Dell Data Protection | Dell Data Guardian para Mac

Guía del administrador v1.2

GUID-5B8DE7B7-879F-45A4-88E0-732155904029

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

GUID-559E7DE2-5F31-4AF0-8A01-987470FAB58C

© 2017 Dell Inc. Todos los derechos reservados. Dell, EMC, y otras marcas comerciales son marcas comerciales de Dell Inc. o de sus filiales. Puede que otras marcas comerciales sean marcas comerciales de sus respectivos propietarios.

Marcas comerciales y marcas comerciales registradas utilizadas en el conjunto de documentos de Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise y Dell Data Guardian: Dell™ y el logotipo de Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® y KACE™ son marcas comerciales de Dell Inc. Cylance®, CylancePROTECT y el logotipo de Cylance son marcas comerciales registradas de Cylance, Inc. en los EE. UU. y en otros países. McAfee McAfee® y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, Inc. en los Estados Unidos y en otros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® y Xeon® son marcas comerciales registradas de Intel Corporation en los EE. UU. y en otros países. Adobe®, Acrobat®, y Flash® son marcas comerciales registradas de Adobe Systems Incorporated. Authen Tec® y Eikon® son marcas comerciales registradas de Authen Tec. AMD® es una marca comercial registrada de Advanced Micro Devices, Inc. Microsoft®, Windows® y Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® y Visual C++® son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y otros países. VMware® es una marca comercial o una marca comercial registrada de VMware, Inc. en Estados Unidos o en otros países. Box® es una marca comercial registrada de Box. DropboxSM es una marca de servicio de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® y Google™ Play son marcas comerciales o marcas comerciales registradas de Google Inc. en los Estados Unidos y en otros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® y Siri® son marcas de servicio, marcas comerciales o marcas comerciales registradas de Apple, Inc. en los Estados Unidos y/o en otros países. GO ID®, RSA® y SecurID® son marcas comerciales registradas de Dell EMC. EnCase™ y Guidance Software® son marcas comerciales o marcas comerciales registradas de Guidance Software. Entrust® es una marca comercial registrada de Entrust®, Inc. en Estados Unidos y otros países. InstallShield® es una marca comercial registrada de Flexera Software en Estados Unidos, China, Unión Europea, Hong Kong, Japón, Taiwán y Reino Unido. Micron® y RealSSD® son marcas comerciales registradas de Micron Technology, Inc. en Estados Unidos y otros países. Mozilla® Firefox® es una marca comercial registrada de Mozilla Foundation en los Estados Unidos y/o en otros países. iOS® es una marca comercial o una marca comercial registrada de Cisco Systems, Inc. en los Estados Unidos y en determinados países y se utiliza bajo licencia. Oracle® y Java® son marcas comerciales registradas de Oracle y/o sus filiales. Los demás nombres utilizados pueden ser marcas comerciales de sus respectivos propietarios. SAMSUNG™ es una marca comercial de SAMSUNG en los Estados Unidos o en otros países. Seagate® es una marca comercial registrada de Seagate Technology LLC en Estados Unidos y otros países. Travelstar® es una marca comercial registrada de HGST, Inc. en Estados Unidos y otros países. UNIX® es una marca comercial registrada de The Open Group. VALIDITY™ es una marca comercial de Validity Sensors, Inc. en los Estados Unidos y en otros países. VeriSign® y otras marcas relacionadas son las marcas comerciales o marcas comerciales registradas de VeriSign, Inc. o sus afiliados o filiales en los Estados Unidos y en otros países y han otorgado la licencia a Symantec Corporation. KVM on IP® es una marca comercial registrada de Video Products. Yahoo!® es una marca comercial registrada de Yahoo! Inc. Este producto utiliza partes del programa 7-Zip. El código fuente se puede encontrar en 7-zip.org. Con licencia GNU LGPL + restricciones de unRAR (7-zip.org/license.txt).

Dell Data Guardian for Mac Administrator Guide (Guía del administrador de Dell Data Guardian para Mac)

2017 - 04

Rev. A01

Tabla de contenido

1 Introducción a Dell Data Guardian para Mac 4
- Descripción general 4
- Cómo ponerse en contacto con Dell ProSupport 4

2 Requisitos de Dell Data Guardian para Mac 6
- Servidor 6
- Hardware del cliente Mac 6
- Sistemas operativos 6
- Proveedores del almacenamiento en la nube 7

