Dell Data Protection | Personal Edition

Guía de instalación v8.13

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.

Guía de instalación de Personal Edition

2017 - 04

Rev. A01

Tabla de contenido

Descripción general de Personal Edition

Esta guía asume que Security Tools se instalará con Personal Edition.

Personal Edition

El objetivo de Personal Edition es proteger los datos de su equipo, incluso si el equipo se pierde o roba.

Para garantizar la seguridad de sus datos confidenciales, Personal Edition cifra los datos en su equipo de Windows. Siempre puede acceder a los datos cuando haya iniciado sesión en el equipo, pero los usuarios no autorizados no tendrán acceso a estos datos protegidos. Los datos siempre estarán cifrados en la unidad, pero debido a que el cifrado es transparente, no es necesario cambiar la forma en la que trabaja con las aplicaciones y los datos.

Normalmente, el cliente Encryption descifra los datos mientras trabaja con ellos. En ocasiones, es posible que una aplicación intente acceder a un archivo a la vez que el cliente Encryption está cifrándolo o descifrándolo. Si esto ocurre, después de un segundo o dos, el cliente Encryption muestra un cuadro de diálogo que le da la opción de esperar o cancelar el cifrado/descifrado. Si decide esperar, el cliente Encryption libera el archivo tan pronto como termine (usualmente en unos segundos).

Security Tools

El propósito de Security Tools es ofrecer una solución integral diseñada para proporcionar soporte de Advanced Authentication.

Security Tools ofrece soportemultifactor para la autenticación de Windows mediante contraseñas, lectores de huellas digitales y tarjetas inteligentes, tanto de contacto como sin contacto, así como a través del registro automático, Contraseñas de un solo uso (OTP) e Inicio de sesión en un solo paso (Inicio de sesión único [SSO]).

La Security Console es la interfaz de Security Tools que guía a los usuarios en la configuración de sus credenciales y preguntas de recuperación automática, en función de la política definida por el administrador local.

La herramienta Configuración de administrador está disponible para los usuarios que tienen privilegios de administrador, y se utiliza para establecer las políticas de autenticación y las opciones de recuperación, administrar los usuarios y definir la configuración avanzada, así como la configuración específica de las credenciales admitidas en el inicio de sesión de Windows.

Consulte Configuración de los valores de administrador de Security Tools y consulte *Dell Console User Guide (Guía del usuario de la consola de Dell)* para aprender a utilizar las aplicaciones de Security Tools.

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 de Personal Edition

Estos requisitos detallan todo lo que es necesario para la instalación de Personal Edition.

Cliente Encryption

- Personal Edition requiere una autorización para instalarse correctamente. Esta autorización se ofrece al comprar Personal Edition. Según cómo haya comprado Personal Edition, es posible que tenga que instalar manualmente la autorización. De ser así, siga estas sencillas instrucciones que acompañan la autorización. Si Personal Edition se ha instalado utilizando el servicio Dell Digital Delivery, dicho servicio se encarga de la instalación de la autorización. (Se utilizan los mismos binarios para Enterprise Edition y Personal Edition). La autorización indica al instalador qué versión deberá instalar).
- Dell recomienda que se utilice una contraseña de Windows, si es que no cuenta ya con una, para proteger el acceso a la información cifrada. La creación de una contraseña en su equipo evita que otras personas puedan iniciar sesiones en su cuenta de usuario sin su contraseña.
  a Vaya al Panel de control de Windows (**Inicio** > **Panel de control**).
  b Haga clic en el icono **Cuentas de usuarios**.
  c Haga clic en **Crear una contraseña para su cuenta**.
  d Introduzca una nueva contraseña y su confirmación.
  e Si lo desea, escriba una pista para la contraseña.
  f Haga clic en **Crear contraseña**.
  g Reinicie el equipo.
- 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.
- Haga una copia de seguridad antes de iniciar la instalación/desinstalación/actualización.
- Durante la instalación/desinstalación/actualización, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Para reducir la duración inicial de cifrado, así como el tiempo de cifrado en la desinstalación, ejecute el Asistente de liberación de espacio en disco de Windows para eliminar los archivos temporales y otros archivos innecesarios.
- Desactive el modo de suspensión durante el barrido de cifrado inicial para evitar que un equipo que no se esté utilizando entre en suspensión. El cifrado se interrumpirá si el equipo entra en modo de suspensión (tampoco podrá realizar el descifrado).
- El cliente Encryption no es compatible con las configuraciones de inicio dual, dado que es posible cifrar archivos de sistema del otro sistema operativo, que podrían interferir con esta operación.
- El instalador maestro no es compatible con las actualizaciones de los componentes anteriores a v8.0. Extraiga los instaladores secundarios del instalador maestro y actualice los componentes individualmente. Si tiene preguntas o dudas, póngase en contacto con Dell ProSupport.
- El cliente Encryption ahora es compatible con el modo de auditoría. El modo de auditoría permite a los administradores implementar el cliente Encryption como parte de la imagen corporativa, en lugar de utilizar un SCCM de terceros o soluciones similares para implementar el cliente Encryption. Para obtener instrucciones acerca de la forma de instalar el cliente de Cifrado en una imagen corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.
- El TPM se utiliza para sellar la GPK. Por lo tanto, si ejecuta el cliente Encryption, borre el TPM en el BIOS antes de instalar un sistema operativo nuevo en el equipo cliente.
- El cliente Encryption se ha probado y es compatible con McAfee, el cliente de Symantec, Kaspersky y Malwarebytes. Se aplican exclusiones no modificables para estos proveedores de antivirus con el fin de evitar incompatibilidades entre la detección del antivirus y el cifrado. El cliente Encryption también se ha probado con el kit de herramientas Microsoft Enhanced Mitigation Experience Toolkit.

Si su empresa utiliza un proveedor antivirus que no se encuentra incluido, consulte el artículo SLN298707 de la base de conocimiento o Póngase en contacto con Dell ProSupport para obtener asistencia.

- La actualización en el lugar del sistema operativo no es compatible con la instalación del cliente Encryption. Desinstale y descifre el cliente Encryption, actualice al nuevo sistema operativo y, a continuación, vuelva a instalar el cliente Encryption.

  De manera adicional, no se admite la reinstalación del sistema operativo. Para volver a instalar el sistema operativo, realice una copia de seguridad del equipo de destino, borre el equipo, instale el sistema operativo y, a continuación, recupere los datos cifrados siguiendo los procedimientos de recuperación establecidos.
- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.

Requisitos previos del cliente Encryption

- Se necesita Microsoft .Net Framework 4.5.2 (o posterior) para los clientes de instalador maestro e instalador secundario.

  Todos los equipos enviados desde la fábrica de Dell vienen con Microsoft .Net Framework 4.5.2 (o posterior) previamente instalado. Sin embargo, si no está instalando en hardware de Dell o si está actualizando el cliente en hardware de Dell más antiguo, deberá comprobar qué versión de Microsoft .Net tiene instalada y actualizar la versión **antes de instalar el cliente**, con el fin de evitar errores durante la instalación/actualización. Para comprobar qué versión de Microsoft .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, vaya a https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- El instalador maestro instala Microsoft Visual C++ 2012 actualización 4 si todavía no está instalado en el equipo. **Cuando utiliza el instalador secundario**, debe instalar este componente antes de instalar el cliente Encryption.

Requisito previo
• Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 y x64)
• Microsoft SQL Server Compact 3.5 SP2 (x86 y x64)

Hardware del cliente Encryption

- La siguiente tabla indica el hardware del equipo compatible.

Hardware
• Los requisitos de hardware mínimos deben cumplir las especificaciones mínimas del sistema operativo.

- La siguiente tabla indica el hardware del equipo opcional compatible.

Hardware integrado opcional
• TPM 1.2 o 2.0

Sistemas operativos del cliente Encryption

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
• Windows Embedded Standard 7 con plantilla de compatibilidad de aplicaciones (no admite cifrado de hardware)
• Windows 8: Enterprise, Pro

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (no admite cifrado de hardware)
- Windows 10: Education, Enterprise, Pro
- VMWare Workstation 5.5 y superior

NOTA: El modo UEFI no es compatible con Windows 7, Windows Embedded Standard 7 ni Windows Embedded 8.1 Industry Enterprise.

Sistemas operativos para External Media Shield (EMS)

- La siguiente tabla indica los sistemas operativos compatibles con el acceso a medios protegido por EMS.

NOTA: El medio externo debe tener aproximadamente 55 MB disponibles, además de una cantidad de espacio libre en el medio igual al tamaño del archivo más grande que vaya a cifrar para alojar EMS.

NOTA:
Es compatible con Windows XP solo cuando se utiliza EMS Explorer.

Sistemas operativos Windows compatibles para el acceso a medios protegidos de EMS (32 y 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Sistemas operativos Mac compatibles para el acceso a medios protegidos de EMS (núcleos de 64 bits)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Compatibilidad de idiomas del cliente Encryption

- El cliente Encryption es una Interfaz de usuario multilingüe (MUI) que cumple los requisitos del sector y se puede configurar en los siguientes idiomas.

Compatibilidad de idiomas

- Inglés (EN)
- Español (ES)
- Francés (FR)
- Italiano (IT)
- Alemán (DE)
- Japonés (JA)
- Coreano (KO)
- Portugués brasileño (PT-BR)
- Portugués europeo (PT-PT)

Cliente Advanced Authentication

- Cuando se utiliza Advanced Authentication, los usuarios protegerán el acceso a este equipo por medio de credenciales de Advanced Authentication que son administradas y registradas mediante Security Tools. Security Tools será el administrador principal de sus

credenciales de autenticación para el inicio de sesión de Windows, lo que incluye la contraseña de Windows, las huellas digitales y las tarjetas inteligentes. Las credenciales de contraseña de imagen, PIN y huellas digitales registradas con el sistema operativo de Microsoft no se reconocerán en el inicio de sesión de Windows.

Para seguir utilizando el sistema operativo de Microsoft para administrar credenciales de usuario, no instale Security Tools o desinstálelas.

- La función de Contraseña de un solo uso (OTP) de Security Tools requiere que haya un TPM presente, habilitado y con propietario. OTP no es compatible con TPM 2.0 . Para borrar y establecer la propiedad del TPM, consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Hardware de cliente de Advanced Authentication

- La siguiente tabla detalla el hardware de autenticación compatible.

Lectores de tarjetas inteligentes y huellas digitales

- Validity VFS495 en modo seguro
- Lector magnético Dell ControlVault
- Lector UPEK TCS1 FIPS 201 Secure 1.6.3.379
- Lectores USB Authentec Eikon y Eikon To Go

Tarjetas sin contacto

- Tarjetas sin contacto con lectores compatibles sin contacto integrados en equipos portátiles específicos de Dell

Tarjetas inteligentes

- Tarjetas inteligentes PKCS n.º 11 que utilizan el cliente ActivIdentity

  NOTA: El cliente ActivIdentity no se carga previamente y debe instalarse por separado.
- Tarjetas CSP
- Tarjetas de acceso común (CAC)
- Tarjetas SIPR Net/Clase B

- Los controladores y el firmware para Dell ControlVault, los lectores de huellas digitales y las tarjetas inteligentes (como se muestra a continuación) no se incluyen en los archivos ejecutables de instaladores secundarios o en el instalador maestro . Los controladores y el firmware deben actualizarse, y pueden descargarse desde http://www.dell.com/support seleccionando su modelo de equipo. Descargue los controladores y el firmware correspondientes en función de su hardware de autenticación.

  - Dell ControlVault
  - Controlador de huellas digitales NEXT Biometrics
  - Controlador de lector de huellas digitales Validity 495
  - Controlador de tarjeta inteligente O2Micro

  Si la instalación se realiza en un hardware que no sea Dell, descargue los controladores y el firmware actualizados del sitio web del proveedor. Las instrucciones de instalación para controladores Dell ControlVault se suministran en Controladores Dell ControlVault.
- La siguiente tabla muestra qué modelos de equipos Dell admiten tarjetas SIPR Net.

Modelos de equipos Dell - Compatibilidad con la tarjeta SIPR Net/Clase B

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Sistemas operativos del cliente Advanced Authentication

Sistemas operativos Windows

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
• Windows 7 SP0-SP1: Enterprise, Professional y Ultimate • Windows 8: Enterprise, Pro • Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition • Windows 10, Education, Enterprise Pro

NOTA: El modo UEFI no es compatible con Windows 7.

Sistemas operativos de dispositivos móviles

- Los siguientes sistemas operativos para móviles son compatibles con la función de Contraseña de un solo uso de Security Tools.

Sistemas operativos Android
• 4.0 - 4.0.4 Ice Cream Sandwich • 4.1 - 4.3.1 Jelly Bean • 4.4 - 4.4.4 KitKat • 5.0 - 5.1.1 Lollipop

Sistemas operativos iOS
• iOS 7.x • iOS 8.x

Sistemas operativos Windows Phone
• Windows Phone 8.1 • Windows 10 Mobile

Compatibilidad de idiomas del cliente Advanced Authentication

- El cliente Advanced Authentication es una Interfaz de usuario multilingüe (MUI) que cumple los requisitos del sector y se puede configurar en los siguientes idiomas. El modo UEFI y la Autenticación previa al inicio (PBA) no están disponibles en ruso, chino tradicional y chino simplificado.

Compatibilidad de idiomas

- Inglés (EN)
- Francés (FR)
- Italiano (IT)
- Alemán (DE)
- Español (ES)
- Coreano (KO)
- Chino simplificado (ZH-CN)
- Chino tradicional /Taiwán (ZH-TW)
- Portugués brasileño (PT-BR)
- Portugués europeo (PT-PT)

Compatibilidad de idiomas

- Japonés (JA)
- Ruso (RU)

Continúe con Cómo obtener software.

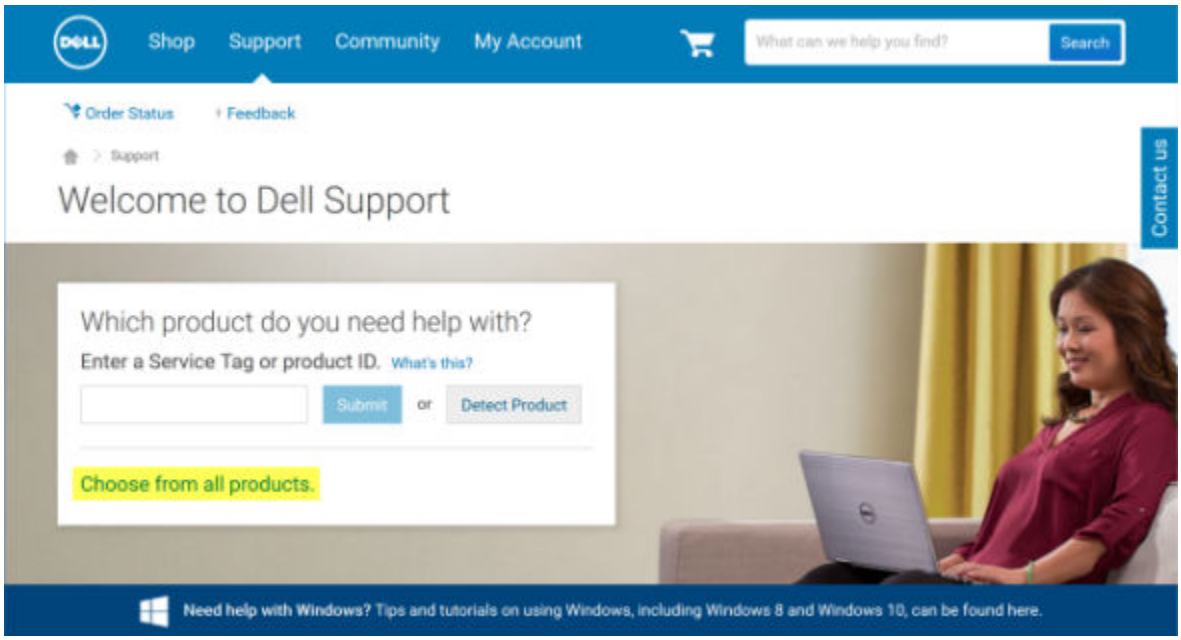
3

Descargar software

Esta sección detalla cómo obtener el software desde dell.com/support. Si ya dispone del software, puede saltarse esta sección.

