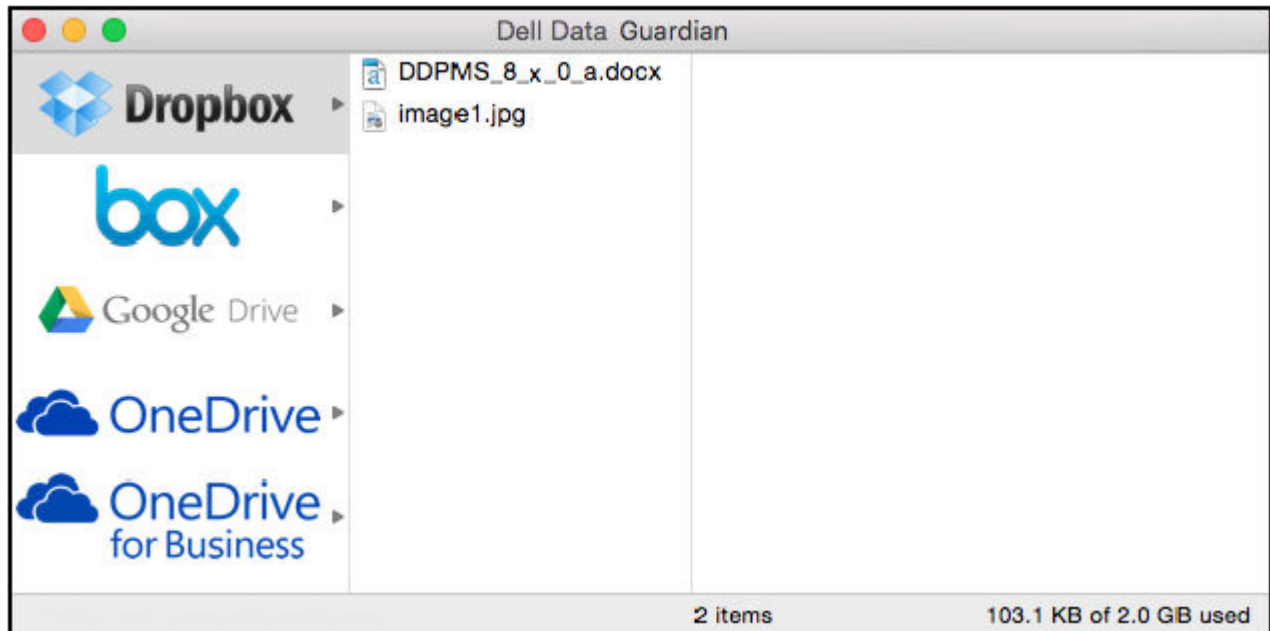
If an enterprise wants all users to collaborate using the same cloud provider, the administrator can set a policy to enable only that provider and to block the others from displaying.

If authentication for Data Guardian is revoked or expires, the cloud storage provider name is also grayed out.



- 1 In the left pane, select the cloud storage provider.
- 2 A window opens, prompting for your credentials. Enter your credentials.

When authenticated, the cloud storage provider name is activated.



Uninstall Data Guardian

This section describes the administrator process to uninstall Data Guardian. You must have a local administrator account to perform the uninstallation. If a user has a local administrator account, they can uninstall Data Guardian for Mac themselves.

Do one of these to remove Data Guardian:

Finder

- 1 While pressing the <option> key, select **Go** from the menu bar.
- 2 Open the **~/Library/Application Support/Dell** folder.
- 3 Right-click the **DellDataGuardian** folder, and select **Move to Trash**.
- 4 From **Go** in the menu bar, open the Applications folder and move the **Dell Data Guardian** application to Trash.
- 5 Click **OK**.
- 6 If prompted, enter the administrator password.

Terminal

You may have Data Guardian in one or both of the following locations .

- 1 Use these commands:
 - `rm -R ~/Applications/Data\ Guardian.app`
 - `rm -R ~/Library/Application Support/Dell/DataGuardian`
- 2 Remove the **DellDataGuardian** folder.

Configure and Install Data Guardian for the Web Client

This web client allows users to view a protected Office document or .xen file without installing the Data Guardian client. As a general rule, Dell recommends installing the Dell Server first.

Download the OVA file

At initial installation, Data-Guardian-Web is delivered as an OVA file, an Open Virtual Application used to deliver software that runs on a virtual machine.