3 Tareas de instalación de Data Guardian 8
- Requisitos previos 8
- Políticas 8
- Tareas de Dell Enterprise Server 8
  - Configuración del servidor de seguridad para permitir que el cliente realice descargas desde la nube 8
  - Permitir o denegar usuarios en la lista de acceso total/lista negra 9
  - Eliminación remota de la cuenta de Dropbox for Business de un miembro del equipo 11
- Tareas del cliente 12
  - Requisitos previos 12
  - Prácticas recomendadas 12
  - Instalación del cliente 12

4 Activación y experiencia de usuario de Data Guardian 14
- Activación del usuario final 14
- Interfaz de usuario 14
  - Evitar la opción Desproteger en el sitio web 15
- Preferencias de la aplicación 15
- Seguridad y otras consideraciones para Data Guardian y clientes de sincronización en la nube 17
  - Google Drive 17
  - OneDrive for Business 17
- Comentarios sobre este producto 17

5 Tareas de desinstalación de Data Guardian 18
- Requisitos previos 18
- Desinstalación de Data Guardian 18

6 Glosario 19

Introducción a Dell Data Guardian para Mac

Esta guía proporciona la información necesaria para administrar el software de cliente en la nube para Mac.

GUID-DC905DCF-89A3-4894-B120-B1ED63272AA5

Descripción general

Dell Data Guardian para Mac protege los datos en sistemas de uso compartido de archivos basados en la nube. Los equipos Mac OS X que utilizan Data Guardian pueden ver, modificar y cifrar archivos en sistemas de uso compartido de archivos basados en la nube para disfrutar de un almacenamiento seguro.

Tanto Data Guardian para Mac como para Windows pueden abrir archivos cifrados por el otro.

Data Guardian para Mac se compone de los siguientes elementos:

- Data Guardian:
  - **Cifrado en la nube**: protege los datos en sistemas de uso compartido de archivos basados en la nube como archivos .xen.
  - **Documentos de Office protegidos**: protege los documentos de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) en la nube y muestra el nombre de archivo y la extensión originales. Si están protegidos, los archivos solo se pueden abrir con un cliente de Data Guardian. Si se abre en otro lugar, aparecerá una página de portada donde se indicará que el documento está protegido y se explicará cómo puede un usuario autorizado solicitar el acceso al archivo cifrado.

    Puede establecer políticas para el cifrado en la nube únicamente o para ambos grupos de políticas. Para obtener más información, consulte *Admin Help*.

    Data Guardian para Mac está diseñado para compartir archivos en proveedores de cifrado en la nube. Sin embargo, si las políticas "Documentos de Office protegidos" están activadas para los Mac, se perderán todas las auditorías y seguimientos de archivos si el usuario final guarda el archivo en el Mac local. Si necesita una auditoría y seguimiento estricto de los archivos en su organización, establezca la política *Permitir la activación de Data Guardian en Mac* en "No seleccionada" para evitar la activación de Data Guardian en Mac.
- Servidor de seguridad: un componente del servidor Dell que administra Data Guardian para Mac. El servidor de seguridad garantiza que los datos estén protegidos en la nube, independientemente de con quien se compartan. El servidor de seguridad también protege los dispositivos internos para evitar que transmitan datos confidenciales.
- Remote Management Console: proporciona una administración centralizada de las políticas de seguridad, se integra con los directorios empresariales existentes y crea informes.

  Estos componentes de Dell interactúan sin ningún problema para ofrecer un entorno seguro sin perjudicar la experiencia del usuario.

GUID-B47CD81A-486F-43A5-816B-86A247C276EA

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell Data Protection 24 horas al día 7 días a la semana.

De manera adicional, puede obtener soporte en línea para su producto Dell Data Protection en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport .

Requisitos de Dell Data Guardian para Mac

En este capítulo se enumeran los requisitos de hardware y software. Asegúrese de que los entornos de implementación cumplen los requisitos antes de continuar con las tareas de implementación.

NOTA:
No es compatible con IPv6.

GUID-213663B0-B65F-4945-B2F1-5BEF78085BDF

Servidor

Data Guardian para Mac requiere que el cliente esté conectado a un Dell Enterprise Server o Dell Enterprise Server - VE, v9.6 o posterior.

GUID-371FFDE5-7A34-4268-AA88-617E73C0F9A4

Hardware del cliente Mac

A continuación se indica el hardware compatible con el cliente Mac.

Hardware de Mac

- Procesadores Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM
- 10 GB de espacio de disco libre

GUID-3F5F6005-9FEE-46AE-8400-336215F15DB2

Sistemas operativos

A continuación se indican los sistemas operativos compatibles.