Vaya a dell.com/support para empezar.

1 En la página web de asistencia de Dell, seleccione **Elegir entre todos los productos**.



2 Seleccione **Software y Seguridad** en la lista de productos.

3 Seleccione **Endpoint Security Solutions** en la sección *Software y seguridad*.
Después de realizar una vez esta selección, el sitio web la recordará.

4 Seleccione el producto de Dell Data Protection.
Ejemplos:

Dell Encryption

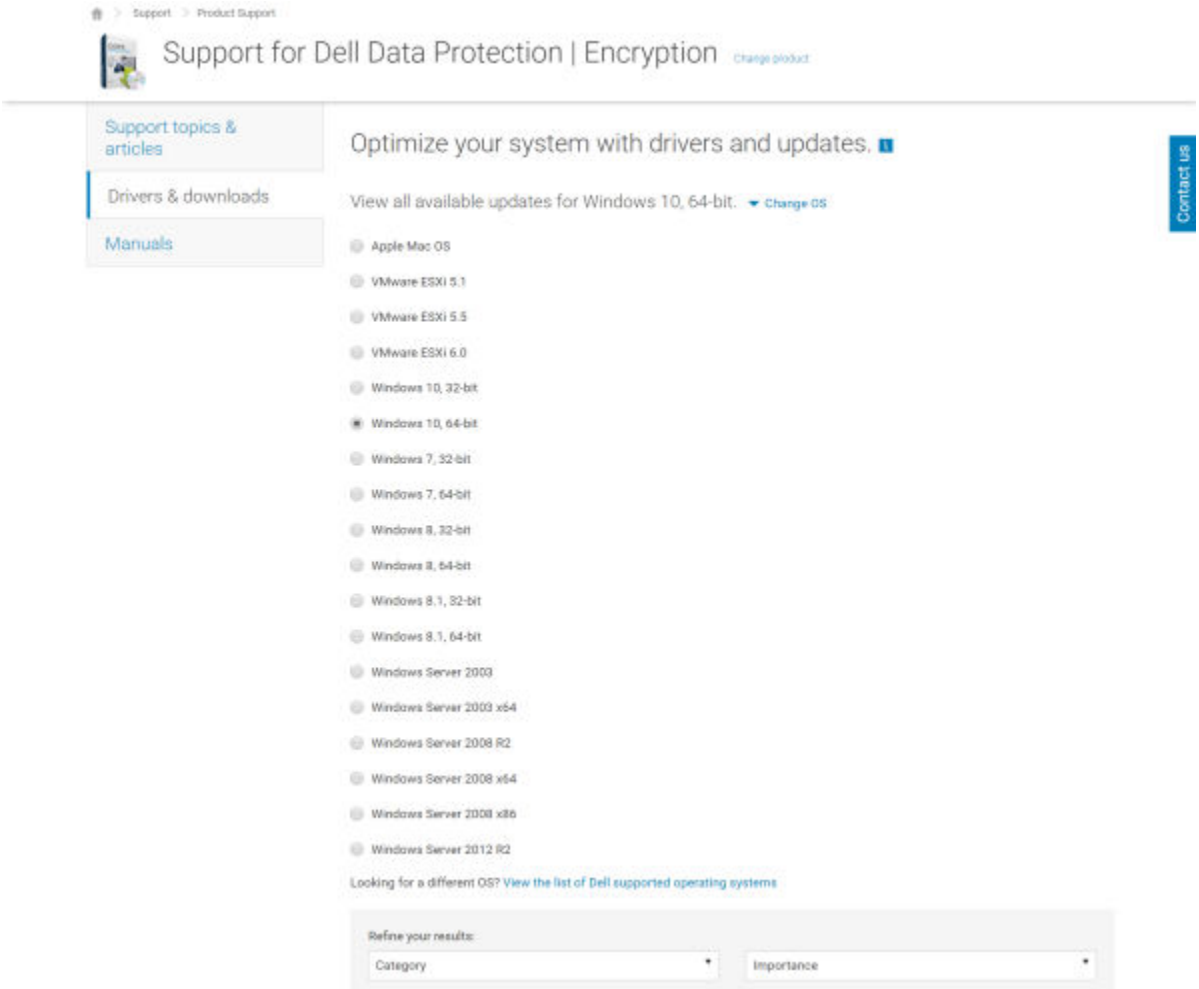
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Seleccione **Controladores y descargas**.

6 Seleccione el tipo de sistema operativo del cliente deseado.

7 Seleccione **Dell Data Protection (4 archivos)** en los resultados. Esto es solo un ejemplo, por lo que podría tener un aspecto ligeramente distinto. Por ejemplo, podría no haber 4 archivos entre los cuales escoger.



8 Seleccione **Descargar archivo** o **Agregar a mi lista de descargas #XX**.
Continúe con instalación de Personal Edition.

4

Instalación de Personal Edition

Puede instalar Personal Edition usando el instalador maestro (recomendado) o extrayendo los instaladores secundarios del instalador maestro. En cualquiera de estas dos formas, Personal Edition se puede instalar por medio de la interfaz de usuario, líneas de comandos o secuencias de comandos, y alguna tecnología push que esté disponible en su organización.

Los usuarios deberán consultar los siguientes archivos de ayuda para obtener ayuda sobre la aplicación:

- Consulte la Ayuda de cifrado de Dell para saber cómo usar la función del cliente Encryption. Acceda a la ayuda de **<Directorio de instalación>:\Archivos de programa\Dell\Dell Data Protection\Encryption\Help**.
- Consulte la Ayuda de EMS para obtener ayuda sobre las funciones de External Media Shield. Acceda a la ayuda desde **<Dir.instalación>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
- Consulte la Ayuda de Security Tools para aprender a utilizar las funciones de Advanced Authentication. Acceda a la ayuda de **<Dir.instalación>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.

Selección de un método de instalación

Hay dos métodos para instalar el cliente; seleccione **uno** de los siguientes:

- Instalación de Personal Edition mediante el instalador maestro - RECOMENDADO
- Instalación de Personal Edition mediante instaladores secundarios

Instalación de Personal Edition mediante el instalador maestro - RECOMENDADO

Para instalar Personal Edition, el instalador debe poder encontrar la autorización específica en el equipo. Si falta esa autorización, no se podrá instalar Personal Edition.

El instalador de Dell Data Protection Installer se conoce comúnmente como Instalador maestro, e instala varios clientes. En el caso de Personal Edition, se instala el cliente Encryption y el cliente Advanced Authentication.

Si instala usando la interfaz para el usuario del instalador maestro, Personal Edition se puede instalar en un equipo cada vez.

Los archivos de registro del instalador maestro están ubicados en **C:\ProgramData\Dell\Dell Data Protection\Installer.**

Seleccione un método:

Instalación mediante la Interfaz de usuario

Instalación mediante la línea de comandos

Instalación mediante la Interfaz de usuario

Instale la autorización en el equipo de destino, si fuera necesario.

Copie DDPSetup.exe al equipo local.

Haga doble clic en DDPSetup.exe para iniciar el instalador.

Se muestran diálogos que le alertan del estado de la instalación de requisitos previos. Tardará unos minutos.

Haga clic en **Siguiente** en la pantalla de bienvenida.

Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.

Haga clic en **Siguiente** para instalar Personal Edition en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\.

Security Tools se instala de forma predeterminada y no se puede anular la selección. Figura como Security Framework en el instalador.

Advanced Authentication se instala de forma predeterminada y no se puede anular la selección.

Haga clic en **Siguiente**.

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

Aparece una ventana de estado. Esta operación tarda varios minutos.

Seleccione **Sí, deseo reiniciar ahora mi equipo** y haga clic en **Finalizar**.

Una vez que se reinicia el equipo, autentíquese en Windows.

La instalación de Personal Edition + Security Tools se ha completado.

El Asistente para la instalación y la configuración de Personal Edition se incluyen por separado.

Una vez finalizados el Asistente para la instalación y la configuración de Personal Edition, inicie la Security Tools Administrator Console.

El resto de esta sección detalla otras tareas de instalación y pueden omitirse. Continúe con Asistentes para la instalación de Security Tools y Personal Edition.

Instalación mediante la línea de comandos

Instale la autorización en el equipo de destino, si fuera necesario.

Modificadores:

Si va a realizar la instalación de la línea de comandos, es necesario especificar primero los modificadores. La siguiente tabla indica los modificadores disponibles para la instalación.

Modificador	Significado
-y -gm2	Pasar datos al archivo de extracción automático
/s	Modo silencioso
/z	Pasar datos a la variable del sistema CMDLINE de InstallScript

Parámetros:

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

Parámetros
InstallPath=Ruta de acceso a una ubicación de instalación alternativa
FEATURE=PE

Ejemplo de instalación con la línea de comandos

Aunque el reinicio se ha eliminado en estos ejemplos, es posible que sea necesario reiniciar. El cifrado no puede comenzar hasta que no se reinicie el equipo.

Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio, en comillas de escape.

Las líneas de comandos distinguen entre mayúsculas y minúsculas.

En el ejemplo siguiente se instala Personal Edition y Security Tools (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

En el ejemplo siguiente se instala Personal Edition y Security Tools (instalación silenciosa, sin reinicio e instalado en la ubicación alternativa **C:\Program Files\Dell\My_New_Folder**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
```

Una vez que haya reiniciado el equipo, realice la autenticación en Windows.

La instalación de Personal Edition + Security Tools se ha completado.

El Asistente para la instalación y la configuración de Personal Edition se incluyen por separado.

Una vez finalizados el Asistente para la instalación y la configuración de Personal Edition, inicie la Security Tools Administrator Console.

El resto de esta sección detalla otras tareas de instalación y pueden omitirse. Continúe con Asistentes para la instalación de Security Tools y Personal Edition.

Instalación de Personal Edition mediante instaladores secundarios

Para instalar Personal Edition mediante los instaladores secundarios, antes hay que extraer dichos archivos ejecutables secundarios del instalador maestro. Consulte Extracción de instaladores secundarios del instalador maestro. Una vez finalizado, vuelva a esta sección.

Instalación 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.

Utilice estos instaladores para instalar los clientes mediante instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.

El reinicio se ha suprimido en los ejemplos de línea de comandos. No obstante, es posible que se requiera un reinicio. El cifrado no puede comenzar hasta que no se reinicie el equipo.

Windows crea archivos de registro de instalación de instaladores secundarios para el usuario que haya iniciado sesión en %temp%, que se encuentra en **C:\Users\<nombre de usuario>\AppData\Local\Temp.**

Si decide agregar un archivo de registro independiente cuando ejecute el instalador, asegúrese de que el archivo de registro tenga un nombre exclusivo, ya que los archivos de registro de instalador secundario no se anexan. El comando .msi estándar se puede usar para crear un archivo de registro mediante **/l*v C:\<cualquier directorio>\<cualquier nombre de archivo de registro>.log**.

Todos los instaladores secundarios utilizan los mismos modificadores y opciones de presentación de .msi básicos, salvo donde se indique, para las instalaciones de línea de comandos. Los modificadores deben especificarse primero. El modificador /v es un requisito y toma un argumento. Otros parámetros se introducen en el argumento que luego pasa al modificador /v.

Las opciones de presentación que pueden especificarse al final del argumento que se envía al modificador /v, para que su comportamiento sea el esperado. No utilice /q ni /qn en la misma línea de comandos. Utilice solamente ! y - después de /qb.

Modificador	Significado
/v	Envía las variables al archivo .msi dentro de *.exe
/s	Modo silencioso
/i	Modo de instalación

Opción	Significado
/q	Sin diálogo de progreso; se reinicia automáticamente tras completar el proceso
/qb	Diálogo de progreso con botón **Cancelar**, indica que es necesario reiniciar
/qb-	Diálogo de progreso con botón **Cancelar**, se reinicia automáticamente al terminar el proceso
/qb!	Diálogo de progreso sin botón **Cancelar**, indica que es necesario reiniciar
/qb!-	Diálogo de progreso sin botón **Cancelar**, se reinicia automáticamente al terminar el proceso
/qn	Sin interfaz de usuario

Instalación de controladores

Los controladores y el firmware para Dell ControlVault, los lectores de huellas digitales y las tarjetas inteligentes **no** se incluyen en los archivos ejecutables de instaladores secundarios o en el instalador maestro. Los controladores y el firmware deben actualizarse, y pueden descargarse desde http://www.dell.com/support seleccionando su modelo de equipo. Descargue los controladores y el firmware correspondientes en función de su hardware de autenticación.

Dell ControlVault

Controlador de huellas digitales NEXT Biometrics

Controlador de lector de huellas digitales Validity 495

Controlador de tarjeta inteligente O2Micro

Si la instalación se realiza en un hardware que no sea Dell, descargue los controladores y el firmware actualizados del sitio web del proveedor.

Luego:

Instalación de clientes Advanced Authentication

Los usuarios inician sesión en PBA mediante sus credenciales de Windows.

Busque el archivo en **C:\extracted\Security Tools** y **C:\extracted\Security Tools\Authentication.**

Ejemplo de instalación con la línea de comandos

\Security Tools

El siguiente ejemplo instala Security Framework (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"/norestart /qn"
```

:

Este cliente es necesario para Advanced Authentication en v8.x.

Luego:

\Security Tools\Autenticación

En el ejemplo siguiente se instala Security Tools (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection).

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

Luego:

Instalación del cliente Encryption

Revise los Requisitos del cliente Encryption si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, como por ejemplo, EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de certificado.

Busque el archivo en **C:\extracted\Encryption.**

Ejemplo de instalación con la línea de comandos

En el ejemplo siguiente se instalan Personal Edition y Encrypt for Sharing, se ocultan los iconos superpuestos, sin diálogos, sin barra de progreso y se omite el reinicio.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Una vez que haya reiniciado el equipo, realice la autenticación en Windows.

La instalación de Personal Edition + Security Tools se ha completado. El Asistente para la instalación y la configuración de Personal Edition se incluyen por separado.

Continúe con Asistentes para la instalación de Security Tools y Personal Edition.

Asistentes para la instalación de Security Tools y Personal Edition

Inicie sesión con su nombre de usuario y contraseña de Windows. Pasará directamente a Windows. La interfaz podría tener un aspecto distinto al que está acostumbrado.

1 UAC le podría solicitar ejecutar la aplicación. Si fuera así, haga clic en Sí.

2 Después del reinicio de la instalación inicial, aparecerá el asistente de activación de Security Tools. Haga clic en **Siguiente**.

3 Escriba y vuelva a introducir una Contraseña de administrador de cifrado (EAP) nueva. Haga clic en **Siguiente**.

4 Introduzca una ubicación de copia de seguridad en una unidad de red o un medio extraíble para almacenar información de recuperación y haga clic en **Siguiente**.

5 Haga clic en **Aplicar** para empezar la activación de ST.

6 Cuando se complete el asistente de activación de Security Tools, inicie el asistente para la configuración de Personal Edition desde el icono de DDP en la bandeja del sistema (podría iniciarse solo).

Este Asistente para la instalación le ayuda a utilizar cifrado para proteger la información en este equipo. El cifrado no podrá comenzar hasta que no se haya completado el asistente.

Lea la Pantalla de bienvenida y haga clic en **Siguiente**.

7 Seleccione una plantilla de políticas. La plantilla de políticas establece la configuración predeterminada para el cifrado.

Una vez finalizada la configuración inicial, es fácil aplicar una plantilla de políticas distinta y también personalizar la plantilla seleccionada, a través de la Local Management Console.

Haga clic en **Siguiente**.

8 Lea y confirme la advertencia de la contraseña de Windows. Si desea crear una contraseña de Windows ahora, consulte Requisitos.

9 Cree una Contraseña de administrador de cifrado (EAP) que tenga entre 9 y 32 caracteres y confírmela. La contraseña debe incluir caracteres alfabéticos, numéricos y especiales. Esta contraseña puede ser igual a la EAP que estableció para Security Tools, pero no están relacionadas. **Anote y guarde esta contraseña en un lugar seguro**. Haga clic en **Siguiente**.