To download the OVA file:

- 1 Navigate to the [Data Guardian](#) Product Support page.
- 2 Click **Drivers & downloads**.
- 3 Next to *View all available updates for <OS version>*, click **Change OS**, and select the appropriate **VMware ESXi** or **Hyper-V** version.
- 4 Under *View by*: select **Show All**.
- 5 Under *Dell Data Security*, select **Download**.

Install Data Guardian for Web

Install and configure Data-Guardian-Web

Before you begin, ensure that all system and virtual environment Requirements are met.

- 1 Locate the Data Guardian files in the installation media and double-click **Data-Guardian-Web-1.x.x.ova** to import into VMware.
- 2 Power on Data-Guardian-Web.
- 3 Select the language for the license agreement, and select **Display EULA**.
- 4 Read the agreement, and select **Accept EULA**.
- 5 If an update is available, select **Accept**.
- 6 At the default password change prompt, select **Yes**.
- 7 In the *Set ddguser Password* screen, enter the current (default) password, **ddguser**, then enter a unique password, re-enter the unique password, and select **OK**.

Passwords must include the following:

- At least 8 characters
 - At least 1 uppercase letter
 - At least 1 digit
 - At least 1 special character
- 8 Repeat the previous step for the *ddgconsole* and *ddgsupport* accounts.



NOTE:

To keep the default password, which is the same as the name, click **Cancel**. To modify the password, enter **ddgconsole** or **ddgsupport** in the *Current Password* field.

- 9 In the *Configure Hostname* dialog, use the backspace key to remove the default hostname. Enter an FQDN hostname and select **OK**.
- 10 If you have multiple nodes and a load balancer, enter a Load Balancer hostname.
- 11 In the *Configure Network Settings* dialog, choose either option below, then select **OK**.
 - (Default) Use DHCP
 - (Recommended) In the Use DHCP field, press the space bar to remove the X and manually enter these addresses, as applicable:
Static IP Network Mask Default Gateway DNS Server 1 DNS Server 2 DNS Server 3

NOTE:

When using a static IP, you must also create a host entry in the DNS server.

When 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.

- 12 When the scp screen displays, do not click OK. You must first add the .cer and .key files to the application or extract it from the CA's .pfx or .p7b file. See [Use the WinSCP tool](#).

NOTE:

If you click OK on the scp screen before extracting these, you must restart Data-Guardian-Web and navigate through to the *Configure Network Settings* dialog.

Use the WinSCP tool

In Windows, use your ddgconsole account to scp the SSL certificate file and SSL key file.

- 1 In Windows, open the WinSCP tool.
- 2 On the WinSCP page, enter the hostname.
- 3 Enter the default ddgconsole user name and default password (or your modified user name and password).
- 4 Click **Login**.
- 5 Drag the certificate and key, .pfx file, or .p7b file from your local drive to the **opt/dell/files** directory.
- 6 If you added a .pfx file or .p7b file, enter a password when prompted. The certificate and key are extracted from the CA and added to **apache2/ssl/folder**.

Optionally, instead of dragging the .pfx or .p7b file, you can manually extract the certificate. Here is sample code:

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

Here is sample code for extracting the private key from the .pfx file:

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

- 7 Return to the Administration Console's scp screen.

Administration Console

On the Administration Console's scp screen:

- 1 Click **OK**. The *Apache2 Reverse Proxy Certificate Installation* screen opens, listing the certificate.
- 2 Select a certificate and press **Enter**.
- 3 Do one of these:
 - If you added a key on the WinSCP tool, select the key at the next screen and press **Enter**.
 - If you entered a password on the WinSCP tool for a .pfx file or .p7b file, enter the password when prompted and click **OK**.
- 4 At the *Set Dell Server* screen, enter the name of your Dell Server hostname and click **OK**. A dialog displays, listing a URL to use when provisioning. The URL is in this format: **https://node.domain.com/edap-admin-ui/provision_node**.

NOTE:

node.domain.com is the name you entered in *Configure Hostname*. The URL points to that node.

- 5 Open a browser and type that URL.
- 6 When the Data Guardian node provisioning page opens, click **Start Node Provisioning**.
- 7 At the Login page, enter your domain email and password and click **Login**. Dell Data Guardian dialog states that provisioning was successful.
- 8 Return to the Administration Console screen that listed your URL and click **OK**. The application server restarts and the Administration Console > Main Menu opens.