Sistemas operativos Mac

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.3 y 10.12.4

Sistemas operativos Android

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow
- 7.0 Nougat

Sistemas operativos iOS

- iOS 8.x
- iOS 9.x
- iOS 10.x-10.3

GUID-C4B25B4F-15E5-42AF-9493-D09F2473A534

Proveedores del almacenamiento en la nube

En función de los valores de la política, pueden mostrarse los elementos siguientes en la interfaz de Dell Data Guardian. El usuario no tiene que descargar ni instalar el cliente de sincronización en la nube.

Proveedores del almacenamiento en la nube

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

Tareas de instalación de Data Guardian

GUID-168A1BC7-0DED-43F2-9A99-08FC43099963

Requisitos previos

Antes de llevar a cabo estas tareas, confirme lo siguiente:

- Instale el servidor Dell y sus componentes. Consulte una de las opciones siguientes:
  - *Enterprise Server Installation and Migration Guide (Guía de instalación y migración de Enterprise Server)*
  - *Virtual Edition Quick Start Guide and Installation Guide (Guía de instalación y Guía de inicio rápido de Virtual Edition)*
- En la Remote Management Console, asigne un rol de administrador de Dell pertinente.

GUID-D9C4A912-436F-415D-9499-BAE4F1B53233

Políticas

De manera predeterminada, Data Guardian cifra los archivos de los usuarios y envía eventos de auditoría al DDP EE Server/VE Server. A efectos del presente documento, ambos servidores se citan como servidor Dell, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Dell Enterprise Server - VE).

Si desea que los eventos de auditoría incluyan datos de geolocalización, debe activar la Wifi. Para obtener más información sobre la geolocalización y los eventos de auditoría, consulte *AdminHelp*.

Para cambiar el comportamiento predeterminado para cada proveedor de almacenamiento en la nube, configure la política *Proveedores de protección del almacenamiento en la nube*. Si su empresa prefiere un proveedor específico de almacenamiento en la nube, establezca la política en **Bloquear** para otros proveedores. Para obtener información acerca de las políticas, consulte *AdminHelp*, al que puede acceder desde la Remote Management Console del servidor Dell.

NOTA:
La opción Omitir de la política es para Windows. Si se selecciona Omitir para Mac, se muestra como Permitir para el usuario final.

GUID-EE401419-8E85-45A9-9776-2C16EEE3FDB0

Tareas de Dell Enterprise Server

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D649C05B

Configuración del servidor de seguridad para permitir que el cliente realice descargas desde la nube

DDP Enterprise Server

1 En DDP Enterprise Server, vaya a <Directorio de instalación de Security Server>\webapps\cloudweb\brand\dell\resources\
2 Abra el archivo **messages.properties** con un editor de texto.
3 Compruebe que las entradas sean las siguientes.
Para la instalación **local**:

download.deviceWin.mode=local

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

Para la instalación **remota**:

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

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

4 Guarde y cierre los archivos.
5 Vaya a <Directorio de instalación de Security Server> y cree una carpeta con el nombre Download (Security Server\Download).
6 En la carpeta Download, cree una carpeta CloudWeb (Security Server\Download\CloudWeb).
7 Añada los instaladores de Dell Data Guardian a dicha carpeta.

Virtual Edition: instalación manual de una versión del cliente de nube diferente

No se requiere ninguna acción para permitir que los usuarios descarguen el instalador de Dell Data Guardian más reciente. El instalador más reciente está preinstalado en VE Security Server.

Para instalar manualmente una versión del instalador de Data Guardian diferente en VE Security Server, actualice el archivo message.properties.

1 Vaya a:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Abra el archivo **messages.properties** con un editor de texto.
Para la instalación **local**:

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

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

Para la instalación **remota**:

download.deviceWin.mode=remote

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

3 Guarde y cierre los archivos.
4 Copie los archivos en /opt/dell/server/security-server/download/cloudweb.
5 Añada los instaladores de Data Guardian a esa carpeta.

GUID-40291F18-814A-40EC-9D60-A185154BA6FC

Permitir o denegar usuarios en la lista de acceso total/lista negra

Las entradas en las listas negra y de acceso total determinan qué usuarios pueden registrarse en el servidor Dell para utilizar Data Guardian.

Lista de acceso total

La lista de acceso total permite a usuarios o grupos de usuarios específicos registrarse en el servidor Dell y utilizar Data Guardian.

Los usuarios externos se deben colocar en la lista de acceso total para permitir el registro. Consulte los ejemplos siguientes para permitir que los usuarios se registren:

Tipo de usuario	Introducir
Todas las direcciones de correo electrónico tipo organizacion.com	`organization.com`
Un usuario específico	`jdoe@organization.com`
Todos los usuarios de Gmail	`gmail.com`

Lista negra

La lista negra evita que usuarios o grupos de usuarios específicos se registren en el servidor Dell y utilicen Data Guardian. Los usuarios de correos electrónicos que se introduzcan en la lista recibirán un mensaje en el que se les informará de que no podrán registrarse en Data Guardian.