10 Haga clic en **Examinar** para elegir una unidad de red o dispositivo de almacenamiento extraíble en el que hacer una copia de seguridad de sus claves de cifrado (que están recogidas en una aplicación llamada LSARecovery_[hostname].exe).

La copia de seguridad de las claves se utiliza para recuperar la información en caso de que se produzcan ciertos errores en su equipo.

Además, los posibles cambios futuros en las políticas a veces requieren que se haga una nueva copia de seguridad de las claves de cifrado. Si la unidad de red o dispositivo de de almacenamiento extraíble están disponibles, la copia de seguridad de las claves de cifrado se ejecuta como un proceso de segundo plano. Si la ubicación de destino no está disponible (por ejemplo, si el dispositivo de almacenamiento extraíble original no está insertado o conectado al equipo), los cambios en las políticas no tendrán efecto sino hasta después de que se haga una copia de seguridad manual de las claves de cifrado.

> **NOTA: Si desea obtener información sobre cómo realizar manualmente copias de seguridad de claves de acceso, haga clic en "? > Ayuda" en la esquina superior derecha de la Local Management Console o haga clic en Inicio > Todos los programas > Dell > Dell Data Protection > Encryption > Ayuda de Encryption.**

Haga clic en **Siguiente**.

11 En la pantalla de confirmación de los valores configurados se mostrará una lista de Configuración de cifrado. Revise los elementos y, cuando esté conforme con la configuración, haga clic en **Confirmar**.

Se inicia la configuración del equipo. El progreso de la configuración se indica con una barra de estado.

12 Haga clic en **Finalizar** para completar la configuración.

13 Será necesario reiniciar cuando el equipo esté configurado para el cifrado. Haga clic en **Reiniciar ahora** o posponga el reinicio 5x20 minutos cada vez.

14 Cuando se haya reiniciado el equipo, abra la Local Management Console desde el menú de Inicio para ver el estado del cifrado.

El cifrado se lleva a cabo en segundo plano. La Local Management Console puede abrirse o cerrarse. En cualquiera de los casos, proseguirá el cifrado de los archivos. Puede continuar utilizando su equipo normalmente mientras se realiza el cifrado.

15 Una vez concluida la exploración, el equipo se reiniciará una vez más.

Una vez concluidos todos los barridos de cifrado y reinicios, puede comprobar el estado de conformidad iniciando la Local Management Console. La unidad quedará etiquetada como "De conformidad".

Continúe con Configuración de los valores de administrador de Security Tools.

Configuración de los valores de administrador de Security Tools

La configuración predeterminada de Security Tools permite que los administradores y usuarios utilicen Security Tools inmediatamente después de la activación y sin necesidad de realizar ninguna configuración adicional. Los usuarios son automáticamente agregados como usuarios de Security Tools cuando inician sesión en el equipo con sus contraseñas de Windows pero, de forma predeterminada, no se habilita la autenticación multifactor de Windows.

Para configurar las funciones de Security Tools debe ser un administrador en el equipo.

Cambio de la Contraseña del administrador y de la Ubicación de las copias de seguridad

Después de la activación de Security Tools, se puede cambiar la Contraseña del administrador y la Ubicación de las copias de seguridad si es necesario.

1 Como administrador, inicie Security Tools desde el acceso directo de su escritorio.
2 Haga clic en el mosaico **Configuración de administrador**.
3 En el diálogo Autenticación, introduzca la contraseña del administrador que fue establecida durante la activación, y haga clic en **Aceptar**
4 Haga clic en la pestaña **Configuración de administrador**.
5 En la página Cambiar contraseña del administrador, si desea cambiar la contraseña, introduzca una nueva que contenga entre 8-32 caracteres e incluya al menos una letra, un número y un carácter especial.
6 Introduzca la contraseña una segunda vez para confirmarla, a continuación haga clic en **Aplicar.**
7 Para cambiar la ubicación donde se ha almacenado la clave de recuperación, en el panel izquierdo, seleccione **Cambiar ubicación de copia de seguridad**.
8 Seleccione una nueva ubicación para la copia de seguridad y haga clic en **Aplicar.**

   El archivo de copia de seguridad debe guardarse en una unidad de red o un soporte extraíble. El archivo de copia de seguridad contiene las claves necesarias para recuperar datos en este equipo. Dell ProSupport debe tener acceso a este archivo para ayudarle a recuperar los datos.

   Se realizará automáticamente una copia de seguridad de los datos de recuperación en la ubicación determinada. Si la ubicación no está disponible (por ejemplo, si no se ha insertado la unidad USB de copia de seguridad), Security Tools solicitará una ubicación para realizar la copia de seguridad de los datos. Será necesario tener acceso a los datos de recuperación para comenzar el cifrado.

Configuración de las opciones de autenticación

Los controles de la pestaña Autenticación de la configuración del administrador le permiten definir opciones de inicio de sesión para los usuarios y personalizar la configuración de cada uno de ellos.

NOTA: La opción Contraseña de un solo uso no aparece en Opciones de recuperación si el TPM no está presente, con propietario ni habilitado.

Configuración de las opciones de inicio de sesión

En la página Opciones de inicio de sesión, puede configurar las políticas de inicio de sesión. De manera predeterminada, todas las credenciales admitidas aparecen en la lista de Opciones disponibles.

Para configurar las opciones de inicio de sesión:

En el panel izquierdo, en Autenticación, seleccione **Opciones de inicio de sesión**.

Para elegir el rol que desea definir, selecciónelo en la lista **Aplicar opciones de inicio de sesión a**: **Usuarios** o **Administradores**. Todos los cambios que realice en esta página se aplicarán únicamente a la función que haya seleccionado.

Defina las Opciones disponibles para la autenticación.

De manera predeterminada, cada método de autenticación se configura para ser utilizado individualmente, no en combinación con otros métodos de autenticación. Puede cambiar los valores predeterminados de la siguiente manera:

Para especificar una combinación de opciones de autenticación, bajo Opciones disponibles haga clic en el icono para seleccionar el primer método de autenticación. En el cuadro de diálogo Opciones disponibles, seleccione el segundo método de autenticación y, a continuación, haga clic en **Aceptar**.

Por ejemplo, puede solicitar una huella digital y una contraseña como credenciales de inicio de sesión. En el cuadro de diálogo, seleccione el segundo método de autenticación que se debe utilizar con la autenticación de huella digital.

Para permitir que cada método de autenticación pueda usarse individualmente, en el cuadro de diálogo Opciones disponibles, establezca el segundo método de autenticación en **Ninguno** y haga clic en **Aceptar**.

Para eliminar una opción de inicio de sesión, en Opciones disponibles de la página Opciones de inicio de sesión, haga clic en **X** para eliminar este método.

Para agregar una nueva combinación de métodos de autenticación, haga clic en **Agregar una opción**.

Establezca las Opciones de recuperación para que los usuarios recuperen el acceso a sus equipos, en el caso de que estén bloqueados.

Para permitir que los usuarios definan un conjunto de preguntas y respuestas que puedan utilizar para recuperar el acceso al equipo, seleccione **Preguntas de recuperación**.

Para evitar que se utilicen las Preguntas de recuperación, desactive la opción.

Para permitir que los usuarios recuperen el acceso mediante un dispositivo móvil, seleccione **Contraseña de un solo uso**. Cuando se selecciona la Contraseña de un solo uso (OTP) como un método de recuperación, no estará disponible como opción de inicio de sesión en la pantalla de inicio de sesión de Windows.

Para utilizar la función OTP para el inicio de sesión, deseleccione la opción en Opciones de recuperación. Cuando se ha deseleccionado como método de recuperación, la opción OTP aparecerá en una página de inicio de Windows siempre que al menos se haya registrado un usuario en OTP.

: Como administrador, usted controla cómo utilizar la Contraseña de un solo uso, ya sea para la autenticación o para la recuperación. La función OTP se puede utilizar para la autenticación o la recuperación, pero no para ambas cosas. La configuración afectará a todos los usuarios del equipo o a todos los administradores, en función de la selección en el campo Opciones de inicio de sesión, Aplicar opciones de inicio de sesión a.

Si la opción Contraseña de un solo uso no aparece en Opciones de recuperación, la configuración de su equipo no la admitirá. Para obtener más información, consulte Requisitos.

Para solicitar al usuario que haga una llamada al soporte técnico si pierde u olvida las credenciales de inicio de sesión, borre ambas casillas de verificación en Opciones de recuperación: Preguntas de recuperación y Contraseña de un solo uso.

Para establecer un período de tiempo durante el que los usuarios puedan registrar sus credenciales de autenticación, seleccione **Período de gracia**.

La función Período de gracia le permite establecer la fecha en la que se empezará a hacer cumplir la Opción de inicio de sesión configurada. Puede configurar una Opción de inicio de sesión antes de la fecha en la que se hará cumplir y establecer un período de tiempo durante el que puedan registrarse los usuarios. De forma predeterminada, la política se hace cumplir inmediatamente.

Para cambiar la fecha en la que se hará cumplir la Opción de inicio de sesión de *Inmediatamente* a otra opción, vaya al cuadro de diálogo Período de gracia y haga clic en el menú desplegable para seleccionar **Fecha especificada**. Haga clic en la flecha abajo situada en el lateral derecho del campo de la fecha para mostrar un calendario y, a continuación, seleccione la fecha en el calendario. La aplicación de la política comienza aproximadamente a las 00:01 en la fecha seleccionada.

A los usuarios se les puede recordar que registren las credenciales que serán necesarias en su próximo inicio de sesión de Windows (de manera predeterminada), o puede especificar recordatorios periódicos. Seleccione el intervalo de aviso desde la lista desplegable *Recordar al usuario*.

:

Al activarse, el recordatorio que se muestra al usuario en la pantalla de inicio de sesión o en una sesión de Windows es ligeramente diferente. Los recordatorios no aparecen en las pantallas de inicio de sesión de Autenticación previa al inicio.

Funcionalidad durante el período de gracia

Durante un Período de gracia determinado, después de cada inicio de sesión, la notificación Credenciales adicionales se mostrará cuando el usuario aún no esté registrado con las credenciales mínimas necesarias para cumplir con la Opción de inicio de sesión que haya cambiado. El contenido del mensaje es: *Hay credenciales adicionales disponibles para registro.*

Si hay credenciales adicionales disponibles que no son necesarias, el mensaje aparece solo una vez después de modificar la política.

Hacer clic en la notificación tiene los siguientes efectos, según el contexto:

Si no se han registrado credenciales, aparecerá el asistente de Configuración, lo que permite a los Usuarios administrativos configurar los valores relacionados con el equipo, y ofrece a los usuarios la posibilidad de registrar las credenciales más comunes.

Después del registro de credenciales inicial, hacer clic en la notificación hará que se muestre el asistente de configuración dentro de la DDP Security Console.

Funcionalidad posterior al vencimiento del período de gracia

En todos los casos, una vez vencido el Período de gracia, los usuarios no podrán iniciar sesión si no han registrado las credenciales que exige la Opción de inicio de sesión. Si un usuario intenta iniciar sesión con una credencial o combinación de credenciales que no cumplan con la Opción de inicio de sesión, el asistente de Configuración aparece en la parte superior de la pantalla de inicio de sesión de Windows.

Si el usuario registra con éxito las credenciales necesarias, podrá iniciar sesión en Windows.

Si un usuario no registra correctamente las credenciales necesarias o cancela el asistente, será llevado de nuevo a la pantalla de inicio de sesión en Windows.

Para guardar la configuración de la función seleccionada, haga clic en **Aplicar**.

Configuración de la autenticación en Password Manager

En la página de Password Manager, puede configurar la manera en la que los usuarios se autentican en Password Manager.

Para configurar la autenticación en Password Manager:

En el panel izquierdo, en Autenticación, seleccione **Password Manager**.

Para elegir el rol que desea definir, selecciónelo en la lista **Aplicar opciones de inicio de sesión a**: **Usuarios** o **Administradores**. Todos los cambios que realice en esta página se aplicarán únicamente a la función que haya seleccionado.

De manera opcional, seleccione la casilla de verificación **No requerir autenticación** para dejar que el rol del usuario seleccionado inicie sesión automáticamente en todas las aplicaciones de software y sitios web de Internet con credenciales guardadas en Password Manager.

Defina las Opciones disponibles para la autenticación.

De manera predeterminada, cada método de autenticación se configura para ser utilizado individualmente, no en combinación con otros métodos de autenticación. Puede cambiar los valores predeterminados de la siguiente manera:

Para especificar una combinación de opciones de autenticación, bajo Opciones disponibles haga clic en el icono para seleccionar el primer método de autenticación. En el cuadro de diálogo Opciones disponibles, seleccione el segundo método de autenticación y, a continuación, haga clic en **Aceptar**.

Por ejemplo, puede solicitar una huella digital y una contraseña como credenciales de inicio de sesión. En el cuadro de diálogo, seleccione el segundo método de autenticación que se debe utilizar con la autenticación de huella digital.

Para permitir que cada método de autenticación pueda usarse individualmente, en el cuadro de diálogo Opciones disponibles, establezca el segundo método de autenticación en **Ninguno** y haga clic en **Aceptar**.

Para eliminar una opción de inicio de sesión, en Opciones disponibles de la página Opciones de inicio de sesión, haga clic en **X** para eliminar este método.

Para agregar una nueva combinación de métodos de autenticación, haga clic en **Agregar una opción**.

Para guardar la configuración de la función seleccionada, haga clic en **Aplicar.**

 **: Seleccione el botón Valores predeterminados para restaurar la configuración a sus valores originales.**

Configuración de preguntas de recuperación

En la página Preguntas de recuperación, puede seleccionar las preguntas que se presentarán a los usuarios cuando definan las Preguntas de recuperación personales y las respuestas. Las Preguntas de recuperación permiten a los usuarios recuperar el acceso a sus equipos si las contraseñas han caducado o se han olvidado.

Para configurar las preguntas de recuperación:

En el panel izquierdo, en Autenticación, seleccione **Preguntas de recuperación**.

En la página Preguntas de recuperación, seleccione, como mínimo, tres Preguntas de recuperación predefinidas.

De manera opcional, puede agregar hasta tres preguntas personalizadas a la lista de selección para el usuario.

Para guardar las Preguntas de recuperación, haga clic en **Aplicar**.

Configuración de la autenticación mediante lectura de huellas digitales

Para configurar la autenticación mediante lectura de huellas digitales:

En el panel izquierdo, bajo **Autenticación,** seleccione **Huellas digitales**.

En Registros, defina el número mínimo y máximo de huellas digitales que el usuario puede registrar.

Defina la sensibilidad de la lectura de huella digital.

Una baja sensibilidad admite una desviación más alta y aumenta las probabilidades de aceptar una lectura falsa. En la configuración más alta, el sistema puede rechazar huellas digitales legítimas. La configuración de Más sensibilidad baja el índice de aceptaciones de lecturas falsas a 1 en 10 000.

Haga clic en **Borrar lector** para eliminar todas las lecturas de huellas y registros de credenciales del búfer del lector de huellas digitales. De esta manera solamente se eliminan datos que actualmente se están agregando. No elimina lecturas y registros almacenados de sesiones previas.

Para guardar los valores de configuración, haga clic en **Aplicar**.

Configuración de la Autenticación de Contraseña de un solo uso

: La función de la Contraseña de un solo uso (OTP) requiere que haya un TPM presente, habilitado y con propietario. Para obtener instrucciones sobre cómo configurar el TPM, consulte Configuración previa a la instalación para la Contraseña de un solo uso.

Para utilizar la función de Contraseñas de un solo uso, el usuario genera una Contraseña de un solo uso con la aplicación Security Tools Mobile de su dispositivo móvil y después escribe la contraseña en el equipo. La contraseña solo se puede utilizar una vez y solo es válida durante un periodo de tiempo limitado.

Para mejorar más la seguridad, el administrador puede garantizar que la aplicación móvil es segura solicitando una contraseña.

En la página Dispositivo móvil, puede configurar los valores que mejoran la seguridad del dispositivo móvil y de la Contraseña de un solo uso.