Additional tasks:

- Provide the URL to internal users to allow them to access the Data Guardian web client.
 - For a single node, the URL is in this format: **https://nodename/** where nodename reflects the hostname entered in the *Configure Hostname* screen.
 - For a multiple nodes, the URL is in this format: **https://loadBalancerName/** where nodename reflects the load balancer hostname entered in the *Configure Hostname* screen.
- To access the Server in the future for updates to this VM or to check the logs, you must enable SSH for this VM. Select **Basic Configuration > SSH Settings** to enable SSH for a ddgsupport user.
- In the Management Console, if you modify any node-based web portal policies, you must reboot the appliance. See [Reboot the Appliance](#). After restart, you must log in with your ddguser credentials.

Open the Management Console

Open the Management Console at <https://server.domain.com:8443/webui/>

The default credentials are **superadmin/changeit**.

The following web browsers are supported to access the Management Console:

- Internet Explorer 11.x or later
- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later
- Safari

Data Guardian Basic Terminal Configuration Tasks

Basic configuration tasks are accessed from the Main Menu.

Change Host Name

This task can be completed at any time. It is not required to begin using Data Guardian.

- 1 From the *Basic Configuration* menu, select **Host Name**.
- 2 Use the backspace key to remove the existing Data-Guardian-Web hostname then replace it with a new host name and select **OK**.

Change Network Settings

This task can be completed at any time. It is not required to begin using Data Guardian.

- 1 From the *Basic Configuration* menu, select **Network**.
- 2 In the *Configure Network Settings* screen, choose either option below then select **OK**.
 - (Default) Use DHCP (IPv4).
 - (Recommended) In *Use DHCP*, press the space bar to remove the X and manually enter these addresses, as applicable:

Static IP

Network Mask

Default Gateway

DNS Server 1

DNS Server 2

DNS Server 3

Either IPv6 or IPv4 can be selected for a static configuration.

 **NOTE:**

When using a static IP, you must create a host entry in the DNS server.

Change User Passwords

This task can be completed at any time. It is not required to begin using Data Guardian.

You can change passwords for these users:

- ddguser (Terminal administrator) - This user has access to the Data Guardian terminal and its menus.
- ddgconsole (shell access) - This user has Data Guardian shell access. Shell access is available for a network administrator to check and troubleshoot network connectivity.
- ddgsupport (Dell ProSupport administrator) - This user has "sudo" rights and should be used sparingly. For security purposes, you control the password for this account.

- 1 From the *Basic Configuration* menu, select **Change User Passwords**.
- 2 In the *Change User Passwords* screen, select user password to change and select **Enter**.
- 3 In the *Set Password* screen, enter the current password, enter the new password, re-enter the new password, and select **OK**.
Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

 **NOTE:**

To select different user accounts, use the "spacebar" key on the keyboard to display the selection list.

Enable SSH

This task can be completed at any time. It is not required to begin using Data Guardian.

You can enable SSH for the support administrator login, shell access, and the terminal command-line interface.

- 1 From the *Basic Configuration* menu, select **SSH**.
- 2 Highlight the user for which you want to enable SSH, press the space bar to enter an **X**, and select **OK**.

Start or Stop Services

Perform this task only if needed.

- 1 To simultaneously start or stop all services, from the *Basic Configuration* menu, select either **Start Application** or **Stop Application**.
- 2 At the confirmation prompt, select **Yes**.

NOTE:

Server state changes may require up to two minutes to complete.

Reboot the Appliance

Perform this task only if needed.

- 1 From the *Basic Configuration* menu, select **Reboot Appliance**.
- 2 At the confirmation prompt, select **Yes**.
- 3 After restart, log in to Data Guardian.

Shut down the Appliance

Perform this task only if needed.

- 1 From the *Basic Configuration* menu, scroll down and select **Shutdown Appliance**.
- 2 At the confirmation prompt, select **Yes**.
- 3 After restart, log in to Data Guardian.

Administrator Tasks

Set or Change Terminal Language

It is a best practice to restart the services any time a settings change is made.

- 1 In the Main Menu, select **Set Language**.
- 2 Use the arrow keys to select the preferred language.

Generate a System Snapshot Log

To generate a System Snapshot Log for Dell ProSupport, in the Main Menu, select **Support Tools**.

- 1 From the *Support Tools* menu, select **Generate System Snapshot Log**.
- 2 At the indication that the file is created, select **OK**.