NOTA:
Si un usuario ya está registrado, esta lista **no** le impedirá utilizar Data Guardian.

Puede usar la lista negra para excluir a ciertos usuarios que forman parte de grupos aprobados en la lista de acceso total. Además, puede incluir dominios enteros en la lista negra, para evitar el registro de cualquiera que tenga un correo electrónico de ese dominio. Consulte los ejemplos siguientes para impedir que un usuario o un grupo se registren en el servidor Dell:

Tipo de usuario	Introducir
Todas las direcciones de correo electrónico tipo organizacion.com	`organization.com`
Un usuario específico y su dirección de correo electrónico	`jdoe@organization.com`
Todos los usuarios de Gmail	`gmail.com`

Para modificar la lista de acceso total/lista negra, siga estas instrucciones:

1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración > Administración de usuario externo**.

2 Haga clic en **Agregar**.

3 Seleccione Tipo de acceso al registro:

Lista negra: bloquea el registro de un usuario o dominio. El usuario no puede abrir un documento de Office o archivo .xen protegido.

Lista de acceso total: permite el registro y el acceso a todos los archivos a un usuario o dominio. Si el usuario o dominio también están en la lista negra, no se le otorgará acceso.

4 En el campo Introducir dominio/correo electrónico, introduzca el dominio del usuario para otorgar acceso a todo el dominio o la dirección de correo electrónico para otorgar acceso únicamente a ese usuario.

5 Haga clic en **Agregar**.

Para obtener más información sobre el uso de la lista de acceso total/lista negra, consulte *AdminHelp*, accesible desde la Remote Management Console del servidor Dell.

Los usuarios externos pueden solicitar el acceso de un usuario interno a la clave de un archivo protegido. Si el usuario interno no está disponible, puede utilizar la Remote Management Console para aprobar o denegar el acceso.

1 Seleccione **Administración > Administración de solicitudes de claves**.

2 Para obtener más información, seleccione **?** (Ayuda).

GUID-036F598E-1FF3-4FC8-A419-2F628C92F934

Eliminación remota de la cuenta de Dropbox for Business de un miembro del equipo

Si su empresa utiliza Dropbox for Business, puede quitar remotamente a un miembro del equipo de la cuenta corporativa del equipo en Dropbox for Business si, por ejemplo, el usuario deja la empresa. Los archivos y las carpetas asociados con la cuenta del miembro del equipo se quitarán de todos los dispositivos que utilicen la cuenta. Esta acción revoca el acceso de ese usuario a los archivos.

Requisitos previos

NOTA:
Antes de llevar a cabo este procedimiento, deberá hacer una copia de seguridad de los archivos y las carpetas de la cuenta del miembro del equipo que la empresa u otros miembros del equipo en Dropbox for Business puedan necesitar.

Solo un administrador de Dropbox for Business puede eliminar remotamente una cuenta de Dropbox for Business.

El usuario final debe tener Dell Data Guardian activado y conectado a Dropbox for Business.

Registrarse en la Remote Management Console

Solo tiene que registrarse un administrador de Dropbox for Business.

1 En el panel izquierdo de la Remote Management Console, seleccione **Administración** > **Administración de Dropbox**.
2 En la página de Dropbox for Business, haga clic en **Registrar**.
El navegador abre el sitio de Dropbox for Business.
3 Si se le solicita, inicie sesión en Dropbox con su cuenta de administrador de Dropbox for Business.
4 Para permitir el acceso a Dell Data Guardian, haga clic en **Permitir**.
Se mostrará una página de confirmación que indica que se otorga la autorización de Dropbox a DDP Enterprise Server - VE.
5 En la Remote Management Console, vuelva a **Administración** > **Administración de Dropbox** y haga clic en **Actualizar**.
Se mostrará el nombre del administrador.

NOTA:
Por lo general, se recomienda no anular el registro. Sin embargo, para retirar los privilegios del Administrador de Dropbox for Business de eliminación de miembros del equipo de Dropbox for Business, haga clic en **Anular registro**.

Eliminación remota de la cuenta de un miembro del equipo

NOTA:
La opción Eliminación remota solo está disponible para cuentas de miembros del equipo de Dropbox for Business registradas. Si la opción Eliminación remota no se muestra para una cuenta de usuario, es porque el usuario no tiene una cuenta registrada de Dropbox for Business.

