Dell Data Guardian

Guía del administrador v. 1.2

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.

Dell Data Guardian Administrator Guide (Guía del administrador de Dell Data Guardian)

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción

Toda la información sobre la política y sus descripciones se encuentran en la AdminHelp.

Antes de empezar

1 Instale EE Server/VE Server antes de implementar los clientes. Localice la guía correcta, tal como se indica a continuación, siga las instrucciones y, a continuación, vuelva a esta guía.

- *DDP Enterprise Server Installation and Migration Guide (Guía de instalación y migración de DDP Enterprise Server)*
- *DDP Enterprise Server – Virtual Edition Quick Start Guide and Installation Guide (Guía de instalación y Guía de inicio rápido de DDP Enterprise Server – Virtual Edition)*

Compruebe que las políticas están establecidas de la forma deseada. Explore la ayuda AdminHelp, disponible a través del signo **?** que se encuentra en el extremo derecho de la pantalla. AdminHelp es una ayuda a nivel de página diseñada para ayudarle a definir y modificar las políticas y conocer qué opciones tiene disponibles con EE Server/VE Server.

2 Lea detenidamente el capítulo Requisitos de este documento.

3 Implemente los clientes en los usuarios finales.

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.

Asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado teniendo su Código de servicio disponible cuando realice la llamada.

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

2

Requisitos

Servidor

Data Guardian requiere que el cliente esté conectado a un Dell Enterprise Server o Dell Enterprise Server - VE, v. 9.6 o superior. 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).

Cliente Data Guardian

- Durante la implementación se deberán seguir las prácticas recomendadas para TI. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados, para las pruebas iniciales e implementaciones escalonadas para los usuarios.
- La cuenta de usuario que realiza la instalación/actualización/desinstalación debe ser un usuario administrador local o de dominio, que puede ser designado temporalmente mediante una herramienta de implementación como Microsoft SMS o Dell KACE. No son compatibles los usuarios con privilegios elevados que no sean administradores.
- Realice copia de seguridad de todos los datos importantes antes de iniciar la instalación/desinstalación.
- Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Data Guardian no es compatible con Microsoft Office 365.
- Para el cifrado en la nube, el equipo debe tener una unidad de disco (valor de letra) asignable disponible.
- Asegúrese de que los dispositivos de destino pueden conectarse a https://yoursecurityservername.domain.com:8443/cloudweb/register y a https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configuradas cuentas de almacenamiento en la nube.

  Si los usuarios desean mantener sus cuentas existentes, deben asegurarse de retirar del cliente de sincronización todos los archivos que quieran conservar *sin cifrar* antes de instalar Data Guardian.
- Los usuarios deberán estar preparados para reiniciar sus equipos una vez que se instale el cliente.
- Data Guardian no interfiere con el comportamiento de los clientes de sincronización. Por lo tanto, los administradores y los usuarios finales deben familiarizarse con el funcionamiento de estas aplicaciones antes de implementar Data Guardian. Para obtener más información, consulte el servicio de asistencia de Box, en https://support.box.com/home, el servicio de asistencia de Dropbox, en https://www.dropbox.com/help, o el servicio de asistencia de OneDrive, en http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Si se ejecuta Office 2010: si las políticas se han establecido para proteger documentos de Office y habilitados para macros, los usuarios deben contar con Office 2010 Service Pack 1 o superior (v. 14.0.6029 o superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar si se ha aplicado un Service Pack a un conjunto de aplicaciones de Microsoft Office 2010. Sin esta actualización, no se puede acceder a los documentos protegidos. Los nuevos documentos de Office no estarán protegidos, independientemente de la política, a menos que la función de barrido se encuentre activada. El siguiente barrido convierte los documentos de Office en archivos protegidos, pero los usuarios no puedan acceder a ellos sin una versión de Office compatible.
- Aunque Dell Encryption no es necesario, si se usa, el cliente Encryption debe ser v. 8.12 o posterior.
- Data Guardian no es compatible con la herramienta Restaurar sistema de Windows.
- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.

Requisitos previos del cliente

Si no se ha instalado todavía, el instalador instala el paquete redistribuible Microsoft Visual C++ 2015 (x86 y x64).

NOTA:
Para los sistemas operativos Windows 7 y Windows 8.1, los equipos deben contar con todas las actualizaciones de Windows. Para obtener más información, consulte https://support.microsoft.com/en-us/help/2919355 y https://support.microsoft.com/en-us/help/2999226.

Se requiere Microsoft .Net 4.5.2 (o una versión posterior) para Data Guardian. Todos los equipos enviados desde la fábrica de Dell vienen con .Net 4.5.2 preinstalado. Sin embargo, si no está instalando en hardware de Dell o si está actualizando Data Guardian en hardware de Dell más antiguo, debería comprobar qué versión de .Net tiene instalada y, si fuera necesario, actualizar la versión antes de instalar Dell Data Guardian, con el fin de evitar errores durante la instalación/actualización. Para comprobar qué versión de .Net tiene instalada, siga estas instrucciones en el equipo en el que se va a realizar la instalación: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar Microsoft .Net Framework 4.5.2, acceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware del cliente de Windows

Los requisitos de hardware mínimos deben cumplir las especificaciones mínimas del sistema operativo. La tabla siguiente explica en detalle el hardware compatible con el cliente de Windows.