Para configurar la autenticación mediante la Contraseña de un solo uso:

En el panel izquierdo, en Autenticación, seleccione **Dispositivo móvil**.

Para solicitar al usuario que introduzca una contraseña para acceder a la aplicación Security Tools Mobile en el dispositivo móvil, seleccione **Solicitar contraseña**.

: Si se habilita la política *Solicitar contraseña* después de que los dispositivos móviles se hayan registrado con un equipo, se cancelará el registro de dichos dispositivos móviles. Se solicitará a los usuarios que vuelvan a registrar sus dispositivos móviles una vez que se haya habilitado la política.

Cuando la casilla de verificación **Solicitar contraseña** esté seleccionada, los usuarios debe desbloquear su dispositivo móvil para acceder a la aplicación Security Tools Mobile. Si el dispositivo móvil no cuenta con un bloqueo de dispositivo, será necesario una contraseña.

Para seleccionar la longitud de la Contraseña de un solo uso (OTP), en **Longitud de la contraseña de un solo uso**, seleccione el número de caracteres de la contraseña que se necesitan.

Para seleccionar el número de intentos que el usuario tiene hasta introducir la Contraseña de un solo uso correctamente, seleccione un número del **5** al **30** en **Intentos de inicio de sesión del usuario permitidos**.

Cuando se ha alcanzado el número máximos de intentos, se deshabilitará la función OTP hasta que el usuario vuelva a registrar el dispositivo móvil.

: Dell recomienda la configuración de al menos otro método de autenticación además de la Contraseña de un solo uso.

Configuración del registro de tarjetas inteligentes

DDP|Security Tools es compatible con dos tipos de tarjetas inteligentes: con contacto y sin contacto.

Las tarjetas con contacto requieren un lector de tarjeta inteligente donde se introducirá la tarjeta. Las tarjetas con contacto son solamente compatibles con equipos de dominio. Las tarjetas CAC y SIPRNet son ambas tarjetas con contacto. Debido a la naturaleza avanzada de estas tarjetas, el usuario necesitará escoger un certificado después de introducir su tarjeta para iniciar sesión.

Las tarjetas sin contacto son compatibles con equipos que no pertenecen a un dominio y con equipos configurados con especificaciones de dominio.

Los usuarios pueden registrar una tarjeta inteligente con contacto por cuenta de usuario, o varias tarjetas sin contacto por cuenta.

Las tarjetas inteligentes no son compatibles con la Autenticación previa al inicio.

: Al eliminar el registro de una tarjeta inteligente de una cuenta con varias tarjetas registradas, se anulará el registro de todas las tarjetas al mismo tiempo.

Para configurar el registro de tarjetas inteligentes

En la pestaña de Autenticación de la herramienta Configuración del administrador, seleccione **Tarjeta inteligente**.

Configuración de permisos avanzados

Haga clic en **Avanzado** para modificar las opciones de usuario final avanzadas. En *Avanzado*, puede permitir de manera opcional a los usuarios el registro automático de credenciales o permitir a los usuarios que modifiquen sus credenciales registradas y habilitar el inicio de sesión en un paso.

Active o desactive las siguientes casillas de verificación:

Permitir a los usuarios registrar credenciales: esta casilla de verificación está seleccionada de manera predeterminada. Se permite a los usuarios registrar credenciales sin la intervención de un administrador. Si desmarca la casilla de verificación, el administrador será el encargado de registrar las credenciales.

Permitir a los usuarios modificar sus credenciales registradas: esta casilla de verificación está seleccionada de manera predeterminada. Cuando está seleccionada, se permite a los usuarios modificar o eliminar sus credenciales registradas sin la intervención de un administrador. Si desmarca la casilla de verificación, las credenciales no podrán ser modificadas ni eliminadas por un usuario normal. Deberá modificarlas o eliminarlas el administrador.

: Para registrar las credenciales de un usuario, vaya a la página *Usuarios* de la herramienta Configuración del administrador, seleccione un usuario y haga clic en Registrar.

Permitir inicio de sesión de un solo paso: el inicio de sesión de un solo paso es un Inicio de sesión único (SSO). De manera predeterminada, se selecciona la casilla de verificación. Cuando esta función está habilitada, los usuarios deben introducir sus credenciales solamente en la pantalla Autenticación previa al inicio. Los usuarios inician sesión en Windows automáticamente. Si desmarca la casilla de verificación, el usuario tendrá que iniciar sesión varias veces.

: Esta opción no se puede seleccionar a menos que se seleccione también el valor Permitir a los usuarios registrar credenciales.

Haga clic en **Aplicar** cuando termine.

Administración de la autenticación de usuarios

Los controles en la pestaña de Autenticación de la Configuración del administrador le permiten establecer opciones para el inicio de sesión del usuario y personalizar la configuración de cada uno.

Para administrar la autenticación de usuarios:

1 Como administrador, haga clic en el mosaico **Configuración del administrador**.

2 Haga clic en la pestaña **Usuarios** para administrar usuarios y ver el estado del registros de los usuarios. Desde esta pestaña, puede:

- Registrar nuevos usuarios
- Agregar o modificar credenciales
- Quitar las credenciales de un usuario

NOTA:

Inicio de sesión y **Sesión** muestran el estado de registro de un usuario.

Cuando el estado **Inicio de sesión** aparece como **OK**, significa que se han realizado todos los registros que el usuario necesita para poder iniciar sesión. Cuando el estado **Sesión** aparece como **OK**, significa que se han realizado todos los registros que el usuario necesita para utilizar el Password Manager.

Si alguno de estos dos estados aparece como **No**, el usuario tendrá que realizar más registros. Para saber qué registros faltan, seleccione la herramienta **Configuración de administrador** y abra la pestaña **Usuarios.** Cuando hay casillas que tienen una marca de verificación gris, significa que hay registros que están incompletos. Como alternativa, haga clic en el mosaico **Registros** y revise la columna **Política** de la pestaña **Estado**, en la que se indican los registros necesarios.

Cómo agregar nuevos usuarios

: Los nuevos usuarios de Windows se agregan automáticamente cuando inician sesión en Windows o registran credenciales.

Haga clic en **Agregar usuario** para iniciar el proceso de registro para un usuario de Windows existente.

Cuando se muestre el cuadro de diálogo *Seleccionar usuario*, seleccione **Tipos de objeto** .

Introduzca un nombre de objeto de usuario en el cuadro de texto y haga clic en **Comprobar nombres**.

Haga clic en **Aceptar** cuando termine.

Se abre el Asistente de registro.

Continúe para Registro o cambio de las credenciales del usuario para obtener instrucciones.

Registro o cambio de las credenciales del usuario

El administrador puede registrar o cambiar las credenciales de un usuario en nombre del usuario, pero algunas actividades de registro requieren la presencia del usuario; por ejemplo, para responder a las preguntas de recuperación y leer las huellas digitales del usuario.

Para registrar o cambiar las credenciales de un usuario:

En Configuración del administrador, haga clic en la pestaña **Usuarios**.

En la página Usuarios, haga clic en **Registrar**.

En la página de Bienvenida, haga clic en **Siguiente**.

En el cuadro de diálogo Se requiere autenticación, inicie sesión con la contraseña de Windows del usuario, y haga clic en **Aceptar**.

En la página Contraseña, para cambiar la contraseña de Windows del usuario, introduzca y confirme la nueva contraseña y haga clic en **Siguiente**.

Si no desea cambiar la contraseña, haga clic en **Omitir**. El asistente le permite omitir una credencial si no desea registrarla. Para volver a la página, haga clic en **Atrás**.

Siga las instrucciones de cada página y haga clic en el botón correspondiente: **Siguiente**, **Omitir**, o **Atrás.**

En la página de Resumen, confirme las credenciales registradas y, cuando se haya terminado con el proceso de registro, haga clic en **Aplicar**.

Para volver a la página de registro de credenciales para hacer un cambio, haga clic en **Atrás** hasta llegar a la página que desea cambiar.

Para obtener información más detallada sobre cómo inscribir o cambiar una credencial, consulte *Console User Guide* (Guía del usuario de la consola).

Cómo quitar una credencial registrada

Haga clic en el mosaico **Configuración de administrador**.

Haga clic en la pestaña **Usuarios** y busque el usuario que desea cambiar.

Desplácese sobre la marca de verificación verde de la credencial que desea eliminar. Se convierte en ⊗.

Haga clic en el símbolo ⊗ y, a continuación, haga clic en **Sí** para confirmar la eliminación.

: No es posible quitar una credencial de este modo si es la única credencial registrada que tiene el usuario. Además, no es posible eliminar la contraseña de este modo. Utilice el comando Quitar para eliminar completamente el acceso de un usuario al equipo.

Cómo quitar todas las credenciales registradas de un usuario

Haga clic en el mosaico **Configuración de administrador**.

Haga clic en la pestaña **Usuarios** y busque el usuario que desea eliminar.

Haga clic en **Quitar**. (El comando Quitar aparece en rojo en la parte inferior de la configuración del usuario).

Tras la eliminación, el usuario no podrá iniciar sesión en el equipo a menos que se vuelva a registrar.

Desinstalación mediante el instalador maestro

- Cada componente debe desinstalarse por separado, seguido de la desinstalación del instalador maestro . Los clientes se deben desinstalar en un **orden específico para evitar errores en la desinstalación**.
- Siga las instrucciones en Extracción de instaladores secundarios del instalador maestro para obtener instaladores secundarios.
- Asegúrese de que se utilice la misma versión del instalador maestro (y de los clientes) tanto para la desinstalación como para la instalación.
- Este capítulo le remite a otro capítulo que contiene instrucciones *detalladas* sobre cómo desinstalar los instaladores secundarios. En este capítulo **solo** se explica el último paso, la desinstalación del instalador maestro .

Desinstale los clientes en el siguiente orden.

1 Desinstalación del cliente Encryption.
2 Desinstalación del cliente Security Framework.
3 Desinstalación de Advanced Authentication.

No es necesario desinstalar el paquete de controladores.

Continúe con Selección de un método de desinstalación.

Selección de un método de desinstalación

Hay dos métodos para desinstalar el instalador maestro; seleccione **uno** de los siguientes:

- Desinstalación desde Agregar/Quitar programas
- Desinstalación desde la línea de comandos

Desinstalación desde Agregar/Quitar programas

Vaya a Desinstalar un programa en el panel de control de Windows (**Inicio** > **Panel de control** > **Programas y características** > **Desinstalar un programa.**).

Seleccione **Dell Data Protection Installer** y haga clic con el botón izquierdo del mouse en **Cambiar** para iniciar el Asistente para la instalación.

Lea la Pantalla de bienvenida y haga clic en **Siguiente**.

Siga las indicaciones para desinstalar y haga clic en **Finalizar**.

Reinicie el equipo e inicie una sesión en Windows.

El instalador maestro está desinstalado.

Desinstalación desde la línea de comandos

En el siguiente ejemplo se desinstala de forma silenciosa el instalador maestro.

```
"DDPSetup.exe" -y -gm2 /S /x
```

Reinicie el equipo cuando finalice.

El instalador maestro está desinstalado.

Continúe con Desinstalación mediante los instaladores secundarios.

8

Desinstalación mediante los instaladores secundarios

- El usuario que lleve a cabo el descifrado y la desinstalación debe tener privilegios de administrador local o de dominio. Si se desinstala mediante líneas de comandos, se requerirán credenciales del administrador de dominio.
- Si instaló Personal Edition mediante el instalador maestro, antes de la instalación deberá extraer los archivos ejecutables secundarios del instalador maestro, como se muestra en el apartado Extracción de instaladores secundarios del instalador maestro.
- Asegúrese de que se utiliza la misma versión de los clientes tanto para la desinstalación como para la instalación.
- De ser posible, planifique el descifrado para la noche.
- Desactive el modo de suspensión para que el equipo no entre en este modo. El descifrado se interrumpirá si el equipo entra en el modo de suspensión.
- Cierre todos los procesos y aplicaciones a fin de reducir al mínimo los errores debidos a archivos bloqueados.

Desinstalación del cliente Encryption

- **Antes de empezar el proceso de desinstalación**, consulte (Opcional) Creación de un archivo de registro de Encryption Removal Agent. Este archivo de registro es útil para el diagnóstico de errores de las operaciones de desinstalación/descifrado. No necesita crear un archivo de registro de Encryption Removal Agent si no quiere descifrar los archivos durante el proceso de desinstalación.
- Ejecute WSScan para asegurarse de que todos los datos se descifren una vez finalizada la desinstalación, pero antes de reiniciar el equipo. Consulte Uso de WSScan para obtener instrucciones.
- Periódicamente Compruebe el estado de Encryption Removal Agent. El descifrado de datos sigue en curso si el servicio Encryption Removal Agent continúa existiendo en el panel Servicios.

Selección de un método de desinstalación

Hay dos métodos para desinstalar el cliente Encryption; seleccione **uno** de los siguientes:

Desinstalación mediante la interfaz de usuario

Desinstalación desde la línea de comandos

Desinstalación mediante la interfaz de usuario

Vaya a Desinstalar un programa en el Panel de control de Windows (**Inicio** > **Panel de control** > **Programas y características** > **Desinstalar un programa.**).

Seleccione **Cifrado** y haga clic con el botón izquierdo en **Cambiar** para iniciar el Asistente para la instalación de Personal Edition.

Lea la Pantalla de bienvenida y haga clic en **Siguiente**.

En la pantalla de instalación de Encryption Removal Agent, puede elegir entre dos opciones:

: Como opción predeterminada, la segunda opción está seleccionada. Si quiere descifrar archivos, asegúrese de cambiar la selección a la opción uno.

Encryption Removal Agent - Importar claves de un archivo

Para cifrados SDE, de Usuario o Común, esta opción descifra archivos y desinstala el cliente Encryption. ***Esta es la selección recomendada.***

No instale Encryption Removal Agent

Esta opción desinstala el cliente Encryption, *pero no descifra archivos*. Esta opción **solo** se debería utilizar para solución de problemas, según indique el Dell ProSupport.

Haga clic en **Siguiente**.

En el cuadro de texto *Archivo de copia de seguridad*, introduzca la ruta de acceso a la unidad de red o ubicación de medios extraíbles del archivo de copia de seguridad o haga clic en **...** para buscar la ubicación. El formato del archivo es LSARecovery_[nombre de host].exe.

Introduzca su contraseña del administrador de Encryption en el cuadro de texto Contraseña. Esta es la contraseña que se estableció en el Asistente para la instalación cuando instaló el software.

Haga clic en **Siguiente**.

En la pantalla *Inicio de sesión en Dell Decryption Agent Service como* existen dos opciones. Seleccione **Cuenta del sistema local**. Haga clic en **Finalizar**.

Haga clic en **Quitar** en la pantalla Quitar el programa.

Haga clic en **Finalizar** en la pantalla Configuración completa.

Reinicie el equipo e inicie sesión en Windows.

El descifrado está en curso ahora.

El proceso de descifrado podría tardar varias horas, en función de la cantidad de unidades que se estén descifrando y la cantidad de información en cada una de dichas unidades. Para comprobar el proceso de descifrado, consulte Comprobación del estado de Encryption Removal Agent.

Desinstalación desde 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. Los parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.

Utilice estos instaladores para desinstalar los clientes mediante instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.

Archivos de registro

Windows crea archivos de registro de instalación de instaladores secundarios para el usuario que haya iniciado sesión en %temp%, que se encuentra en C:\Users\<nombre de usuario>\AppData\Local\Temp.

Si decide agregar un archivo de registro independiente cuando ejecute el instalador, asegúrese de que el archivo de registro tenga un nombre exclusivo, ya que los archivos de registro de instalador secundario no se anexan. El comando .msi estándar se puede usar para crear un archivo de registro mediante /l C:\<cualquier directorio>\<cualquier nombre de archivo de registro>.log. Dell no recomienda usar "/l*v" (registro detallado) en una desinstalación de línea de comandos, ya que el nombre de usuario/contraseña se registra en el archivo de registro.

Todos los instaladores secundarios utilizan los mismos modificadores y opciones de presentación de .msi básicos, salvo donde se indique, para las desinstalaciones de línea de comandos. Los modificadores deben especificarse primero. El modificador /v es un requisito y toma un argumento. Otros parámetros se introducen en el argumento que luego pasa al modificador /v.