1 En la Remote Management Console, seleccione **Poblaciones** > **Usuarios** en el panel izquierdo.
2 Busque el usuario específico.
3 Acceda a la página **Detalles del usuario**.
4 En la columna Comando, haga clic en **Eliminación remota**.
Se llevará a cabo la eliminación remota.

NOTA:
Antes de seleccionar Eliminación remota, deberá hacer una copia de seguridad de los archivos y las carpetas de la cuenta del miembro del equipo que la empresa u otros miembros del equipo en Dropbox for Business puedan necesitar.

5 Cuando se solicite la confirmación para la eliminación remota, haga clic en **Sí**.
En la página Detalles del usuario se indica la fecha en la que se realizó la eliminación remota.

6 En la página de miembros de la administrator Console de Dropbox for Business, actualice la lista de Miembros del equipo.
El usuario se quita de la lista. Puede seleccionar la pestaña **Miembros eliminados** para comprobar qué usuarios se han eliminado.

GUID-B495F3E1-6516-4DFC-9107-4AA52FE296AB

Tareas del cliente

GUID-88098FA1-F419-45AD-A4BA-F5C30D04DDE3

Requisitos previos

- Asegúrese de que los dispositivos de destino pueden conectarse a:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Asegúrese de que el usuario que lleva a cabo la instalación tiene cuenta de administrador local para instalar.
- Si la instalación se hace con la línea de comandos, asegúrese de que tiene el nombre de dominio completo del Dell Security Server en el que los usuarios se activarán.

GUID-5A15F45E-2F97-4EB4-90CD-66CD73275BAB

Prácticas recomendadas

Durante la implementación, asegúrese de que sigue los métodos recomendados para TI. Esas prácticas incluyen, pero sin limitarse a:

- Entornos de prueba controlados para las pruebas iniciales.
- Implementaciones escalonadas para los usuarios.

GUID-CF4B88F3-DBAF-4834-B15B-8815EEA72B9D

Instalación del cliente

En este punto, los usuarios que se añadieron a la lista blanca pueden registrase en: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Tras registrarse, el usuario recibe un correo electrónico que le dirige a https://yoursecurityservername.domain.com:8443/cloudweb para que inicie sesión y se descargue el cliente apropiado.

La instalación del cliente Mac es opcional para los administradores, ya que los usuarios finales suelen instalar el cliente Mac ellos mismos (después del registro) desde https://yoursecurityservername.domain.com:8443/cloudweb.

No obstante, puede instalar el cliente Mac si su organización lo considera necesario. Instale el cliente de Data Guardian mediante la interfaz de usuario o la línea de comandos, utilizando cualquier tecnología de inserción que esté disponible en su organización. El registro y la activación por parte del usuario final siguen siendo necesarios.

Actualización desde versiones anteriores de Cloud Edition

Si una empresa tiene una versión anterior de Cloud Edition y actualiza a Data Guardian, se elimina la versión anterior de Cloud Edition.

NOTA:
Si una empresa actualiza de Cloud Edition a Data Guardian, los usuarios deben autenticarse y volver a vincular Data Guardian con su proveedor de almacenamiento en la nube. Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

Opciones de instalación

Para instalar/actualizar el cliente, seleccione una de las opciones siguientes:

- Instalación interactiva: este es el método más sencillo para instalar Data Guardian para Mac. No obstante, utilice este método si únicamente tiene previsto instalar el cliente en un equipo cada vez.

  O bien

- Instalación con la línea de comandos: para este método avanzado de instalación, los administradores deben tener experiencia en sintaxis de la línea de comandos. Este método puede utilizarse para una instalación con secuencia de comandos, utilizando archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.

Instalación interactiva

1. Para el cliente de Data Guardian, localice el instalador en **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilice el archivo **.pkg** almacenado en DDPSL-Explorer-0.x.x.xxxx.dmg para la instalación o actualización. Puede utilizar una instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.
3. Haga doble clic en el paquete **Dell-Data-Guardian-x.x.x**.
4. Haga clic en **Continuar**.
5. En la ventana Introducción, haga clic en **Continuar**.
6. En la ventana Contrato de licencia de software, haga clic en **Continuar**.
7. Haga clic en **Aceptar** para continuar.
8. En la ventana Tipo de instalación, realice una de estas acciones:
   - Haga clic en **Instalar** y, a continuación, vaya al paso 9.
   - En la ventana Selección de destino, seleccione una de las siguientes opciones, haga clic en **Continuar con la instalación** y, a continuación, vaya al paso 9.
     - Instalar para todos los usuarios de este equipo
     - Instalar solo para mí
9. En el diálogo, introduzca su nombre de usuario y contraseña y haga clic en **Instalar software**.
10. En la página Resumen, haga clic en **Cerrar**.
11. Consulte Activación del usuario final.