Hardware de Windows

- 200 MB de espacio libre en el disco, dependiendo del sistema operativo
- Tarjeta de interfaz de red 10/100/1000 o Wi-Fi
- Protocolo TCP/IP instalado y activado

Si su empresa cifra los datos para el almacenamiento en la nube, su equipo debe tener un carácter alfabético disponible para asignar a una unidad de disco.

Sistemas operativos

La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (32 bits y 64 bits)

- Windows 7 SP0-SP1
- Windows 8.1
- Windows 10

NOTA:
Windows 7 no es compatible con la política de geolocalización para los eventos de auditoría de Data Guardian.

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

Clientes de sincronización en la nube

La siguiente tabla muestra los clientes de sincronización en la nube compatibles con Data Guardian. A menudo se publican actualizaciones de los clientes de sincronización. Dell recomienda probar nuevas versiones de clientes de sincronización con Data Guardian antes de introducirlas en el entorno de producción.

Clientes de sincronización en la nube

- Dropbox
- Dropbox for Business (solo para Windows)

  NOTA:
  En función de la versión de servidor de Dell que utilice su empresa, todos los archivos y las carpetas de cuentas personales de Dropbox vinculadas a cuentas empresariales podrían cifrarse.

- Box

  NOTA:
  Las herramientas y la edición de Box no son compatibles con Data Guardian. El uso de herramientas de Box puede provocar que la pantalla se vuelva azul.

- Google Drive
- OneDrive
- OneDrive para la Empresa
- Unified OneDrive

  NOTA:
  Unified OneDrive es un cliente de sincronización unificado tanto para OneDrive como para OneDrive para la Empresa.

Navegadores web

Puede utilizar Data Guardian > Cifrado en la nube con Internet Explorer, Mozilla Firefox y Google Chrome.

NOTA:
Data Guardian > El cifrado en la nube no es compatible con el explorador Microsoft Edge.

Compatibilidad de idiomas

Estos clientes cumplen los requisitos de Multilingual User Interface (MUI) y se pueden configurar en los siguientes idiomas.

Compatibilidad de idiomas

- Inglés (EN)
- Español (ES)
- Francés (FR)
- Japonés (JA)
- Coreano (KO)
- Portugués brasileño (PT-BR)

Compatibilidad de idiomas

- Italiano (IT)
- Alemán (DE)
- Portugués europeo (PT-PT)

3

Configuración de registro

- Esta sección detalla toda la configuración de registro aprobada por Dell ProSupport para equipos **cliente** locales, con independencia del motivo de la configuración de registro. Si una configuración de registro coincide en dos productos, aparecerá en cada categoría.
- Los cambios de registro deben realizarlos únicamente los administradores y es posible que no sean adecuados para todas las situaciones.

Configuración del registro del cliente Data Guardian

- Se pueden aumentar los niveles de registro para ayudar a solucionar problemas. Cree o modifique el siguiente parámetro de registro:

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

  "LogVerbosity"=dword:0x1f (31)

  De manera predeterminada, el nivel de registro es 0xf (15).

  Valores disponibles:

  Desactivado = 0x0 (0)

  Crítico = 0x1 (1)

  Error = 0x3 (3)

  Aviso = 0x7 (7)

  Información = 0xf (15)

  Depuración = 0x1f (31)

- Una vez finalizada la instalación de Data Guardian, los usuarios internos se activan automáticamente. Si es necesario, puede modificar una configuración de registro para invalidar la activación automática.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valor DWORD: DisableAutomaticActivation=1

  NOTA:
  También puede confirmar los alias para su dominio en el servidor de Dell. Consulte Solución de problemas de activación automática.

Configuración del servidor para Data Guardian

En función de las políticas establecidas por el administrador, Data Guardian protege, por ejemplo, los siguientes datos:

- Sistemas de intercambio de archivos basados en la nube: los equipos o dispositivos móviles de Windows capturan datos destinados al almacenamiento en la nube, los cifra, y, a continuación, vuelva a cargarlos en la nube.
- Documentos de Office guardados en una ubicación local, compartidos con otros usuarios de diferentes formas o almacenados en medios extraíbles. Estos documentos de Office pueden estar protegidos: .docx, .pptx, .xlsx, .docm, .pptm o .xlsm.

Informe a los usuarios si su empresa utiliza Data Guardian solo con almacenamiento en la nube, solo con documentos de Office o con ambos.

Configuración de VE Server para Data Guardian

Si desea configurar VE Server para que sea compatible con Data Guardian, en la Remote Management Console, active una o ambas políticas de Data Guardian:

- *Documentos de Office protegidos*: solo nivel de empresa
- *Cifrado de nube*: empresa, grupos de extremos o nivel de extremos

Configuración de EE Server para Data Guardian

Si desea configurar EE Server para que sea compatible con Data Guardian, en la Remote Management Console, active una o ambas políticas de Data Guardian:

- *Documentos de Office protegidos*: solo nivel de empresa
- *Cifrado de nube*: empresa, grupos de extremos o nivel de extremos

A continuación, configure el servidor de seguridad para permitir descargas del cliente Cloud.