Las opciones de presentación que pueden especificarse al final del argumento que se envía al modificador /v, para que su comportamiento sea el esperado. No utilice /q ni /qn en la misma línea de comandos. Utilice solamente ! y - después de /qb.

Modificador	Significado
/v	Envía las variables al archivo .msi dentro de setup.exe
/s	Modo silencioso
/x	Modo de desinstalación

Opción	Significado
/q	Sin diálogo de progreso; se reinicia automáticamente tras completar el proceso
/qb	Diálogo de progreso con botón **Cancelar** , indica que es necesario reiniciar
/qb-	Diálogo de progreso con botón **Cancelar**, se reinicia automáticamente al terminar el proceso
/qb!	Diálogo de progreso sin botón **Cancelar**, indica que es necesario reiniciar
/qb!-	Diálogo de progreso sin botón **Cancelar** , se reinicia automáticamente al terminar el proceso
/qn	Sin interfaz de usuario

Una vez extraído del instalador maestro, el instalador del cliente Encryption puede encontrarse en **C:\extracted\Encryption \DDPE_XXbit_setup.exe**.

La tabla a continuación indica los parámetros disponibles para la desinstalación.

Parámetro	Selección
CMG_DECRYPT	Propiedad para seleccionar el tipo de instalación de Encryption Removal Agent: 2 - Obtener claves mediante un paquete de Forensic Key 0 - No instalar Encryption Removal Agent
CMGSILENTMODE	Propiedad para desinstalación silenciosa: 1 - Silencioso 0 - No silencioso
DA_KM_PW	La contraseña para la cuenta del Administrador de dominio.
DA_KM_PATH	Ruta de acceso al paquete del material de claves.

El siguiente ejemplo desinstala el cliente de Cifrado sin instalar Encryption Removal Agent.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe
DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

El siguiente ejemplo desinstala el cliente de Cifrado mediante un paquete de Forensic Key. Copie el paquete de Forensic Key en el disco local y, a continuación, ejecute este comando.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Reinicie el equipo cuando finalice.

El proceso de descifrado podría tardar varias horas, en función de la cantidad de unidades que se estén descifrando y la cantidad de información en cada una de dichas unidades. Para comprobar el proceso de descifrado, consulte Comprobación del estado de Encryption Removal Agent.

Desinstalación de Advanced Authentication

Elija una desinstalación Método

Existen dos métodos para desinstalar el cliente de codificación, seleccione **uno** de los siguientes:

- Desinstalar utilizando la interfaz de usuario
- Desinstalar desde la línea de comandos

Desinstalar utilizando la interfaz de usuario

1. Vaya a Desinstalar un programa en el panel de control de Windows (**Inicio** > **Panel de control** > **Programs and Features (Programas y Funciones** > **Desinstalar un programa.**).
2. Resalte **Herramientas de seguridad autenticación** y haga clic con el botón izquierdo en **Cambiar** para iniciar el asistente para la instalación.
3. Lea la pantalla de bienvenida y, a continuación, haga clic en **Siguiente**.
4. Introduzca la contraseña de administrador.
5. Siga las indicaciones para desinstalar y haga clic en **Finalizar**.
6. Reinicie el equipo y iniciar sesión en Windows.

Herramientas de seguridad Autenticación está desinstalado.

Desinstalar desde la línea de comandos

1. Una vez que se extrae del maestro instalador, la autenticación avanzada client installer (instalador se puede encontrar en **C: \extraídos \Herramientas de seguridad\Authentication\ <x64/x86 > \setup.exe**.
2. El siguiente ejemplo silenciosamente, desinstala la autenticación avanzada cliente.

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

3. Apague y reinicie el equipo cuando haya terminado.

Continúe con las políticas y descripciones de plantillas.

Desinstalación del cliente Security Framework

Selección de un método de desinstalación

Hay dos métodos para desinstalar el cliente Encryption; seleccione **uno** de los siguientes:

- Desinstalación mediante la interfaz de usuario
- Desinstalación desde la línea de comandos

Desinstalación mediante la interfaz de usuario

1. Vaya a Desinstalar un programa en el Panel de control de Windows (**Inicio** > **Panel de control** > **Programas y características** > **Desinstalar un programa.**).
2. Resalte **Client Security Framework** y haga clic con el botón izquierdo en **Cambiar** para iniciar el asistente para la instalación.
3. Lea la Pantalla de bienvenida y haga clic en **Siguiente**.
4. Siga las indicaciones para desinstalar y haga clic en **Finalizar**.
5. Reinicie el equipo e inicie sesión en Windows.

Cliente Security Framework está desinstalado.

Desinstalación desde la línea de comandos

Una vez extraído del instalador maestro, el instalador del cliente Security Framework se puede encontrar en C:extracted\Security Tools \EMAgent_.

El siguiente ejemplo desinstala de forma silenciosa el cliente SED.

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

Apague y reinicie el equipo cuando finalice.

Descripciones de plantillas y políticas

Al pasar el puntero del mouse sobre una política en la Local Management Console, se muestra información sobre herramientas.

Políticas

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
Políticas de almacenamiento fijo										
Cifrado de SDE habilitado	Verdadero								Falso	Esta política es la “política maestra” de todas las demás políticas de System Data Encryption (SDE). Si el valor de esta política es Falso, no tendrá lugar el cifrado de SDE, sin importar el valor de las demás políticas. El valor Verdadero significa que todos los datos que no estén cifrados por otras políticas del Cifrado Inteligente serán cifrados conforme a la política de las Reglas de cifrado de SDE. Al cambiar el valor de esta política, es necesario reiniciar la máquina.
Algoritmo de cifrado de SDE	AES256									AES 256, AES 128, 3DES
Reglas de cifrado de SDE										Las reglas de cifrado que se utilizarán para cifrar/no cifrar ciertas unidades, directorios y carpetas. Póngase en contacto con Dell ProSupport para obtener asesoramiento si no está

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										seguro de si debe cambiar los valores predeterminados.
Políticas de configuración general										
Cifrado habilitado	Verdadero							Falso		Esta política es la "política maestra" para todas las políticas de la configuración general. Un valor Falso significa que no tendrá lugar el cifrado, sin importar el valor de las demás políticas. Un valor Verdadero significa que todas las políticas de cifrado están habilitadas. Si se cambia el valor de esta política se activará un nuevo barrido de cifrado/descifrado de archivos.
Las carpetas cifradas de archivos comunes										Cadena: máximo de 100 entradas de 500 caracteres cada una (hasta un máximo de 2048 caracteres) Una lista de carpetas presentes en las unidades de los extremos a ser cifrados o excluidos del cifrado, a la que tienen acceso todos los usuarios administrados que tengan acceso al extremo. Las letras de unidad disponibles son: #: Se refiere a todas las unidades f#: Se refiere a todas las unidades fijas r#: Se refiere a todas las unidades extraíbles Importante: El reemplazo por jerarquía de la protección de los directorios podría hacer que el equipo no se inicie y/o requiera que se vuelvan a

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										formatear las unidades de disco. Si la misma carpeta está incluida en esta política y en la política de carpetas cifradas por claves de usuario, esta política prevalece.
Algoritmo común de cifrado	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Los archivos de paginación del sistema se cifran mediante AES 128.
Lista de Application Data Encryption	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									Cadena: un máximo de 100 entradas de 500 caracteres cada una Dell recomienda no incluir explorer.exe ni iexplorer.exe a la lista ADE, ya que los resultados podrían ser inesperados o no los resultados deseados. No obstante, el proceso explorer.exe es el utilizado para crear nuevos archivos del bloc de notas en el escritorio, mediante el menú de clic con el botón de la derecha. La configuración del cifrado con el uso de extensiones de archivos, en vez de la lista ADE, ofrece una cobertura más exhaustiva. Enumere los nombres de procesos de aplicaciones (sin rutas) cuyos nuevos archivos desea cifrar, separados por retornos de carro. No utilice caracteres comodín en las entradas. Dell recomienda no incluir en la lista ninguna aplicación ni instalador que escriba archivos cruciales del sistema. Hacerlo podría provocar que se cifren archivos importantes del

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										sistema y que el equipo no pueda iniciarse. Nombres de proceso comunes: outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Los siguientes nombres de procesos codificados del sistema y de instaladores no se toman en cuenta si se especifican en esta política: hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe
Clave de Application Data Encryption	Común									Común o usuario Elija una clave para indicar quiénes deben poder tener acceso a los archivos cifrados por la lista de Application Data Encryption, y en qué lugar. "Común" si desea que el acceso a los archivos esté disponible para todos los usuarios administrados del extremo donde fueron creados (el mismo nivel de acceso de las carpetas cifradas con clave común), y que los archivos sean cifrados con el algoritmo de cifrado común. "Usuario" si desea que el acceso a los archivos esté disponible únicamente para el usuario que los creó, solamente en el extremo donde fueron creados (el mismo nivel de acceso de las carpetas cifradas con clave de usuario), y que los archivos

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										sean cifrados con el algoritmo de cifrado de clave de usuario. Los cambios a esta política no afectan a los archivos que ya fueron cifrados como resultado de esta política.
Cifrar las carpetas personales de Outlook	Verdadero							Falso		El valor Verdadero cifra las carpetas personales de Outlook.
Cifrar archivos temporales	Verdadero							Falso		El valor Verdadero cifra las rutas indicadas en las variables de entorno TEMP y TMP con la Clave de cifrado de los datos del usuario.
Cifrar los archivos temporales de Internet	Verdadero	Falso								El valor Verdadero cifra la ruta indicada en la variable de entorno CSIDL_INTERNET_CACHE con la Clave de cifrado de los datos del usuario. A fin de reducir la duración de los barridos de cifrado, el cliente borra el contenido de CSIDL_INTERNET_CACHE antes de realizar el cifrado inicial, así como las actualizaciones a esta política. Esta política rige solo cuando se utiliza Microsoft Internet Explorer.
Cifrar documentos del perfil de usuario	Verdadero								Falso	El valor Verdadero cifra: · El perfil de usuario (C:\Usuarios\jperez) con la Clave de cifrado de los datos del usuario · \Usuarios\Acceso con la clave de cifrado común
Cifrar el archivo de paginación	Verdadero								Falso	El valor Verdadero cifra el archivo de paginación de Windows. Al realizar un cambio en esta política, se debe reiniciar el equipo.

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
de Windows										
Servicios administrados										Cadena: máximo de 100 entradas de 500 caracteres cada una (hasta un máximo de 2048 caracteres) Cuando un servicio es administrado por esta política, el servicio se inicia solo después de que el usuario haya iniciado una sesión y que el cliente esté desbloqueado. Esta política también garantiza que se detenga el servicio administrado por esta política antes de que el cliente se bloquee durante el cierre de la sesión. Esta política también puede impedir el cierre de la sesión del usuario si el servicio no responde. La sintaxis es un nombre de servicio por línea. Se admiten espacios en el nombre de servicio. No se admiten comodines. Los servicios administrados no arrancarán si un usuario no administrado inicia una sesión.
Limpieza segura post-cifrado	Sobrescribir tres veces	Sobrescribir una vez							Sin sobrescribir	Sin sobrescribir, Sobrescribir una vez, Sobrescribir tres veces, Sobrescribir siete veces Una vez que se hayan cifrado las carpetas especificadas en otras políticas de esta categoría, esta política determina lo que ocurre con los archivos originales residuales no cifrados: · "Sin sobrescribir" los borra. Este valor brinda el proceso de cifrado más rápido.

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										• "Sobrescribir una vez" sobrescribe el archivo original con datos aleatorios. • "Sobrescribir tres veces" sobrescribe el archivo original con un patrón estándar de 1s y 0 s, después con su complemento, y finalmente con datos aleatorios. • "Sobrescribir siete veces" sobrescribe el archivo original con un patrón estándar de 1s y 0 s, después con su complemento, y finalmente cinco veces con datos aleatorios. Esta última opción dificulta al máximo la recuperación de los archivos originales de la memoria, y ofrece el proceso de cifrado más seguro.
Proteger el archivo de hibernación de Windows	Verdadero					Falso		Verdadero	Falso	Al habilitar esta opción, el archivo de hibernación se cifrará únicamente cuando el equipo realice la hibernación. El cliente desactivará la protección cuando el equipo salga de la hibernación, y brindará protección sin afectar a los usuarios ni a las aplicaciones mientras el equipo esté en uso.
Evitar la hibernación no protegida	Verdadero					Falso		Verdadero	Falso	Al habilitar esta opción, el cliente no permitirá la hibernación del equipo si el cliente no puede cifrar los datos de hibernación.
Prioridad de la exploración de la estación de trabajo	Alto	Normal								Más alta, Alta, Normal, Baja, Más baja Especifica la prioridad relativa de exploración de carpetas cifradas de Windows.
Carpetas cifradas del usuario										Cadena: máximo de 100 entradas de 500 caracteres cada una (hasta un máximo de 2048 caracteres)

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										Una lista de carpetas de la unidad de disco duro del extremo que serán cifradas con la Clave de cifrado de los datos del usuario o que serán excluidas del cifrado. Esta política se aplica a todas las unidades que Windows clasifique como unidades de disco duro. No puede utilizar esta política para cifrar unidades o medios externos cuyo tipo figure como disco extraíble. En ese caso, deberá utilizar el medio externo de cifrado de EMS.
Algoritmo de cifrado del usuario	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES El algoritmo utilizado para cifrar la información a nivel del usuario individual. Se pueden especificar distintos valores para los distintos usuarios de un mismo extremo.
Clave de cifrado de los datos del usuario	Usuario	Común		Usuario	Común				Usuario	Común o usuario Elija una clave para indicar quiénes deben poder tener acceso a los archivos cifrados por las siguientes políticas, y en qué lugar. · Carpetas cifradas del usuario · Cifrar las carpetas personales de Outlook · Cifrar archivos temporales (solo en \Documents and Settings\username\Local Settings\Temp) · Cifrar los archivos temporales de Internet · Cifrar documentos del perfil de usuario Seleccione:

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										• "Común" si desea que el acceso a los archivos/carpetas cifrados con clave de usuario esté disponible para todos los usuarios administrados del extremo donde fueron creados (el mismo nivel de acceso de las carpetas cifradas con clave común), y que los archivos sean cifrados con el algoritmo de cifrado de clave común. • "Usuario" si desea que el acceso a los archivos esté disponible únicamente para el usuario que los creó, solamente en el extremo donde fueron creados (el mismo nivel de acceso de las carpetas cifradas con clave de usuario), y que los archivos sean cifrados con el algoritmo de cifrado de clave de usuario. Si opta por incorporar una política de cifrado para cifrar todas las particiones del disco, se recomienda utilizar la política de cifrado SDE predeterminada, en lugar de una con clave común o de usuario. Esto garantiza el acceso a cualquier archivo del sistema operativo que se encuentre cifrado durante estados en los que el usuario administrado no tenga la sesión abierta.
Hardware Crypto Accelerator (solamente compatible con v8.3 a través de clientes de Cifrado v8.9.1)										
Hardware Crypto Accelerator (HCA)	Falso									Esta política es la “política maestra” de todas las demás políticas de Hardware Crypto Accelerator (HCA). Si el valor de esta política es Falso, no tendrá lugar el cifrado de HCA, independientemente del valor de las demás políticas. Las políticas de HCA solamente se pueden utilizar

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										en equipos que cuenten con Hardware Crypto Accelerator.
Volúmenes destinados a cifrado	Todos los volúmenes fijos									Todos los volúmenes fijos o solo el volumen del sistema Especifique qué volúmenes desea marcar para el cifrado.
Metadatos forenses disponibles en la unidad cifrada HCA	Falso									Verdadero o Falso Si el valor es Verdadero, los metadatos forenses se incluyen en la unidad para facilitar el análisis forense. Los metadatos consisten en lo siguiente: • Id. de equipo (MCID) del equipo actual • Id. de dispositivo (DCID/SCID) de la instalación de Shield actual Si el valor es Falso, los metadatos forenses no se incluyen en la unidad. El cambio de valores de Falso a Verdadero iniciará un nuevo barrido en función de las políticas de HCA para agregar el análisis forense.
Permitir la aprobación del usuario de cifrado de la unidad secundaria	Falso									El valor Verdadero permite que los usuarios decidan si desean cifrar unidades adicionales.
Algoritmo de cifrado	AES256									AES 256 o AES 128
Políticas de control de puertos										
Sistema de control de puertos	Deshabilitado									Habilitar o deshabilitar todas las políticas del sistema de control de puertos. Si esta política se configura como Deshabilitar, no se aplicará ninguna política del sistema de