NOTA:
Si una empresa actualiza de Cloud Edition a Data Guardian, los usuarios deben autenticarse y volver a vincular Data Guardian con su proveedor de almacenamiento en la nube. Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

Instalación con la línea de comandos

1. Monte el .dmg.
2. Utilice el comando de instalación para realizar la instalación del paquete con la línea de comandos:
   ```
   sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
   ```
3. Indique a los usuarios finales que activen Data Guardian. Consulte Activación del usuario final.

Activación y experiencia de usuario de Data Guardian

GUID-FCD7AF63-06D4-4D0C-8FA3-369265AB00E2

Activación del usuario final

Después de abrir Dell Data Guardian en el Mac por primera vez, siga estos pasos:

1 En Finder, seleccione **Aplicaciones** y haga doble clic en **Dell Data Guardian**.
2 Cuando se abra la ventana del servidor Dell, especifique la dirección del DDP Server y haga clic en **Guardar**.

   Se abrirá la ventana Credenciales.

3 Introduzca la dirección de correo electrónico y la contraseña de su dominio.
4 Haga clic en **Inicio de sesión** para activar Dell Data Guardian.

   Cuando la aplicación Dell Data Guardian se abra y la activación se realice correctamente, el nombre del proveedor de almacenamiento en la nube se activará en el panel de la izquierda.

   Si una empresa desea que todos los usuarios colaboren con el mismo proveedor de nube, el administrador puede establecer una política para permitir solo dicho proveedor y bloquear la visualización del resto.

   Si la activación no es correcta o si la autenticación para la aplicación Dell Data Guardian se revoca o caduca, se desactivará el nombre del proveedor de almacenamiento de nube.

5 En el panel de la izquierda, seleccione el proveedor de almacenamiento en la nube.

   Se abrirá una ventana en la que se le solicitarán sus credenciales.
6 Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

GUID-9917238E-00E5-4F56-909D-C76F09426D53

Interfaz de usuario

La interfaz de Dell Data Guardian es parecida a la interfaz de *Ver como columnas* del Finder de OS X. Cada columna representa una carpeta en el proveedor de almacenamiento en la nube seleccionado.

NOTA:
La barra de título puede variar según el sistema operativo.

Para cifrar y descifrar archivos, debe utilizar la interfaz de Dell Data Guardian, no el sitio web del proveedor de almacenamiento en la nube.

Puede realizar estas tareas en la ventana de Dell Data Guardian:

- **Archivo** > **Nueva carpeta** : para crear carpetas nuevas.

NOTA:
Google Drive y OneDrive agregan automáticamente una carpeta compartida. No obstante, no se admite el uso compartido de datos en OneDrive for Business.

- Menú contextual: seleccione una o más carpetas o archivos en la ventana principal. A continuación, haga clic en Control (o haga clic con el botón derecho) y seleccione una opción de menú:
  - **Descargar**
  - **Cambiar nombre**: cuando cambie el nombre de un archivo en la interfaz de Dell Data Guardian, Dell Data Guardian sincronizará el cambio con el sitio web del proveedor de almacenamiento en la nube. No cambie el nombre de un archivo .xen en el sitio web del proveedor de almacenamiento en la nube. No se sincronizará.
  - **Eliminar**

    NOTA:
    Google Drive con Data Guardian no tiene la opción de Quitar (pone el elemento en la papelera). Solo ofrece la opción de Eliminar, para ofrecer consistencia con otra funcionalidad de Data Guardian.
- **Desvincular**: para desvincular Dell Data Guardian de un proveedor de almacenamiento en la nube, seleccione el proveedor en el panel izquierdo, haga clic en Control (o haga clic con el botón derecho) y, a continuación, seleccione Desvincular en el menú.

Información adicional sobre archivos y carpetas:

- Para agregar archivos y carpetas a carpetas mostradas en la interfaz de usuario de Dell Data Guardian, arrástrelos del Finder de OS X u otras aplicaciones que admitan la función arrastrar y soltar. Los archivos se cifrarán conforme a la política actual.
- Para descifrar y abrir archivos en aplicaciones, haga doble clic en el archivo en la ventana de Dell Data Guardian. Si el archivo se modifica en una aplicación externa, el archivo modificado se cifrará y se cargará como una nueva revisión en el proveedor de almacenamiento en la nube.
- Para realizar una copia local no cifrada, arrastre un archivo o una carpeta desde la ventana de Dell Data Guardian hasta Finder.
- El cifrado en la nube de Data Guardian no permite que se editen archivos sin extensiones. Esos archivos se tratan como archivos de solo lectura. Para editar un archivo sin extensión, descárguelo desde el sitio web del proveedor de almacenamiento en la nube, edítelo y, a continuación, súbalo mediante la interfaz de Dell Data Guardian.
- Los atributos extendidos no se copian en la nube.