Configuración del servidor de seguridad para permitir descargas del cliente Data Guardian

Esta sección explica en detalle los pasos a seguir para permitir que los usuarios finales descarguen el cliente Data Guardian de Windows desde su Security Server.

1 En EE Server, acceda a **<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources**y abra el **archivo messages.properties** con un editor de texto.

2 Compruebe que las entradas sean las siguientes:

download.deviceWin.mode=remote

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

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe

3 Edite las entradas con los siguientes

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 Guarde y cierre el archivo.

5 Vaya a <Directorio de instalación de Security Server> y cree una carpeta nueva dentro con el nombre Download (Security Server \Download).

6 En la carpeta Descarga, cree otra carpeta nueva y denomínela cloudweb (Servidor de seguridad\Descarga\cloudweb).

7 Agregue los archivos de configuración de 64 y 32 bits de Data Guardian a la carpeta cloudweb y cámbieles el nombre si lo desea, por ejemplo, a DataGuardian64.exe y DataGuardian32.exe, respectivamente.

Estos están definidos por el usuario, pero deben coincidir con los nombres de archivo en el documento versions.xml.

8 Reinicie el servidor de seguridad para que los cambios surtan efecto.

Configuración de EE Server para descargas automáticas del cliente Data Guardian (opcional)

Para las descargas automáticas, el archivo versions.xml y los elementos binarios deben estar en la misma ubicación. La ubicación debe ser accesible para el cliente, por lo que podría ser IIS o podría utilizar la carpeta **Servidor de seguridad\Descarga\cloudweb** que ha creado. En caso de que se utilice la carpeta cloudweb, a continuación se presenta un ejemplo de cómo configurar el servidor.

1 Vaya a la carpeta **Servidor de seguridad\Descarga\cloudweb**. (Consulte el paso 6 en Configuración del servidor de seguridad para permitir las descargas del cliente Data Guardian.)

2 Cree una carpeta con el nombre DataGuardianUpdate.

> **NOTA:**
> DataGuardianUpdate es solo un ejemplo; puede elegir el nombre que desee.

3 Coloque los ejecutables actualizados en la carpeta DataGuardianUpdate.

4 Cree un archivo *versions.xml* en la carpeta DataGuardianUpdate.

5 Abra el archivo *versions.xml* con un editor de texto y compruebe que la ruta de acceso del nombre del archivo es la correcta para su entorno.

Ejemplo:

```
<?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>
```

Versión: indica la versión del archivo de los ejecutables actualizados

Nombre de archivo setup.exe: el usuario define el nombre de configuración de los archivos ejecutables, pero este debe coincidir con el nombre de configuración del archivo messages.properties. (Consulte el paso 3 en Configuración del servidor de seguridad para permitir las descargas del cliente Data Guardian.)

6 Guarde y cierre el archivo.

7 Agregue los archivos binarios a esta carpeta.

8 Si utiliza IIS, reinicie IIS.

9 Como administrador de Dell, inicie sesión en la Remote Management Console.

10 En el panel izquierdo, haga clic en **Poblaciones** > **Empresa**; se mostrará la pestaña Políticas de seguridad.

11 En el grupo de tecnología Data Guardian, haga clic en **Cifrado en la nube**.

12 Haga clic en **Mostrar la configuración avanzada**.

13 Desplácese hasta la política *URL del servidor de actualización de software* e introduzca **https://<YOUR HOST URL> / DataGuardianUpdate**.

> **NOTA:**
> DataGuardianUpdate es solo un ejemplo que se utiliza para que coincida con la información proporcionada anteriormente.

14 Haga clic en **Guardar** para guardar la modificación de la política en la cola para confirmar.

15 Haga clic en **Administración** > **Confirmar**.

16 Escriba un comentario y haga clic en **Confirmar políticas**.

Administrar perfiles de proveedor de protección de almacenamiento en la nube

Data Guardian cifra los archivos del usuario y envía eventos de auditoría al EE Server/VE Server. Para cambiar el comportamiento de cada proveedor admitido de almacenamiento en la nube, establezca cada proveedor con uno de estos valores:

Valor	Descripción
Proteger	Permitir al proveedor/conexión, cifrar los archivos y enviar eventos de auditoría acerca de la actividad del archivo/carpeta.
Bloquear	Bloquear todo el acceso al proveedor/conexión.
Permitir	Permitir al proveedor/conexión que pase sin cifrado, pero con auditoría de la actividad del archivo/carpeta.
Omitir	Omitir la protección del proveedor/conexión sin cifrado o auditoría. Cuando se establece este valor, no se muestra la carpeta del proveedor de almacenamiento en la nube en la unidad virtual Data Guardian del equipo cliente.

Para obtener más información, consulte *AdminHelp*, al que puede acceder desde la Remote Management Console.

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

Determine qué usuarios externos podrán registrarse en EE Server/VE Server para utilizar Data Guardian. Para mantener la seguridad adecuada, asegúrese de configurar y administrar con cuidado estas listas.

- Un usuario interno se encuentra dentro del dominio.
- Un usuario externo es un usuario que no pertenece al dominio, se trata bien de una persona de otra organización con la que un usuario interno desea compartir documentos empresariales confidenciales o de un usuario interno que quiere acceder a su equipo desde un dispositivo fuera del dominio.