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										control de puertos, sin importar las demás políticas de control de puertos. **Nota:** Las políticas de PC requieren un reinicio antes de surtir efecto.
Puerto: Ranura de Express Card	Habilitado									Habilita, deshabilita o evita los puertos expuestos mediante la ranura de Express Card.
Puerto: eSATA	Habilitado									Habilita, deshabilita o evita el acceso de los puertos a puertos externos SATA.
Puerto: PCMCIA	Habilitado									Habilita, deshabilita o evita el acceso de los puertos a puertos PCMCIA.
Puerto: Firewire (1394)	Habilitado									Habilita, deshabilita o evita el acceso de los puertos a puertos externos de Firewire (1394).
Puerto: SD	Habilitado									Habilita, deshabilita o evita el acceso de los puertos a puertos para tarjetas SD.
Subclase de almacenamiento: Control de unidad externa	Bloqueado	Solo lectura			Acceso total			Solo lectura	Acceso total	SECUNDARIO de clase: Almacenamiento. Clase: El almacenamiento debe estar establecido en Habilitado para utilizar esta política. Esta política interactúa con PCS. Consulte Interacciones entre EMS y PCS. Acceso total: El puerto de unidad externa no tiene restricciones de lectura o escritura de datos Solo lectura: Habilita la función de lectura. La función de escritura queda deshabilitada Bloqueado: El puerto queda bloqueado para la lectura y escritura

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										Esta política está restringida al extremo, por lo que no puede anularse mediante políticas de usuario.
Puerto: Dispositivo de transferencia de memoria (MTD)	Habilitado									Habilita, deshabilita o evita el acceso a puertos de Dispositivos de transferencia de memoria (MTD).
Clase: Almacenamiento	Habilitado									PRINCIPAL de las siguientes tres políticas. Establezca esta política como Habilitada para utilizar las siguientes 3 políticas de subclase de almacenamiento. Establecer esta política en Deshabilitado deshabilita las 3 políticas de subclase de almacenamiento, sin importar cuál sea su valor.
Subclase de almacenamiento: Control de unidad óptica	Solo lectura	Solo UDF				Acceso total	Solo UDF	Acceso total		SECUNDARIO de clase: Almacenamiento. Clase: El almacenamiento debe estar establecido en Habilitado para utilizar esta política. Acceso total: El puerto de unidad óptica no tiene restricciones de lectura o escritura de datos Solo UDF: Bloquea la escritura de datos cuando no está en el formato UDF (grabación de CD/DVD o ISO). La función de lectura queda habilitada. Solo lectura: Habilita la función de lectura. La función de escritura queda deshabilitada Bloqueado: El puerto queda bloqueado para la lectura y escritura Esta política está restringida al extremo, por lo que no puede anularse mediante políticas de usuario.

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										El Universal Disk Format (Formato de disco universal - UDF) es una implementación de la especificación que se conoce como ISO/IEC 13346 y ECMA-167. Se trata de un sistema genérico de archivos que se halla disponible para el almacenamiento de datos en una amplia variedad de medios. Esta política interactúa con PCS. Consulte Interacciones entre EMS y PCS.
Subclase de almacenamiento: Control de unidad de disco flexible	Bloqueado	Solo lectura				Acceso total		Solo lectura	Acceso total	SECUNDARIO de clase: Almacenamiento. Clase: El almacenamiento debe estar establecido en Habilitado para utilizar esta política. Acceso total: El puerto de unidad de disco flexible no tiene restricciones de lectura o escritura de datos Solo lectura: Habilita la función de lectura. La función de escritura queda deshabilitada Bloqueado: El puerto queda bloqueado para la lectura y escritura Esta política está restringida al extremo, por lo que no puede anularse mediante políticas de usuario.
Clase: Dispositivo portátil de Windows (WPD)	Habilitado									PRINCIPAL de la siguiente política. Establezca esta política como Habilitada para usar la política de Subclase de Dispositivo portátil de Windows (WPD): Almacenamiento. Establecer esta política como Deshabilitada desactiva la política de Subclase de Dispositivo portátil de Windows (WPD):

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										Almacenamiento, sin importar cuál sea su valor. Controle el acceso a todos los Dispositivos portátiles de Windows.
Subclase de Dispositivo portátil de Windows (WPD): Almacenamiento	Habilitado									SECUNDARIO de clase: Dispositivo portátil de Windows (WPD) Clase: Dispositivo portátil de Windows (WPD) debe establecerse en Habilitada, para utilizar esta política. Acceso total: El puerto no tiene restricciones de lectura o escritura de datos. Solo lectura: Habilita la función de lectura. La función de escritura queda deshabilitada. Bloqueado: El puerto queda bloqueado para la lectura y escritura.
Clase: Dispositivo de interfaz humana (HID)	Habilitado									Controle el acceso a todos los Dispositivos de interfaz humana (teclado, mouse). **Nota:** El bloqueo a nivel de puerto USB y a nivel de clase de dispositivo de HID se ejecuta únicamente si se detecta que el tipo de chasis del equipo es un factor de forma de portátil/portátil ligero. La identificación del chasis se realiza a través del BIOS del equipo.
Clase: Otra	Habilitado									Controle el acceso a todos los dispositivos que no estén incluidos en otras clases.
Políticas de almacenamiento extraíble										
Medios externos de	Verdadero					Falso		Verdadero	Falso	Esta política es la "política maestra" para todas las políticas de almacenamiento

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
cifrado de EMS										extraíble. Un valor Falso significa que no tendrá lugar el cifrado de los dispositivos de almacenamiento extraíbles, sin importar el valor de las demás políticas. Un valor Verdadero significa que todas las políticas de cifrado de dispositivos de almacenamiento extraíbles están habilitadas. Esta política interactúa con PCS. Consulte Interacciones entre EMS y PCS.
Excluir cifrado de CD/DVD de EMS	Falso								Verdadero	Un valor Falso cifra los dispositivos CD/DVD. Esta política interactúa con PCS. Consulte Interacciones entre EMS y PCS.
Acceso de EMS a medios no protegido por Shield	Bloquear		Solo lectura			Acceso total	Solo lectura		Acceso total	Bloquear, Solo lectura, Acceso total Esta política interactúa con PCS. Consulte Interacciones entre EMS y PCS. Cuando esta política está configurada en Bloquear acceso, no se tendrá acceso al almacenamiento extraíble a menos que esté cifrado. Seleccionar Solo lectura o Acceso total le permite decidir qué dispositivos de almacenamiento extraíbles se van a cifrar. Si selecciona que no se desea cifrar el almacenamiento extraíble, y se configura esta política a Acceso total, se tendrá acceso total de lectura y escritura a los dispositivos de almacenamiento extraíble. Si selecciona que no quiere cifrar los dispositivos de

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										almacenamiento extraíbles, y configura esta política en Solo lectura, no se podrán leer ni eliminar los archivos existentes en los dispositivos de almacenamiento extraíbles no cifrados, pero el cliente no permitirá la modificación de ningún archivo ni tampoco agregar archivos nuevos al almacenamiento extraíble, a menos que esté cifrado.
Algoritmo de cifrado de EMS	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES
Exploración de medios externos de EMS	Verdadero	Falso								El valor Verdadero permite que EMS explore los dispositivos de almacenamiento extraíbles cada vez que se inserten. Si esta política está configurada en Falso y la política Cifrar medios externos de EMS está configurada en Verdadero, EMS cifrará solamente los archivos nuevos y modificados. Se producirá una exploración cada vez que se introduzcan, de modo que EMS pueda encontrar todos los archivos agregados sin autenticación al dispositivo de almacenamiento extraíble. Puede agregar archivos al almacenamiento extraíble si opta por no autenticar, pero no se tendrá acceso a los datos cifrados. En este caso, los archivos que se agreguen no serán cifrados, de modo que la próxima vez que se realice la autenticación en el medio extraíble para trabajar con datos cifrados, EMS explorará y cifrará todos los archivos que podrían haberse agregado sin cifrado.
Acceso de datos	Verdadero									El valor Verdadero permite el acceso del usuario a la

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
cifrados de EMS en un dispositivo no protegido por Shield										información cifrada en dispositivos de almacenamiento extraíbles, ya sea que el extremo esté o no esté cifrado.
Lista blanca de EMS de dispositivos										Esta política permite especificar los dispositivos de medios externos que se desean excluir del cifrado de EMS. Se protegerán todos los dispositivos de medios externos que no estén en esta lista. Se permite una cantidad máxima de 150 dispositivos con un máximo de 500 caracteres por PNPDeviceID. Máximo permitido de 2048 caracteres en total. Para buscar el PNPDeviceID para almacenamiento extraíble: 1 Introduzca el dispositivo de almacenamiento extraíble en un equipo protegido. 2 Abra EMSService.log en C:\Programdata\Dell \Dell Data Protection \Encryption\EMS. 3 Busque "PNPDeviceID=" Por ejemplo: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR \DISK&VEN_SEAGATE& PROD_USB&REV_0409\ 2HC015KJ&0 Especifique lo siguiente en la directiva de lista blanca de EMS de dispositivos: VEN = Proveedor (Ej.: USBSTOR \DISK&VEN_SEAGATE) PROD = Nombre de producto/ modelo (Ej.: &PROD_USB); también excluye del cifrado de EMS todas las unidades USB

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										de Seagate; un valor VEN (Ej.: USBSTOR \DISK&VEN_SEAGATE) debe preceder a este valor REV = Revisión del firmware (Ej.: &REV_0409); también excluye el modelo específico en uso; los valores VEN y PROD deben preceder a este valor Número de serie (Ej.: \2HC015KJ&0); excluye solo este dispositivo; los valores VEN, PROD y REV deben preceder a este valor Delimitadores permitidos: tabulador, coma, punto y coma, caracteres hexadecimales 0x1E (carácter separador de registro)
Se requieren caracteres alfabéticos de EMS en la contraseña.	Verdadero									El valor Verdadero obliga a que la contraseña tenga uno o más caracteres alfabéticos.
Se requieren letras mayúsculas y minúsculas de EMS en la contraseña.	Verdadero	Falso								El valor Verdadero obliga a que la contraseña tenga caracteres en mayúsculas y minúsculas.
Cantidad de caracteres de EMS. Requisitos de contraseña	8					6		8		1-40 caracteres La cantidad mínima de caracteres requerida en la contraseña.
Se requieren caracteres	Verdadero	Falso								El valor Verdadero obliga a que la contraseña tenga uno o más caracteres numéricos.

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
numéricos de EMS en la contraseña.										
Intentos de contraseña de EMS permitidos	2	3				4		3		1-10 La cantidad de veces que el usuario puede intentar introducir la contraseña correcta.
Se requieren caracteres especiales de EMS en la contraseña.	Verdadero	Falso							Verdadero	El valor Verdadero obliga a que la contraseña tenga uno o más caracteres especiales.
Retraso del tiempo de espera de EMS	30									0-5000 segundos Cantidad de segundos que el usuario debe esperar entre la primera y la segunda ronda de intentos de introducir el código de acceso.
Incremento en el tiempo de espera de EMS	30	20				10	30	10		0-5000 segundos El lapso en segundos que se sumará al tiempo de espera anterior después de cada ronda sin éxito de introducción del código de acceso.
Reglas de cifrado de EMS										Las reglas de cifrado para cifrar /no cifrar ciertas unidades, directorios y carpetas. Se permite un total de 2048 caracteres. Los caracteres "Espacio" e "Intro" utilizados para agregar líneas entre filas cuentan como caracteres utilizados. Se ignorará toda regla que exceda el límite de 2048 caracteres. Los dispositivos de almacenamiento que incluyen

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										conexiones de múltiples interfaces, tales como Firewire, USB, eSATA, etc., podrían requerir el uso de reglas EMS y de cifrado para poder cifrar el dispositivo. Lo anterior es necesario debido a las diferencias en la manera en que el sistema operativo Windows administra los dispositivos de almacenamiento según el tipo de interfaz. Consulte Cómo cifrar un iPod con EMS.
Acceso bloqueado de EMS a medios no protegidos	Verdadero								Falso	Se bloquea el acceso a cualquier dispositivo de almacenamiento extraíble que tenga menos de 17 MB y, por lo tanto, tenga una capacidad de almacenamiento insuficiente para instalar una protección Shield de medios extraíbles (como un disco flexible de 1,44 MB). Se bloquea todo acceso si Cifrar medios externos y esta política están configurados en Verdadero. Si la política de medios externos de cifrado está configurada en Verdadero, pero esta política está configurada en Falso, se puede leer información de los dispositivos extraíbles no descifrables, pero se bloquea el acceso de escritura a dichos dispositivos. Si la política de medios externos de cifrado está configurada en Falso, esta política no tendrá efecto y no afectará el acceso a los dispositivos extraíbles no descifrables.
Políticas de control de experiencia del usuario										
Forzar reinicio al actualizar	Verdadero								Falso	Cuando está establecido en Verdadero, el equipo se reinicia inmediatamente para permitir

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										el procesamiento del cifrado o actualizaciones relacionadas con la política basada en dispositivos, como System Data Encryption (SDE).
Duración de cada retraso del reinicio	5	10				20		15		El número de minutos de retraso cuando el usuario elige retrasar el reinicio para las políticas basadas en dispositivos.
Cantidad permitida de retrasos del reinicio	1					5		3		El número de veces que se le permitirá al usuario retrasar el reinicio para las políticas basadas en dispositivos.
Eliminar las notificaciones de contención de archivos	Falso									Esta política controla si a los usuarios se les muestran ventanas emergentes de notificación cuando las aplicaciones intenten tener acceso a un archivo mientras el cliente lo esté procesando.
Mostrar control de procesamiento de cifrado local	Falso		Verdadero					Falso		Cuando está establecido en Verdadero, el usuario visualiza una opción de menú en el icono de la bandeja del sistema que le permite pausar/reanudar el cifrado/descifrado (en función de la acción que Shield esté realizando actualmente). **NOTA: Permitir a un usuario pausar el cifrado podría autorizarle a evitar que Shield cifre o descifre datos completamente según la política.**
Permitir el procesamiento de cifrado solo cuando la pantalla está bloqueada	Falso		Opcional del usuario					Falso		Verdadero, Falso, A elección del usuario Cuando el valor esté configurado en Verdadero, no se cifrará ni descifrará la información mientras el usuario esté trabajando activamente. El cliente procesará la

Política	Protección intensa para todas las unidades fijas y externas	Regulación de PCI	Normas sobre el incumplimiento de datos	Regulación de HIPAA	Protección básica para todas las unidades fijas y externas (predeterminado)	Protección básica para todas las unidades fijas	Protección básica solo para la unidad del sistema	Protección básica de las unidades externas	Cifrado deshabilitado	Descripción
										información únicamente cuando la pantalla esté bloqueada. El valor A elección del usuario agrega una opción al icono de bandeja del sistema, al permitir al usuario activar o desactivar esta función. Cuando el valor esté configurado en Falso, el proceso de cifrado se llevará a cabo en cualquier momento, incluso cuando el usuario esté trabajando. Habilitar esta opción prolongará significativamente la cantidad de tiempo que llevará completar el cifrado o descifrado.

Descripción de plantillas

Protección intensa para todas las unidades fijas y externas

Esta plantilla de políticas está diseñada para organizaciones cuyo objetivo principal es la implementación de medidas de seguridad firmes y la prevención de riesgos en toda la empresa. Ofrece mayor utilidad cuando la seguridad es más importante que la facilidad de uso, así como cuando hay una menor necesidad de contar con excepciones de políticas seguras para usuarios, grupos o dispositivos específicos.