GUID-12385ECF-2D63-4BD1-8719-260F247D161E

Evitar la opción Desproteger en el sitio web

Data Guardian no protege o cifra los archivos que se utilizan con la opción *Abrir y desproteger* en el sitio web de OneDrive for Business o de cualquier proveedor de almacenamiento en la nube. Si abre y desprotege un archivo, no utilice el comando de abrir en la interfaz de Dell Data Guardian, porque se bloqueará la carga automática.

Al proteger archivos con Data Guardian, utilice la interfaz de Dell Data Guardian para trabajar con los archivos.

Si desea trabajar con un archivo que tiene propiedades especiales desde el sitio web del proveedor de almacenamiento en la nube:

1 En la interfaz de Dell Data Guardian, haga clic en Control (o haga clic con el botón derecho) en un archivo y seleccione **Descargar**.
2 Seleccione y edite el archivo.
3 Desde la interfaz de Dell Data Guardian, cargue el archivo.

GUID-B18B3439-4C04-4F3A-AADA-DD5552F902D6

Preferencias de la aplicación

Para iniciar las Preferencias:

1 Inicie Dell Data Guardian.
2 En la barra de menú Dell Data Guardian, seleccione **Preferencias.**

NOTA:
Esta información también está disponible desde el icono de Ayuda.

Puede modificar estos valores:

- Ocultar archivos que comienzan con ".": de manera predeterminada, la casilla está marcada, de modo que se ocultan los archivos. Para ver los archivos ocultos, desmarque la casilla de verificación.

  NOTA:
  Normalmente, los archivos que llevan como prefijo un separador de punto se ocultan en el Finder de OS X.

- **Desvincular proveedor de almacenamiento en la nube**: muestra los proveedores almacenamiento en la nube autenticados por Data Guardian. Para quitar a un proveedor de almacenamiento en la nube de Data Guardian, seleccione el nombre del proveedor y haga clic en el botón con el signo menos (-) en la parte inferior izquierda de la ventana Preferencias.

Políticas de servidor: el administrador de DDP Server establece las siguientes políticas que controlan la forma en que Data Guardian administra archivos y carpetas:

- **DDP Server**: muestra la URL del servidor.
- **Intervalo de sondeo:** muestra el intervalo en minutos que el software de cliente sondea en busca de actualizaciones de política.
- **Cifrar**: la política de cifrado maestra que permite cifrar las carpetas y archivos en el sitio web de almacenamiento en la nube.
- **Solo extensión** u **Ofuscación**

  Solo extensión (valor predeterminado de la política) muestra el nombre del archivo en el sitio web.

  Si una empresa exige protección adicional para los archivos, establezca esta política en **Ofuscación** para ocultar los nombres de archivo en el sitio web de la nube como nombres de GUID.

  NOTA:
  Si la política se estableció primero en Solo extensión y los usuarios tienen archivos en el sitio web de la nube y, a continuación, la política se cambia a Ofuscación, los nombres de los archivos preexistentes en el sitio web no se ofuscarán. Para ofuscar los nombres de los archivos preexistentes, el usuario debe descargar y, a continuación, volver a cargar los archivos mediante la interfaz de Data Guardian. O bien, si el usuario edita un archivo, se cargará con un nombre de archivo ofuscado.

- **Documentos de Office protegidos**: protege los documentos de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) en la nube pero muestra la extensión de archivo, no una extensión .xen.

  Si se habilita esta política, los documentos de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) en la nube mostrarán la extensión de archivo, no una extensión .xen. Sin embargo, los archivos no se pueden abrir en la nube o si se descargan. En caso de abrirlos, solo se mostrará una portada que indica que el documento está protegido. Si ha instalado Data Guardian pero no se ha autenticado, la portada lo indicará.
- **Eventos de auditoría**: si está activada, se envían eventos de auditoría al servidor Dell.
- **Geolocalización**: si está activada, los eventos de auditoría que se envían al servidor de Dell incluyen datos de geolocalización (latitud y longitud).
- **Punto de referencia de devolución de llamada**: si está activada, se envía un punto de referencia de devolución de llamada en todos los archivos protegidos de Office.
- **URL de punto de referencia de devolución de llamada**: si está activada, especifica la URL que se utilizará cuando se inserte el punto de referencia de devolución de llamada en los archivos protegidos de Office.
- **Proveedores de protección del almacenamiento en la nube**: se muestra un nombre de proveedor según la configuración de la política. Las opciones son **Box/Dropbox/Google Drive/OneDrive y OneDrive for Business**.