Si desea permitir que un usuario que no pertenece al dominio de la organización se registre para utilizar Data Guardian:

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 un 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 de Dell.

Recreación de la imagen de un equipo con Data Guardian

Si es necesario recrear la imagen del equipo de un usuario remoto y este dispone de Dell Data Guardian, pregunte si el usuario ha trabajado sin conexión y creado algún documento de Office protegido en ese tiempo. Si es así, las claves sin conexión que se han generado para esos documentos y esas claves no están custodiadas en el servidor de Dell.

1 Para obtener más información acerca de cómo recuperar las claves de Data Guardian generadas sin conexión y no custodiadas en el servidor de Dell, consulte la *Recovery Guide* (Guía de recuperación).

2 Busque una carpeta de claves sin conexión antes de volver a crear la imagen del equipo del usuario.

Cuando se crean las primeras claves de custodia, se añade una carpeta de Data Guardian a **C:\Program Files\Dell\Dell Data Protection**. Acceda a la carpeta **Data Guardian > Claves sin conexión**. Si no hay ninguna carpeta de claves sin conexión, compruebe la carpeta **Mis documentos** del usuario.

5

Instalación de Data Guardian

Existen dos métodos para realizar la instalación de Data Guardian:

- Instalación de Data Guardian de forma interactiva
- Instalación de Data Guardian con la línea de comandos

Los usuarios de Data Guardian deben realizar las tareas siguientes para que los archivos y las carpetas de sus clientes de sincronización en la nube estén protegidos. Una vez finalizada la instalación del cliente Data Guardian, los usuarios deben descargar un proveedor de almacenamiento en la nube:

- El administrador debe especificar el proveedor de sincronización en la nube que se va a utilizar.

  O bien

- Proporcionar a los usuarios un vínculo para descargar e instalar Dropbox for Business o OneDrive para la Empresa/Unified OneDrive si su empresa utiliza alguno de estos proveedores. Recuerde que los usuarios de Dropbox for Business deben conectarse a Dropbox for Business a través de Data Guardian.

Carpetas preexistentes con archivos sin cifrar

Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configurada una cuenta de almacenamiento en nube.

Si la cuenta de un proveedor de almacenamiento en la nube está configurada con carpetas sincronizadas con el equipo local antes de la instalación de Data Guardian:

- Los archivos y carpetas preexistentes que se hayan sincronizado en la nube se mantendrán como texto no cifrado.
- Los archivos que agregue a estas carpetas preexistentes se mantendrán como texto no cifrado.
- Los archivos que se sincronicen desde la nube, se cifrarán.

  Si desea cifrar los archivos preexistentes, acceda a la Unidad virtual DDG VDisk (creada durante la instalación de Data Guardian), cree una nueva subcarpeta en el cliente de sincronización en la nube y mueva los archivos preexistentes a dicha carpeta.

Instalación de Data Guardian

Debe ser un administrador local en el equipo para instalar Data Guardian.

El equipo debe tener una letra alfabética disponible para asignarla a una unidad de disco.

Después de instalar Data Guardian, esté preparado para reiniciar el equipo.

1. Para descargar el instalador Data Guardian, vaya a la ubicación especificada por su administrador.
2. En función de su sistema operativo, seleccione el instalador de 32 o 64 bits, normalmente **setup32.exe** o **setup64.exe**, y cópielo en el equipo local.
3. Haga doble clic en el archivo para iniciar el instalador.
4. Si se muestra un aviso de seguridad, haga clic en **Ejecutar**.
5. Seleccione un idioma y haga clic en **Aceptar**.
6. Si se le solicita que instale el paquete redistribuible Microsoft Visual C++ 2015 o el perfil de cliente Microsoft .Net Framework 4.0, haga clic en **Aceptar**.

7 En la ventana de Bienvenida, haga clic en **Siguiente**.

8 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.

9 En la pantalla de la carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\.

En C:\, no instale Data Guardian en carpetas de usuarios o Windows, ni en la raíz de ninguna unidad. Se mostrará un error.

10 En el campo *Nombre del servidor:*, introduzca el nombre del servidor con el que se comunicará este equipo, como, por ejemplo, server.domain.com. No es necesario incluir www o http(s). Esta información se la proporciona el administrador.

No desmarque la casilla *Activar verificación de SSL Trust* a menos que se lo indique el administrador.

11 Haga clic en **Siguiente**.

12 En la pantalla Confirmar información del servidor de activación, confirme si la dirección URL del servidor es correcta. El instalador añade www o http(s) y el puerto. Haga clic en **Siguiente**.

13 En la ventana Tipo de administración, seleccione esta opción:

- Uso interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.

14 Haga clic en **Instalar** para comenzar la instalación.

Se mostrará una ventana de estado que muestra el progreso de la instalación.

15 Cuando se muestre la pantalla Instalación completa, haga clic en **Finalizar**.

16 Haga clic en **Sí** para reiniciar.

Se ha completado la instalación de Data Guardian.

17 El icono de la bandeja del sistema Data Guardian muestra una marca de verificación verde  después de la activación. En función de la manera en que se implemente Data Guardian dentro de la empresa, puede que la activación no sea inmediata.

Instalación de Data Guardian con la línea de comandos

- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio en la línea de comandos, en comillas de escape.
- La siguiente tabla indica los modificadores disponibles para la instalación.