Esta plantilla de políticas incluye:

- configuración de alta restricción que suministra una mayor protección.
- protección para la unidad del sistema y todas las unidades fijas.
- cifrado de todos los datos de los dispositivos de almacenamiento extraíble, así como restricción de uso de aquellos que no estén cifrados.
- funcionalidad de solo lectura de controles de unidades ópticas.

Orientada a la conformidad con las regulaciones PCI

El Payment Card Industry Data Security Standard (Estándar de Seguridad de los datos de la Industria de las Tarjetas de Pago - PCI DSS) es un estándar polifacético de seguridad que incluye requisitos para el control de la seguridad, políticas, procedimientos, arquitecturas de red, diseño de software y otras medidas cruciales de protección. Esta exhaustiva norma tiene el propósito de contribuir a la inclusión de pautas para que las organizaciones protejan de manera proactiva los datos de las cuentas de sus clientes.

Esta plantilla de políticas incluye:

protección para la unidad del sistema y todas las unidades fijas.
pide a los usuarios que cifren los dispositivos de almacenamiento extraíble.
escritura de CD y DVD (UDF únicamente). La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Orientada a la conformidad con las regulaciones sobre el incumplimiento de datos

La ley Sarbanes-Oxley exige controles adecuados a la información financiera. Como mucha de dicha información existe en formatos electrónicos, el cifrado es un punto clave de control cuando dicha información se almacena o transfiere. Las directrices de la ley Gramm-Leach-Bliley (GLB) (también conocida como la Ley de Modernización de los Servicios Financieros) no exigen el cifrado. Sin embargo, el Federal Financial Institutions Examination Council (Consejo Federal de Investigaciones de las Instituciones Financieras - FFIEC) recomienda que "las instituciones financieras deben utilizar el cifrado para mitigar el riesgo de divulgación y/o alteración de información restringida, en el almacenamiento y en el tránsito". El proyecto de ley 1386 del Senado de California (Ley de California de Notificaciones de Violaciones de la Seguridad de las Bases de Datos) busca proteger del robo de identidad a los residentes de California, al exigir a las organizaciones que hayan sufrido violaciones de la seguridad de sus sistemas de computación que deben informar a todas las personas afectadas. La única manera de que las organizaciones puedan dejar de notificar a sus clientes es que puedan demostrar que toda la información personal estaba cifrada antes de que ocurriese el incumplimiento.

Esta plantilla de políticas incluye:

protección para la unidad del sistema y todas las unidades fijas.
pide a los usuarios que cifren los dispositivos de almacenamiento extraíble.
escritura de CD y DVD (UDF únicamente). La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Orientada a la conformidad con las regulaciones HIPAA

La ley HIPAA de Contratación y Responsabilidad en los Seguros de Salud establece que las organizaciones de cuidados médicos deben implementar varios mecanismos técnicos a fin de proteger la confidencialidad y la integridad de toda información relativa a la salud que pueda ser asociada a personas en particular.

Esta plantilla de políticas incluye:

protección para la unidad del sistema y todas las unidades fijas.
pide a los usuarios que cifren los dispositivos de almacenamiento extraíble.
escritura de CD y DVD (UDF únicamente). La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Protección básica para todas las unidades fijas y externas (predeterminada)

Esta plantilla de políticas ofrece la configuración recomendada, ya que garantiza un alto nivel de protección sin tener un impacto importante en la facilidad de uso del sistema.

Esta plantilla de políticas incluye:

protección para la unidad del sistema y todas las unidades fijas.
pide a los usuarios que cifren los dispositivos de almacenamiento extraíble.
escritura de CD y DVD (UDF únicamente). La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Protección básica para todas las unidades fijas

Esta plantilla de políticas incluye:

protección para la unidad del sistema y todas las unidades fijas.

escritura de CD y DVD en cualquier formato compatible. La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Esta plantilla de políticas no incluye:

cifrado para dispositivos de almacenamiento extraíble.

Protección básica solo para la unidad del sistema

Esta plantilla de políticas incluye:

protección para la unidad del sistema (por lo general, la unidad C, en donde se halla instalado el sistema operativo).

escritura de CD y DVD en cualquier formato compatible. La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Esta plantilla de políticas no incluye:

cifrado para dispositivos de almacenamiento extraíble.

Protección básica de las unidades externas

Esta plantilla de políticas incluye:

protección para dispositivos de almacenamiento extraíble.

escritura de CD y DVD (UDF únicamente). La configuración de control de puertos permite la lectura de todas las unidades ópticas.

Esta plantilla de políticas no incluye:

protección para la unidad del sistema (por lo general, la unidad C, en donde se halla instalado el sistema operativo) u otras unidades fijas.

Cifrado deshabilitado

Esta plantilla de políticas no suministra protección mediante cifrado. Si se utiliza esta plantilla, se deben tomar medidas adicionales a fin de proteger contra pérdidas y hurtos a los dispositivos.

Esta plantilla es útil para las organizaciones que prefieren comenzar sin ningún cifrado en el proceso de transición a la seguridad sistémica. A medida que se sienta mayor seguridad en cuanto a la implementación, se podrá habilitar el cifrado por etapas mediante la configuración de políticas específicas o el uso de otras plantillas integrales parcial o totalmente en la organización.

Continúe con Configuración previa a la instalación para la contraseña de un solo uso.

10

Configuración previa a la instalación para la contraseña de un solo uso

Estas funciones de Personal Edition requieren que se realice una configuración **antes** de proceder con la instalación.

Inicialización del TPM

- Deberá ser miembro del grupo de administradores locales, o de otro equivalente.
- El equipo debe tener un TPM y un BIOS compatibles.

Esta tarea es necesaria si usa la Contraseña de un solo uso (OTP).

- Siga las instrucciones que se encuentran en http://technet.microsoft.com/en-us/library/cc753140.aspx.

Extracción de instaladores secundarios del instalador maestro

- Para instalar cada cliente de manera individual, extraiga los archivos secundarios ejecutables del instalador.
- Si el instalador maestro ha sido utilizado para instalar, se deben desinstalar los clientes de manera individual. Utilice este proceso para extraer los clientes del instalador maestro con el fin de poder utilizarlos para la desinstalación.

1 Desde el medio de instalación de Dell, copie el archivo `DDPSetup.exe` al equipo local.

2 Abra un símbolo del sistema en la misma ubicación en la que está el archivo `DDPSetup.exe` e introduzca:

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

La ruta de acceso de extracción no puede superar los 63 caracteres.

Antes de iniciar la instalación, asegúrese de que se cumplen todos los requisitos previos y que todo el software necesario está instalado para cada instalador secundario que planea instalar. Consulte Requisitos para obtener más detalles.

Los instaladores secundarios extraídos están ubicados en **C:\extracted\.**

Continúe con Solución de problemas.

Solución de problemas

Realización de la actualización de aniversario de Windows 10

Los equipos instalados con Cifrado deben utilizar un paquete de actualización de Windows 10 especialmente configurado para realizar la actualización de aniversario de Windows 10. La versión configurada del paquete de actualización garantiza que Dell Data Protection pueda administrar el acceso a los archivos cifrados para protegerlos de cualquier daño durante el proceso de actualización.

Para actualizar a la versión de aniversario de Windows 10, siga las instrucciones en el siguiente artículo:

http://www.dell.com/support/article/us/en/19/SLN298382

Solución de problemas de los clientes Encryption

Realizar la actualización de aniversario de Windows 10

Para realizar la actualización de aniversario de Windows 10, siga las instrucciones en el siguiente artículo: http://www.dell.com/support/article/us/en/19/SLN298382.

(Opcional) Creación de un archivo de registro de Encryption Removal Agent

- Antes de iniciar el proceso de desinstalación, se puede como opción crear un archivo de registro de Encryption Removal Agent. Este archivo de registro es útil para el diagnóstico de errores de las operaciones de desinstalación/descifrado. No necesita crear este archivo de registro si no desea descifrar los archivos durante el proceso de desinstalación.
- No se crea el archivo de registro de Encryption Removal Agent hasta después de que el servicio de Encryption Removal Agent se haya ejecutado, lo que ocurre después de reiniciar el equipo. Se eliminará permanentemente el archivo de registro, una vez que el cliente esté totalmente desinstalado y el equipo totalmente descifrado.
- La ruta de acceso del archivo de registro es C:\ProgramData\Dell\Dell Data Protection\Encryption.
- Cree la siguiente entrada de registro en el equipo destinado para el descifrado.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: sin registros

  1: registra errores que evitan la ejecución del servicio

  2: registra errores que evitan el descifrado de datos completo (nivel de inicio de sesión recomendado)

  3: registra la información relacionada con todos los volúmenes y archivos de descifrado

  5: registra la información de depuración

Búsqueda de versión TSS

- TSS es un componente que funciona como interfaz con TPM. Para encontrar la versión TSS, vaya a (ubicación predeterminada) **C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe**. Haga clic con el botón derecho del mouse y seleccione **Propiedades**. Compruebe la versión del archivo en la pestaña **Detalles**.

Interacciones entre EMS y PCS

Asegurarse de que los medios no sean de Solo lectura y de que el puerto no esté bloqueado.

La política de Acceso EMS a medios no protegidos por Shield interactúa con el Sistema de control de puertos -política Clase de almacenamiento: Control de unidad externa. Si desea configurar el Acceso EMS a medios no protegidos por Shield como *Acceso total*, asegúrese de que la política Clase de almacenamiento: Control de unidad externa también está establecida como *Acceso total* para asegurarse de que los medios no estén establecidos en Solo lectura y de que el puerto no esté bloqueado.

Cifrar datos de escritura en medios de CD/DVD:

- Establecer EMS - Cifrar medios externos = Verdadero.
- Establecer EMS - Excluir cifrado de CD/DVD = Falso
- Establecer subclase de almacenamiento: Control de unidad óptica = Solo UDF.

Uso de WSScan

- WSScan le permite asegurarse de que todos los datos se descifran al desinstalar el cliente Encryption, así como ver el estado de cifrado e identificar los archivos no cifrados que se deben cifrar.
- Se requieren privilegios de administrador para ejecutar esta utilidad.

Ejecutar WSScan

1. Desde el medio de instalación de Dell, copie WSScan.exe en el equipo de Windows que desea explorar.
2. Inicie la línea de comandos en la ubicación anterior e introduzca **wsscan.exe** en el símbolo del sistema. Se inicia WSScan.
3. Haga clic en **Avanzado**.
4. Seleccione el tipo de unidad que desea explorar desde el menú desplegable: *Todas las unidades, Unidades fijas, Unidades extraíbles o CD-ROM/ DVD-ROM*.
5. Seleccione el tipo de informe de Encryption en el menú desplegable: *archivos cifrados*, *archivos sin cifrar*, *todos los archivos* o *archivos sin cifrar en infracción*:
   - *Archivos cifrados*: para garantizar que todos los datos se descifran cuando se desinstala el cliente Encryption. Siga el actual proceso para el descifrado de datos, como la emisión de la actualización de una política de descifrado. Después de descifrar los datos, pero antes de proceder al reinicio para la desinstalación, ejecute WSScan a fin de asegurarse de que todos los datos hayan sido descifrados.
   - *Archivos no cifrados*: para identificar archivos que no están cifrados, con una indicación de si los archivos se deben cifrar (Y/N).
   - *Todos los archivos*: para generar una lista de todos los archivos cifrados y no cifrados, con una indicación de si los archivos se deben cifrar (Y/N).
   - *Archivos sin cifrar en infracción*: para identificar los archivos que no están cifrados y se deben cifrar.
6. Haga clic en **Buscar**.

O bien

1. Haga clic en **Avanzado** para cambiar la vista a **Simple** para explorar una carpeta específica.
2. Vaya a Configuración de exploración e introduzca la ruta de acceso de la carpeta en el campo **Ruta de búsqueda**. Si se utiliza este campo, se ignora la selección realizada en el cuadro desplegable.
3. Si no desea escribir la salida de WSScan en un archivo, desactive la casilla de verificación **Salida a archivo**.

4 Cambie la ruta de acceso y el nombre de archivo predeterminados en *Ruta de acceso*, si lo desea.

5 Seleccione **Agregar a archivo existente** si no desea sobrescribir ningún archivo de salida de WSScan existente.

6 Seleccione el formato de salida:

- Seleccione Formato del informe para ver una lista de estilos de informe de la salida de la exploración. Este es el formato predeterminado.
- Seleccione Archivo delimitado por valor para obtener un archivo de salida que se pueda importar en una aplicación de hoja de cálculo. El delimitador predeterminado es "|", aunque se puede cambiar a un máximo de nueve caracteres alfanuméricos, espacios o caracteres de puntuación disponibles en el teclado.
- Seleccione la opción Valores entre comillas para delimitar cada uno de los valores con comillas dobles.
- Seleccione Archivo de ancho fijo para obtener un archivo de salida no delimitado que contenga una línea continua de información de ancho fijo acerca de cada uno de los archivos cifrados.

7 Haga clic en **Buscar**.

Haga clic en **Detener búsqueda** para detener la búsqueda. Haga clic en **Borrar** para borrar los mensajes mostrados.

Salida de WSScan

La información de WSScan acerca de los archivos cifrados contiene los siguientes datos.

Ejemplo de salida:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" todavía está cifrado según AES256

Salida	Significado
Sello con la fecha/hora	La fecha y la hora en la que se exploró el archivo.
Tipo de cifrado	El tipo de cifrado utilizado para cifrar el archivo. **SysData:** clave de cifrado de SDE. **Usuario:** clave de cifrado de Encryption. **Común:** clave de cifrado común. WSScan no informa archivos cifrados mediante Encrypt for Sharing.
KCID	La Id. de equipo clave Como se muestra en el ejemplo anterior, "**7vdlxrsb**" Si se exploró una unidad de red asignada, el informe de exploración no proporciona una KCID.
UCID	La Id. del usuario. Como se muestra en el ejemplo anterior, "**_SDENCR_**" La UCID la comparten todos los usuarios de ese equipo.
Archivo	La ruta de acceso del archivo cifrado. Como se muestra en el ejemplo anterior, "**c: \temp\Dell: test.log**"
Algoritmo	El algoritmo de cifrado utilizado para cifrar el archivo. Como se muestra en el ejemplo anterior, "**todavía está cifrado según AES256**" RIJNDAEL 128 RIJNDAEL 256

Salida	Significado
	AES 128
	AES 256
	3DES

Comprobación del estado de Encryption Removal Agent

Encryption Removal Agent muestra su estado en el área de descripción del panel Servicios (Inicio > Ejecutar... > Services.msc > Aceptar) como se indica a continuación. Actualice el Servicio de forma periódica (seleccione Servicio > haga clic con el botón derecho del mouse > Actualizar) para actualizar el estado.

- **En espera de desactivación de SDE**: el cliente Encryption aún está instalado, configurado, o ambos. El descifrado no se inicia hasta que el cliente Encryption se haya desinstalado.
- **Barrido inicial**: el servicio está realizando un barrido inicial, calculando el número de archivos cifrados y los bytes. El barrido inicial se produce una sola vez.
- **Barrido de descifrado**: el servicio está descifrando archivos y posiblemente solicitando el descifrado de archivos bloqueados.
- **Descifrar al reiniciar (parcial)**: el barrido de descifrado ha terminado y en el próximo reinicio se descifrarán algunos archivos (no todos) bloqueados.
- **Descifrar al reiniciar**: el barrido de descifrado ha terminado y todos los archivos bloqueados se descifrarán en el próximo reinicio.
- **No se han podido descifrar todos los archivos**: el barrido de descifrado ha terminado pero no se han podido descifrar todos los archivos. Este último estado significa que ocurrió una de las siguientes situaciones:
  - No se pudo programar el descifrado de los archivos bloqueados porque eran demasiado grandes, o porque se produjo un error al hacer la solicitud de desbloqueo.
  - Se produjo un error entrada/salida durante el cifrado de los archivos.
  - No se pudieron descifrar los archivos debido a una política.
  - Los archivos están marcados como deben ser cifrados.
  - Se produjo un error durante el barrido de descifrado.
  - Cualquiera que sea el caso, se crea un archivo de registro (si llevar un registro está configurado) cuando la configuración sea LogVerbosity=2 (o superior). Para solucionar problemas, configure LogVerbosity en 2 y reinicie Encryption Removal Agent Service a fin de forzar otro barrido de descifrado.
- **Completado**: el barrido de descifrado se ha completado. El Servicio, el ejecutable, el controlador y el ejecutable del controlador están programados para ser eliminados en el siguiente reinicio.