Habilite o deshabilite el cifrado de los archivos cargados en ese proveedor de almacenamiento en la nube. Se mostrará una de las opciones siguientes:

- **Cifrar:** se cifran los archivos que se envían a la nube.
- **Permitir:** el usuario puede acceder a los archivos de la nube, pero los archivos que se envían a un proveedor de almacenamiento en la nube no se cifran.
- **Bloqueado:** el proveedor de almacenamiento en la nube no está disponible y en este momento significa que el nombre del proveedor de almacenamiento en la nube no aparece en la ventana principal.

GUID-74395D32-C5C3-46A5-A090-CE195AD50CC0

Seguridad y otras consideraciones para Data Guardian y clientes de sincronización en la nube

GUID-ED3DC4CF-B650-4593-83F3-84FE0268BBC3

Google Drive

El cifrado en la nube de Data Guardian cifra los archivos y carpetas en la nube para proteger los datos. Tenga en cuenta estas consideraciones.

- La política de seguridad corporativa, si se establece en Proteger, prohíbe el uso de documentos de Google Docs con Data Guardian. Si se establece en Permitir, podrá editarlos. Para obtener más información, póngase en contacto con su administrador de TI.

  Google Drive contiene una aplicación de Google Docs que permite a los usuarios colaborar con documentos en tiempo real. No obstante, la colaboración se produce en un servidor de Google y los archivos no están cifrados. Los documentos que cree con Google Docs se mostrarán en las carpetas del proveedor de almacenamiento en la nube de Google Docs.

  Sin embargo, si abre la carpeta, un cuadro de diálogo le advertirá de que Data Guardian no puede cifrar ese documento.

GUID-5454F809-40A1-4609-BED2-7D3D06391FC4

OneDrive for Business

OneDrive for Business no admite compartir datos.

GUID-A6AA7EB4-E62B-44A2-BAC2-902473A21C42

Comentarios sobre este producto

Si la política lo permite, los usuarios pueden ofrecer sus comentarios sobre Dell Data Guardian. El formulario de comentarios está disponible en la barra de menú > **Ofrecer comentarios sobre Dell Data Protection**.

Tareas de desinstalación de Data Guardian

Esta sección describe el proceso del Administrador para desinstalar Data Guardian. Si el usuario final tiene cuenta de administrador local, puede realizar la desinstalación de Data Guardian para Mac por sí mismo.

GUID-0AEC84CA-AADA-44B7-A403-5D8C97FFAFD5

Requisitos previos

Debe tener una cuenta de administrador local para realizar la desinstalación.

GUID-C8A4F2ED-6FE8-4B26-A3FB-60795DD70304

Desinstalación de Data Guardian

Lleve a cabo una de estas acciones para quitar Data Guardian:

Finder

1 Mientras mantiene pulsada la tecla <opción>, seleccione **Ir** en la barra de menú.
2 Abra la carpeta **~/Library/Application Support/Dell**.
3 Elimine la carpeta **DataGuardian**.
4 Desde la barra de menú **Ir**, abra la carpeta Applications y elimine la aplicación **Data Guardian**.

Terminal

Es posible que tenga Data Guardian en una o ambas ubicaciones siguientes.

1 Utilice uno o los dos comandos siguientes:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Elimine la carpeta **DataGuardian**.

Glosario

Activar/activado: la activación se produce cuando el equipo se ha registrado en el servidor Dell y ha recibido al menos un conjunto de políticas inicial.

Servidor Dell: el servidor Dell lo forman un conjunto de componentes. Cuando se hace referencia a la parte de servidor del producto completo, se denomina conjuntamente como el servidor Dell.

Remote Management Console: la consola de administración remota es la consola administrativa para la implementación en toda la empresa. La Remote Management Console es un componente de Dell Enterprise Server.

Servidor de seguridad: un componente del servidor Dell que administra Dell Data Guardian. El servidor de seguridad garantiza que los datos estén protegidos en la nube, independientemente de con quien se compartan. El servidor de seguridad también protege los dispositivos internos para evitar que transmitan datos confidenciales.

Usuarios externos: son usuarios que están fuera del dominio de la empresa.