Modificador	Significado
/V	Envía las variables al archivo .msi en setup.exe. El contenido siempre debe introducirse entre comillas de texto sin formato.
/s	Modo silencioso

Opción	Significado
/QB	Diálogo de progreso con botón **Cancelar** , indica que es necesario reiniciar
/QB!	Diálogo de progreso sin botón **Cancelar**, indica que es necesario reiniciar
/QN	Sin interfaz de usuario

- La tabla a continuación indica los parámetros disponibles para la instalación.

Parámetros
SERVIDOR=<ServerName> (FQDN del servidor Dell para la activación)
EMPRESA=1 (usuario interno)
ACTIVARSSLTRUST=0 (Desactivar la validación de SSL Trust)
REINICIAR=SUPRIMIR (El valor nulo permite la configuración automática, SUPRIMIR desactiva el reinicio)

Ejemplo de línea de comandos

- El siguiente ejemplo instala Data Guardian de forma silenciosa, para un usuario interno, en C:\Biblioteca\Registros\Install.log.

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

Uso de Data Guardian con Dropbox for Business

Data Guardian con Dropbox for Business ofrece funciones adicionales a las de Dropbox básico.

- Eliminación remota de la cuenta de un miembro del equipo
- Puede establecer políticas para controlar cómo se protegen las carpetas de Dropbox empresariales y personales. Si su empresa permite las cuentas de empresa y personales, los usuarios finales deben comprender cómo funciona el cifrado de cada tipo de cuenta. Consulte Política para cuentas de empresa personales.

Política de cuentas de empresa y personales

En su empresa pueden aplicarse pautas sobre si los miembros del equipo pueden utilizar cuentas de empresa y personales. Además, la empresa puede permitir que solo determinados usuarios tengan cuentas de empresa y personales.

NOTA:
Si su empresa permite las cuentas de empresa y personales, y un usuario final elige utilizar ambas, debe entender la administración de carpetas de ambos tipos de cuentas.

La siguiente tabla describe el cifrado basado en la configuración de la política *Carpetas personales de cifrado de Dropbox*.

Cifrado	Configuración de política	Consideraciones sobre la implementación
Cifre todos los archivos y carpetas de empresa y personales.	Política > Carpetas personales de cifrado de Dropbox > Establecida en **Seleccionada** (predeterminado)	Antes de implementar Data Guardian, los usuarios deben realizar una copia de seguridad de los archivos empresariales preexistentes en las carpetas de sincronización de almacenamiento en la nube, en ubicaciones situadas fuera de las carpetas sincronizadas. Los usuarios con archivos personales que deben permanecer sin cifrar deben mover esos archivos fuera de las carpetas sincronizadas de empresa o desvincular las cuentas personales de los clientes de sincronización de la empresa. Después de que se haya implementado Data Guardian, los archivos y las carpetas en la nube solo podrán visualizarse en equipos o dispositivos que ejecuten Data Guardian. Si una carpeta personal se cifra accidentalmente, consulte "Decrypting Folders in a Personal Account" (Descifrar carpetas en una cuenta personal) en la Dell Data Guardian User Guide (Guía del usuario de Dell Data Guardian).
Cifre todos los archivos y las carpetas de la cuenta de empresa.	Política > Carpetas personales de cifrado de Dropbox > Establecida en **Sin seleccionar**	Puede utilizar la política opcional Mensaje para cifrar carpetas personales en Dropbox para mostrar un mensaje personalizado que recuerde a los usuarios que **no** guarden

Cifrado	Configuración de política	Consideraciones sobre la implementación
Permita que los archivos y las carpetas de la cuenta personal permanezcan sin cifrar.		archivos de la empresa en cuentas personales, porque esos archivos no estarán protegidos. El mensaje se mostrará en estos momentos. • Cada vez que el usuario inicie la sesión • Cuando el usuario cree o agregue un nuevo archivo o carpeta a una cuenta personal de Dropbox Si establece la política Cifrar carpetas personales en Dropbox en **Falso** para un extremo o grupo de extremos, las cuentas personales de todos los usuarios en esos extremos seguirán sin estar cifradas.

Carpetas personales y de empresa

Si su empresa utiliza Dropbox for Business y permite que los usuarios finales tengan carpetas personales y de empresa, quizá desee ejecutar informes para asegurar que todos los archivos de la empresa tengan la extensión .xen, por si acaso el usuario final copia un archivo confidencial desprotegido en una carpeta de empresa. Consulte Solución de problemas de Data Guardian.

Eliminación remota de la cuenta 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

- Antes de realizar una eliminación remota, deberá hacer una copia de seguridad de los archivos o 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.
- Data Guardian debe haberse activado y el usuario final debe estar conectado a Dropbox for Business.

Registrarse en la Remote Management Console

Solo tiene que registrarse un administrador de Dropbox for Business.

1. En la Remote Management Console, seleccione **Administración de Dropbox** en el panel izquierdo.
2. 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. Haga clic en **Permitir** para permitir el acceso a Data Guardian. Se mostrará una página de confirmación que indica que se otorga la autorización de Dropbox a VE Server.
5. En la Remote Management Console, regrese a **Administración de Dropbox** y actualice la página. 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 para eliminar miembros del equipo de Dropbox for Business, haga clic en **Anular registro**.