Cómo cifrar un iPod con EMS

Estas reglas deshabilitan o habilitan el cifrado para estas carpetas y tipos de archivo, para todos los dispositivos extraíbles, no solo los iPod. Tenga cuidado al definir las reglas.

- No recomendamos el uso de dispositivos iPod Shuffle ya que podrían ocurrir resultados inesperados.
- A medida que los dispositivos iPod cambien, es posible que esta información también cambie, por lo que debe tener precaución al permitir el uso de dispositivos iPod en equipos con cifrado EMS habilitado.
- Debido a que los nombres de las carpetas en los iPods dependen del modelo de iPod en particular, recomendamos crear una política de exclusión que cubra todos los nombres de carpetas en todos los modelos de iPod.
- Para garantizar que el cifrado de un iPod mediante EMS no haga que el dispositivo sea inutilizable, aplique las siguientes reglas en la política de reglas de cifrado de EMS:

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

-R#:\Notes

-R#:\Photos

- También puede forzar el cifrado de tipos específicos de archivos en los directorios anteriores. Al agregar las siguientes reglas, se garantiza que se cifren los archivos ppt, pptx, doc, docx, xls y xlsx en los directorios *excluidos* del cifrado, según las reglas anteriores:

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- Reemplazar las cinco reglas anteriores con la siguiente forzará el cifrado de los archivos ppt, pptx, doc, docx, xls y xlsx que se encuentren en todos los directorios del iPod, incluso los directorios Calendars, Contacts, iPod_Control, Notes y Photos:

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- Las reglas anteriores han sido probadas con estos iPod:

  iPod Video 30 GB de quinta generación

  iPod Nano 2 GB de segunda generación

  iPod Mini 4 GB de segunda generación

Controladores Dell ControlVault

Actualización del firmware y de los controladores Dell ControlVault

El firmware y los controladores Dell ControlVault instalados en fábrica en los equipos Dell son obsoletos y necesitan ser actualizados siguiendo este procedimiento, en el orden indicado.

Si recibe un mensaje de error durante la instalación del cliente pidiéndole que salga del instalador para actualizar los controladores Dell ControlVault, puede ignorar tranquilamente el mensaje y continuar con la instalación del cliente. Los controladores Dell ControlVault (y el firmware) pueden ser actualizados una vez finalizada la instalación del cliente.

Descarga de los controladores más recientes

1. Vaya a support.dell.com.
2. Seleccione el modelo del equipo.
3. Seleccione **Controladores y descargas**.
4. Seleccione el **Sistema operativo** del equipo de destino.
5. Expanda la categoría **Seguridad**.
6. Descargue y guarde los controladores Dell ControlVault.
7. Descargue y guarde el firmware Dell ControlVault.
8. Si es necesario, copie el firmware y los controladores en los equipos de destino.

Instalación del controlador Dell ControlVault

Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del controlador.

Haga doble clic sobre el controlador Dell ControlVault para iniciar el archivo ejecutable autoextraíble.

:

Asegúrese de instalar primer el controlador. El nombre de archivo del controlador *tal como era cuando se creó este documento* es ControlVault_Setup_2MYJC_A37_ZPE.exe.

Haga clic en **Continuar** para empezar.

Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada C:\Dell\Drivers\<Nueva carpeta>

Haga clic en **Sí** para permitir la creación de una nueva carpeta.

Haga clic en **Aceptar** cuando aparezca el mensaje correctamente descomprimido.

Tras la extracción, debería aparecer la carpeta que contiene los archivos. Si no aparece, vaya hasta la carpeta en la que haya extraído los archivos. En este caso, la carpeta es **JW22F**.

Haga doble clic sobre **CVHCI64.MSI** para iniciar el instalador del controlador. [este ejemplo es **CVHCI64.MSI** en este ejemplo (CVHCI para un equipo de 32 bits)].

Haga clic en **Siguiente** en la pantalla de bienvenida.

Haga clic en **Siguiente** para instalar los controladores en la ubicación predeterminada C:\Program Files\Broadcom Corporation \Broadcom USH Host Components\.

Seleccione la opción **Completar** y haga clic en **Siguiente**

Haga clic en **Instalar** para empezar la instalación de los controladores.

De forma opcional, puede marcar la casilla de verificación para ver el archivo de registro del instalador. Haga clic en **Finalizar** para salir del asistente.

Comprobación de la instalación del controlador

Device Manager tendrá un dispositivo Dell ControlVault (y otros dispositivos) dependiendo de la configuración del hardware y del sistema operativo.

Instalación del firmware Dell ControlVault

1 Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del firmware.

2 Haga doble clic sobre el firmware Dell ControlVault para iniciar el archivo ejecutable autoextraíble.

3 Haga clic en **Continuar** para empezar.

4 Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada C:\Dell\Drivers\<Nueva carpeta>

5 Haga clic en **Sí** para permitir la creación de una nueva carpeta.

6 Haga clic en **Aceptar** cuando aparezca el mensaje correctamente descomprimido.

7 Tras la extracción, debería aparecer la carpeta que contiene los archivos. Si no aparece, vaya hasta la carpeta en la que haya extraído los archivos. Seleccione la carpeta **firmware**.

8 Haga doble clic en **ushupgrade.exe** para iniciar el instalador de firmware.

9 Haga clic en **Iniciar** para empezar la actualización del firmware.

:

Si está realizando la actualización desde una versión de firmware más antigua, es posible que necesite introducir su contraseña de administrador. Introduzca `Broadcom` como contraseña y haga clic en **Intro** si aparece este diálogo.

Aparecerán varios mensajes de estado.

10 Haga clic en **Reiniciar** para finalizar la actualización del firmware.

Ha finalizado la actualización del firmware y de los controladores Dell ControlVault.

Configuración de registro

Esta sección detalla toda la configuración de registro aprobada por Dell ProSupport para equipos cliente locales.

Cliente Encryption

(Opcional) Creación de un archivo de registro de Encryption Removal Agent

Antes de iniciar el proceso de desinstalación, se puede como opción crear un archivo de registro de Encryption Removal Agent. Este archivo de registro es útil para el diagnóstico de errores de las operaciones de desinstalación/descifrado. No necesita crear este archivo de registro si no desea descifrar los archivos durante el proceso de desinstalación.

No se crea el archivo de registro de Encryption Removal Agent hasta después de que el servicio de Encryption Removal Agent se haya ejecutado, lo que ocurre después de reiniciar el equipo. Se eliminará permanentemente el archivo de registro, una vez que el cliente esté totalmente desinstalado y el equipo totalmente descifrado.

La ruta de acceso del archivo de registro es **C:\ProgramData\Dell\Dell Data Protection\Encryption.**

Cree la siguiente entrada de registro en el equipo destinado para el descifrado.

[HKLM\Software\Credant\DecryptionAgent]

"LogVerbosity"=dword:2

0: sin registros

1: registra errores que evitan la ejecución del servicio

2: registra errores que evitan el descifrado de datos completo (nivel de inicio de sesión recomendado)

3: registra la información relacionada con todos los volúmenes y archivos de descifrado

5: registra la información de depuración

Uso de tarjetas inteligentes con autenticación de Windows.

Para utilizar tarjetas inteligentes con autenticación de Windows, el valor de registro siguiente debe estar establecido en el equipo cliente.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Conservación de archivos temporales durante la instalación

De forma predeterminada, todos los archivos temporales del directorio c:\windows\temp se eliminan automáticamente durante la instalación. La eliminación de los archivos temporales acelera el cifrado inicial y se produce antes del barrido de cifrado inicial.

No obstante, si su organización utiliza aplicaciones de terceros que requieren que se conserve la estructura de archivos contenida en el directorio \temp, no se debe realizar dicha eliminación.

Para deshabilitar la eliminación de archivos temporales, cree o modifique la configuración de registro de la siguiente forma:

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

No eliminar los archivos temporales aumenta el tiempo de cifrado inicial.

Cambio del comportamiento predeterminado de la petición del usuario para iniciar o retrasar el cifrado.

El cliente Encryption muestra el indicador de `duración de cada retraso de actualización de política` durante cinco minutos cada vez. Si el usuario no responde a la indicación, comenzará el siguiente retraso. La indicación de retraso final incluye una

cuenta atrás y una barra de progreso, y se visualiza hasta que el usuario responde o el retraso final caduca y se produce el cierre de sesión/reinicio requerido.

Puede cambiar el comportamiento de la indicación al usuario para iniciar o retrasar el cifrado, para evitar el procesamiento del cifrado cuando el usuario no responda a la indicación. Para ello, establezca el registro en el siguiente valor:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Cualquier valor distinto de cero cambiará el comportamiento predeterminado a postergar. Si no se produce ninguna interacción del usuario, se retrasará el procesamiento del cifrado hasta la cantidad configurable de retrasos permitidos. El procesamiento del cifrado se inicia una vez caducado el retraso final.

Calcule el máximo retraso posible del siguiente modo (un retraso máximo implicaría que el usuario responda a una indicación de retraso, que se muestra durante 5 minutos):

(CANTIDAD PERMITIDA DE RETRASOS DE LA ACTUALIZACIÓN DE LA POLÍTICA + DURACIÓN DE CADA RETRASO DE ACTUALIZACIÓN DE LA POLÍTICA) + (5 MINUTOS x [CANTIDAD PERMITIDA DE RETRASOS DE LA ACTUALIZACIÓN DE LA POLÍTICA - 1])

Cambio del uso predeterminado de la clave SDUser

El Cifrado de datos del sistema (SDE) se exige según el valor de la política para las Reglas del cifrado de SDE. Cuando se selecciona la política de Cifrado de SDE habilitado, se protegen otros directorios de forma predeterminada. Para obtener más información, busque "Reglas de Cifrado de SDE" en AdminHelp. Cuando el cliente Encryption está procesando una actualización de la política que incluye una política de SDE activa, se cifra de forma predeterminada el directorio del perfil del usuario actual con la clave SDUser (una clave de usuario), en lugar de hacerlo con la clave SDE (una clave de dispositivo). La clave SDUser también se utiliza para cifrar los archivos o carpetas que se hayan copiado (no trasladado) a un directorio de usuarios que no esté cifrado con SDE.

Para deshabilitar la clave SDUser y utilizar la clave SDE con el fin de cifrar estos directorios de usuarios, cree la siguiente entrada de registro en el equipo:

[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

"EnableSDUserKeyUsage"=dword:00000000

Si esta clave de registro no está presente o se establece un valor distinto de 0, la clave SDUser se utilizará para cifrar estos directorios de usuarios.

Cliente Advanced Authentication

Deshabilitación de Servicios biométricos y tarjetas inteligentes (opcional)

Si no desea que Security Tools cambie los servicios asociados a las tarjetas inteligentes y los dispositivos biométricos a un tipo de inicio "automático", puede deshabilitar la función de inicio del servicio.

Cuando esté deshabilitado, Security Tools no tratará de iniciar estos tres servicios:

SCardSvr: administra el acceso a las tarjetas inteligentes leídas por el equipo. Si el servicio se detiene, el equipo no podrá leer tarjetas inteligentes. Si el servicio se deshabilita, no podrán iniciarse los servicios que dependan explícitamente de él.

SCPolicySvc: permite que el sistema se configure para bloquear el escritorio del usuario cuando se retire la tarjeta inteligente.

WbioSrvc: el servicio biométrico de Windows otorga a las aplicaciones de cliente la capacidad de capturar, comparar, manipular y almacenar datos biométricos sin obtener acceso directo a ningún hardware o muestras biométricos. El servicio está alojado en un proceso SVCHOST privilegiado.

La deshabilitación de esta función también suprime los avisos asociados con el mal funcionamiento de los servicios necesarios.

De manera predeterminada, si la clave de registro no existe o si el valor está establecido en 0, se habilita esta función.

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Establezca en 0 para habilitar.

Establezca en 1 para Deshabilitar.

Uso de tarjetas inteligentes con autenticación de Windows.

Para utilizar tarjetas inteligentes con autenticación de Windows, el valor de registro siguiente debe estar establecido en el equipo cliente.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Continúe con Glosario.

13

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.

Contraseña de administrador de cifrado (EAP): la EAP es una contraseña administrativa que es exclusiva para cada equipo. La mayoría de los cambios de configuración que se hacen en la Local Management Console requieren de esta contraseña. Además, es la misma que necesitaría si tiene que utilizar su archivo LSARecovery_[nombre de host].exe para recuperar sus datos. Anote y guarde esta contraseña en un lugar seguro.

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.

Claves de cifrado: en la mayoría de los casos, el cliente Encryption utiliza la clave de usuario más dos claves de cifrado adicionales. Sin embargo, hay excepciones: todas las políticas de SDE y la política Proteger credenciales de Windows utilizan la clave de SDE. La política Cifrar archivo de paginación de Windows y Proteger archivo de hibernación de Windows utilizan su propia clave, la Clave de propósito general (GPK). La clave Común permite que todos los usuarios administrados tengan acceso a los archivos en el dispositivo en el que fueron creados. La clave Usuario determina que solo tenga acceso a los archivos la persona que los crea, únicamente en el dispositivo en el que hayan sido creados. La clave Usuario en roaming da acceso a los archivos solo a la persona que los crea, en cualquier dispositivo Windows (o Mac) protegido por Shield.

Barrido de cifrado: un barrido de cifrado es el proceso de explorar las carpetas que se vayan a cifrar en un extremo protegido por Shield 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, algoritmos de cifrado, uso de claves de cifrado (común con usuario), desencadenará 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.

Autenticación previa al inicio (PBA): la autenticación previa al inicio sirve como una extensión del BIOS o del firmware de arranque y garantiza un entorno seguro, a prueba de manipulaciones y externo al sistema operativo como un nivel de autenticación fiable. La PBA impide la lectura de la unidad de disco duro, incluido el sistema operativo, hasta que el usuario haya confirmado que tiene las credenciales correctas.

Inicio de sesión único (SSO): El inicio de sesión único simplifica el proceso de inicio de sesión cuando está habilitada la autenticación multifactor tanto antes del arranque como al inicio de sesión en Windows. Si está habilitada, la autenticación se requiere solo en el preinicio, y los usuarios inician sesión en Windows automáticamente. Si está deshabilitada, la autenticación puede requerirse varias veces.

System Data Encryption (SDE): el SDE está diseñado para cifrar el sistema operativo y los archivos de programa. Para cumplir con este propósito, SDE debe poder abrir su clave mientras se inicia el sistema operativo. La finalidad de este requisito es evitar que el sistema operativo quede expuesto a alteraciones o ataques perpetrados por piratas informáticos. SDE no está desarrollado para proteger datos de usuario. Los procesos de cifrado común y de usuario están pensados para proteger información de usuarios que se considera confidencial, ya que particular, exigen una contraseña de usuario para efectuar el desbloqueo de las claves de cifrado. Las políticas de SDE no cifran los archivos que necesita el sistema operativo para el proceso de inicio. Las políticas de SDE no requieren de autenticación antes del inicio ni interfieren de manera alguna con el registro de inicio maestro. Cuando el equipo arranca, los archivos cifrados están disponibles antes del inicio de sesión de los usuarios (a fin de activar la administración de revisiones, SMS y las herramientas de copias de seguridad y de recuperación). La deshabilitación del cifrado SDE desencadena el descifrado automático de todos los archivos y directorios cifrados de SDE de los usuarios correspondientes, sin tener en cuenta las otras políticas de SDE, como las Reglas de cifrado de SDE

Trusted Platform Module (TPM): el TPM es un chip de seguridad que cumple tres funciones importantes: atestación, medición y almacenamiento seguro. El cliente Encryption utiliza el TPM por su función de almacenamiento seguro. El TPM también sirve para proporcionar contenedores cifrados al almacén de software. El TPM también es necesario para utilizarlo con la función de Contraseña de un solo uso.