Eliminación remota de la cuenta de un miembro del equipo

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 Haga clic en la pestaña **Detalles y acciones**.
4 En la columna Comando, haga clic en **Eliminación remota**.

> **NOTA:**
> Deberá realizar una copia de seguridad de los archivos o carpetas de la cuenta del miembro del equipo que la empresa u otros miembros del equipo en Dropbox for Business puedan necesitar antes de eliminar remotamente la cuenta.

5 Haga clic en **Sí** en la confirmación de Eliminación remota. En la página Detalles del usuario se indica la fecha en la que se realizó la eliminación remota.
6 Actualice la lista de Miembros del equipo en la página de miembros de la consola del administrador de Dropbox for Business. El usuario se quita de la lista. Puede seleccionar la pestaña **Miembros quitados** para ver los usuarios que se han quitado.

Visualización de informes

La información sobre el entorno de Data Guardianse encuentra disponible en la Remote Management Console del servidor Dell. Seleccione **Informes > Eventos de auditoría** para los eventos de auditoría relacionados con las carpetas de cliente de sincronización en la nube y los documentos de Office protegidos.

Para obtener más información, consulte *AdminHelp*, al que puede acceder desde la Remote Management Console.

Solución de problemas de Data Guardian

Utilizar la pantalla Detalles

Puede utilizar la pantalla **Detalles** para resolver problemas. Por ejemplo:

- Si un usuario crea una carpeta pero no se está realizando el cifrado, seleccione **Detalles** > **Archivos** > **Estado de la carpeta** para comprobar el estado.
- Si un usuario final solicita soporte, puede indicarle que configure la pantalla Detalles mejorados y seleccione la pestaña **Detalles** > **Política**. En dicha pestaña aparecen las políticas que se están ejecutando.
- Para solucionar problemas, examine los registros .

Utilizar la pantalla Detalles mejorados

- Mientras mantiene pulsado **<Ctrl><Shift>**, haga clic en el icono de la bandeja del sistema Data Guardian y, a continuación, seleccione **Detalles**.
- Además de los archivos y las carpetas, se muestra lo siguiente:

  Seguridad: muestra la clave, el tipo de clave y el estado. Este panel ofrece una lista temporal de algunos de los archivos de Office protegidos hasta que se envían al servidor. La longitud de tiempo depende del intervalo de sondeo.

  Auditoría: enumera los módulos, el ID de usuario y el tipo de evento. En este registro de auditoría la información se encuentra en cola y, a continuación, será enviada al EE Server/VE Server a intervalos específicos. El administrador puede ver los **Eventos de auditoría** en el panel izquierdo de la Remote Management Console para la auditoría.

  Política: enumera los nombres y valores de la política.

Ver archivos de registro

- Haga clic en **Ver Registro** de la esquina inferior izquierda de la pantalla Detalles.

  Los archivos de registro también se pueden consultar en **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian**.

  Los archivos de registro de documentos de Office protegidos se encuentran en la carpeta Custom.xml.

Solución de problemas de activación automática

Si Data Guardian no se activa automáticamente para varios usuarios, puede cambiar la configuración de registro del cliente Data Guardian. También debe comprobar los alias en el servidor de Dell:

1. En la Remote Management Console, vaya a **Poblaciones > Dominios**, y seleccione un dominio y sus subdominios.
2. En la página Detalles del dominio, seleccione la pestaña **Configuración**.
3. En el campo *Alias*, confirme que todos los alias son correctos.

Proporcionar derechos temporales de administración de carpetas

Puede conceder derechos temporales para administrar carpetas a un administrador o usuario. Por ejemplo, si los usuarios cargaron los archivos a la nube antes de la instalación de Data Guardian, puede proporcionar derechos de administración de la carpeta temporales a algunos usuarios para que administren el cifrado carpeta a carpeta en las carpetas del cliente de sincronización.

Para proporcionar derechos de administración de carpetas:

1 En la Remote Management Console, haga clic en **Poblaciones** > **Extremos**.

2 Busque o haga clic en un extremo y, a continuación, haga clic en la ficha **Políticas de seguridad**.

3 Seleccione **Cifrado en la nube** y luego haga clic en **Mostrar configuración avanzada**.

4 Haga clic en la casilla situada junto a *Administración de carpetas habilitada* para seleccionar la política.

5 Haga clic en **Guardar**.

6 En el panel izquierdo, haga clic en **Administración** > **Confirmar**.

7 Escriba un comentario y haga clic en **Confirmar políticas**.

NOTA:
Dell recomienda que después de cifrar las carpetas o completar la solución de problemas, deje en blanco la casilla de la política *Administración de carpetas habilitada* para desactivar la política en ese extremo.

Para administrar carpetas en el extremo:

1 Cree una carpeta dentro de la carpeta del cliente de sincronización y agregue archivos, de modo que los archivos queden cifrados en la nube.

2 Haga clic en el icono de la bandeja del sistema Data Guardian y seleccione **Administrar carpetas**.

Para cada cliente de sincronización, se muestra una vista jerárquica de las carpetas sincronizadas en la nube. Todas las carpetas se encuentran seleccionadas de manera predeterminada. Desmarque las carpetas que no desea cifrar. Si anula la selección de una carpeta en Administrar carpetas, un barrido de descifrado descifrará los archivos existentes en esa carpeta. Los nuevos archivos de esa carpeta no estarán cifrados en la unidad local o en la nube.

NOTA:
Si arrastra un archivo cifrado a una carpeta que no se encuentra seleccionada en Administrar carpetas, bien en la nube, bien en la unidad virtual DDP|SL, el archivo permanecerán cifrado y no podrá visualizar el contenido. Además, si comparte la carpeta con otro usuario de Data Guardian que no tenga la política Administrar carpetas habilitada, los archivos se mantendrán cifrados para él y no podrá visualizarlos.

3 Si desea cifrar una carpeta ya existente, active el cifrado para esa carpeta manualmente. Los archivos se cifrarán cuando se sincronicen en la nube.

Preguntas más frecuentes

Preguntas más frecuentes de administración de carpetas

Pregunta

Tengo una carpeta con archivos que he compartido con otro usuario. En la bandeja del sistema, he utilizado la utilidad **Data Guardian > Administrar carpetas** para desproteger el contenido de esa carpeta. Recientemente, mis archivos vuelven a estar cifrados en la nube. Esa carpeta ya no se muestra en la utilidad Administrar carpetas, por lo que ya no puedo descifrar esos archivos en la nube.

Respuesta

Una Id. de clave de cifrado está asociado con una carpeta basada en el primer usuario que agregó un archivo en esa carpeta. Si un usuario crea una carpeta y no agrega archivos, su clave no se asocia a esa carpeta. El usuario cuya Id. de clave de cifrado se ha definido en la carpeta es el único que puede ver la carpeta en la utilidad Administrar carpetas. Si el usuario con ID de clave de cifrado asociado a la carpeta la desmarca en la utilidad Administrar carpetas y la comparte con otro usuario de Data Guardian, el segundo usuario de Data Guardian volverá a cifrar el contenido.

Solución

1 Cree una nueva carpeta.

2 Mueva todos los archivos que desee cifrar a la nueva carpeta.

3 En la bandeja del sistema, use la utilidad **Dell Data Guardian** > **Administrar carpetas** para descifrar esos archivos.

NOTA:
Si descifra el contenido de una carpeta que se comparte con otros usuarios de Data Guardian, el cliente Data Guardian forzará la ejecución de la política para cifrarlos. La práctica recomendada es utilizar la utilidad Administrar carpetas para descifrar solo los archivos que no se comparten con otros usuarios de Data Guardian.

Pregunta

Estoy sincronizando una carpeta descifrada que he desmarcado con la utilidad Administrar carpetas. Sin embargo, cuando intento cargarla mediante el navegador web, solo puedo cargar archivos cifrados.

Respuesta

Data Guardian no se ha diseñado para buscar activamente carpetas en la nube. En el caso de carpetas sin cifrar, Data Guardian puede sincronizarse mediante el cliente de sincronización porque controla el entorno. Es necesario que los archivos que se envían a través del explorador web estén protegidos.

Solución

Agregue archivos a la carpeta de sincronización.

Pregunta

Recientemente desinstalé mi sistema de archivos compartidos basado en la nube desde mi equipo, pero cuando abrí la utilidad Administrar carpetas, uno de los clientes de sincronización todavía estaba incluido como una opción.

Respuesta

Data Guardian no supervisa la instalación o desinstalación del software de terceros. Esas opciones siguen en la lista porque, por diseño, cuando se desinstalan estos clientes, no quitan los archivos existentes. Esos archivos siguen estando protegidos por Data Guardian, a pesar de que el cliente de sincronización ya no está instalado.

Solución

Para eliminar la opción del cliente de sincronización desinstalado de la utilidad Administrar carpetas, mueva las carpetas o los archivos que desea conservar fuera de la carpeta de sincronización, y, a continuación, elimine la carpeta. Después de eliminar la carpeta, esta ya no estará incluida en la utilidad Administración de carpetas.

Otras preguntas más frecuentes

Pregunta

Un usuario dispone de Data Guardian con Documentos de Office protegidos y no puede copiar o pegar.

Respuesta

Para Data Guardian, algunas funciones se controlan desde la bandeja del sistema. Compruebe si el usuario ha modificado la bandeja del sistema.

Solución

Debe utilizarse la configuración predeterminada de la bandeja del sistema. El usuario debe conservar la configuración predeterminada de la bandeja del sistema.

Pregunta

Cambié la política **Ofuscación de nombres de archivos** de GUID a Solo Extensión. Sin embargo, las carpetas que había sincronizado anteriormente siguen cifrando esos archivos en el formato previo, con nombres de archivos GUID. ¿Por qué?

Respuesta

Cuando se cambia una política en el EE Server/VE Server, Data Guardian mantiene la política anterior de esa carpeta. Todas las carpetas nuevas tendrán la nueva política aplicada y se cifrarán en el formato **Solo extensión**.

Solución

Para volver a aplicar el formato **Solo extensión** a los archivos previos, cópielos y péguelos en una nueva carpeta a la que se le haya aplicado la nueva política.

8

Glosario

Advanced Authentication: el producto Advanced Authentication ofrece opciones de lectura de huellas digitales, tarjetas inteligentes y tarjetas inteligentes sin contacto. Advanced Authentication ayuda a administrar estos diversos métodos de autenticación, admite inicio de sesión con unidades de cifrado automático, SSO, y administra credenciales de usuario y contraseñas. Además, Advanced Authentication se puede utilizar para acceder no solo a PC sino también a sitios web, SaaS, o aplicaciones. Una vez los usuarios registran sus credenciales, Advanced Authentication permite el uso de dichas credenciales para iniciar sesión en el dispositivo y para realizar sustitución de contraseñas.

BitLocker Manager: Windows BitLocker está diseñado para ayudar a proteger los equipos Windows mediante el cifrado de datos y archivos de sistema operativo. Para mejorar la seguridad de las implementaciones de BitLocker y simplificar y reducir el costo de propiedad, Dell ofrece una única consola de administración central que soluciona muchos problemas de seguridad y ofrece un enfoque integrado para administrar el cifrado en otras plataformas no BitLocker, ya sean físicas, virtuales o basadas en nube. BitLocker Manager admite cifrado de BitLocker para sistemas operativos, unidades fijas y BitLocker To Go. BitLocker Manager le permite integrar perfectamente BitLocker en sus necesidades de cifrado existentes y administrar BitLocker con el mínimo esfuerzo a la vez que perfecciona la seguridad y la conformidad. BitLocker Manager ofrece administración integrada para recuperación de claves, administración de políticas y cumplimiento, administración automatizada de TPM, conformidad de FIPS e informes de conformidad.

Desactivar: la desactivación se produce cuando se desactiva SED Management en la Remote Management Console. Una vez que el equipo ha sido desactivado, la base de datos de PBA se elimina y ya no figura un registro de usuarios en la memoria caché.

EMS, External Media Shield: este servicio incluido en el cliente Dell Encryption aplica políticas a los medios extraíbles y los dispositivos de almacenamiento externos.

Código de acceso EMS: este servicio incluido en Dell Enterprise Server/VE permite la recuperación de dispositivos External Media Shield protegidos cuando el usuario ha olvidado su contraseña y ya no puede iniciar sesión. La finalización de este proceso permite al usuario restablecer la contraseña configurada en el soporte extraíble o dispositivo de almacenamiento externo.

Cliente Encryption: el cliente Encryption es el componente en dispositivo que aplica las políticas de seguridad, independientemente de que un extremo esté conectado a la red, desconectado de la red, perdido o robado. Creando un entorno informático de confianza para extremos, el cliente Encryption funciona como capa sobre el sistema operativo del dispositivo, y ofrece autenticación, cifrado y autorización aplicados de forma coherente para maximizar la protección de información confidencial.

Extremo: un equipo o dispositivo de hardware móvil administrado por Dell Enterprise Server/VE.

Barrido de cifrado: un barrido de cifrado es el proceso de explorar las carpetas que se van a cifrar en un extremo administrado para garantizar que los archivos que contiene estén en el estado de cifrado correcto. Las operaciones de creación de archivo ordinaria y cambio de nombre no desencadenan un barrido de cifrado. Es importante entender cuándo se puede producir un barrido de cifrado y cómo pueden afectar los tiempos de barrido resultantes, de la siguiente forma: se producirá un barrido de cifrado durante el recibo inicial de una política que tenga habilitado el cifrado. Esto puede ocurrir inmediatamente después de la activación si la política tiene habilitado el cifrado. - Si la política Explorar estación de trabajo o Inicio de sesión están habilitadas, las carpetas especificadas para cifrado se barrerán en cada inicio de sesión del usuario. - Se puede volver a desencadenar un barrido con determinados cambios de política posteriores. Cualquier cambio de política relacionado con la definición de las carpetas de cifrado, los algoritmos de cifrado o el uso de claves de cifrado (común frente a usuario), activará un barrido. Además, cambiar entre cifrado habilitado y deshabilitado desencadenará un barrido de cifrado.

Contraseña de un solo uso (OTP): una Contraseña de un solo uso es una contraseña que se puede utilizar solamente una vez y es válida durante un periodo de tiempo limitado. OTP requiere que haya un TMP presente, habilitado y con propietario. Para habilitar OTP, se asocia un dispositivo móvil con el equipo mediante la Security Console y la aplicación Security Tools Mobile. La aplicación Security Tools Mobile genera la contraseña en el dispositivo móvil que se utiliza para iniciar sesión en el equipo en la pantalla de inicio de sesión de Windows. En función de la política, es posible que la función OTP se utilice para recuperar el acceso al equipo si la contraseña ha caducado o se ha

olvidado, si la OTP no ha sido utilizada para iniciar sesión en el equipo. La función OTP se puede utilizar para la autenticación o la recuperación, pero no para ambas cosas. La seguridad OTP supera la de otros métodos de autenticación ya que la contraseña generada se puede utilizar una sola vez y se vence en un periodo corto de tiempo.

SED Management: SED Management ofrece una plataforma para administrar de forma segura unidades de cifrado automático. A pesar de que las SED proporcionan su propio cifrado, no cuentan con una plataforma para administrar el cifrado y las políticas disponibles. SED Management es un componente de administración central y escalable que le permite proteger y administrar, de forma más efectiva, sus datos. SED Management garantiza que podrá administrar su empresa de forma más rápida y fácil.