Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Notas, precauciones y advertencias

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

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Contents

1

Descripción general

En esta guía, se presume que Advanced Authentication se instalará junto con Encryption Personal.

Encryption Personal

El objetivo de Encryption Personal es proteger los datos de su computadora, incluso si se roban el equipo o se pierde.

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

Advanced Authentication

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

Consulte Configurar los valores de administrador de Advanced Authentication y consulte *Dell Data Security Console User Guide* (Guía de usuario de la consola de Dell Data Security) para obtener información sobre el uso de Advanced Authentication.

Comuníquese con el equipo de Dell ProSupport for Software

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

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

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

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

2

Requisitos

Estos requisitos describen todo lo necesario para la instalación de Encryption Personal.

Cifrado

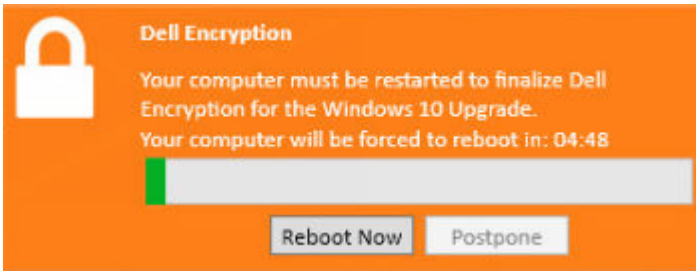
- Encryption Personal requiere autorización para que se instale correctamente. La autorización se ofrece al comprar Encryption Personal. Según cómo adquiera Encryption Personal, es posible que instale manualmente la autorización, utilizando las instrucciones simples que la acompañan. También puede escribir la autorización en la línea de comandos. Si Encryption Personal se instaló utilizando el servicio Dell Digital Delivery, dicho servicio se encarga de la instalación de la autorización. (Se utilizan los mismos binarios para Encryption Enterprise y Encryption Personal. La autorización indica al instalador qué versión deberá instalar).
- Las cuentas de Microsoft y Office 365 se admiten cuando se ejecuta Encryption Personal v11.0 o una versión posterior en Windows 10.
- Para activar una cuenta Microsoft Live con Encryption Personal, consulte el artículo de la base de conocimientos 124722.
- Se requiere una contraseña de Windows (si 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. Encryption Personal no se activará si no se crea una contraseña.
- Dell Encryption no se puede actualizar a las versiones v10.7.0 desde versiones anteriores a v8.16.0. Los terminales con versiones anteriores a v8.16.0 se deben actualizar a v8.16.0 y, luego, a las versiones v10.7.0.
- Dell Encryption utiliza los conjuntos de instrucción de cifrado de Intel, Integrated Performance Primitives (IPP). Para obtener más información, consulte el artículo de la base de conocimientos 126015.

1. Vaya al Panel de control de Windows (**Inicio** > **Panel de control**).
2. Haga clic en el ícono **Cuentas de usuarios**.
3. Haga clic en **Crear una contraseña para su cuenta**.
4. Introduzca una nueva contraseña y su confirmación.
5. Si lo desea, escriba una pista para la contraseña.
6. Haga clic en **Crear contraseña**.
7. 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, el cual se puede designar temporalmente mediante una herramienta de implementación como Microsoft SMS. 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 en 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, comuníquese 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 Encryption en una imagen corporativa, consulte el artículo de la base de conocimientos 129990.
- El TPM se usa para sellar la clave de finalidad general. Por lo tanto, si ejecuta el cliente Encryption, borre el TPM en el BIOS antes de instalar un sistema operativo nuevo en la computadora de destino.

- El cliente Encryption es compatible y se prueba con varios antivirus basados en firmas y las soluciones antivirus impulsadas por IA, en las que se incluyen McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense y varias otras. Para muchos antivirus, se incluyen exclusiones codificadas por hardware de forma predeterminada para evitar incompatibilidades entre el escaneo del antivirus y el cifrado.

  Si la organización utiliza un proveedor de antivirus que no está en la lista o si observa cualquier problema de compatibilidad, consulte el artículo de la base de conocimientos 126046 o comuníquese con Dell ProSupport para obtener asistencia y validar la configuración de la interoperabilidad entre las soluciones de software y las soluciones de Dell Data Security.
- 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 revisar periódicamente dell.com/support para obtener la documentación y la asesoría técnica más recientes.
- Después de la actualización de funciones de Windows 10, se **debe** reiniciar para finalizar Dell Encryption. El siguiente mensaje se muestra en el área de notificación después de las actualizaciones de funciones de Windows 10:



Requisitos previos

- Se necesita Microsoft .Net Framework 4.5.2 (o posterior) para los instaladores maestro y secundario. El instalador no instala el componente de Microsoft .Net Framework.

  NOTA: Se necesita .Net Framework 4,6 (o posterior) cuando se está ejecutando el modo FIPS.

- El instalador maestro instala los siguientes requisitos previos si todavía no se encuentra instalado en la computadora. **Cuando utiliza el instalador secundario**, debe instalar este componente antes de Encryption.

Requisito previo
○ Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 o x64) ○ Paquete redistribuible Visual C++ 2017 actualización 3 o posterior (x86 o x64) ○ Si no se instalan estas actualizaciones, las aplicaciones y los paquetes de instalación firmados con certificados SHA1 funcionarán, pero se mostrará un error en el terminal durante la instalación o la ejecución de la aplicación

Hardware

- En la siguiente tabla se indica el hardware mínimo de computadora compatible.

Hardware
○ Procesador Intel Pentium o AMD ○ 110 MB de espacio disponible en el disco ○ 512 MB de RAM **NOTA:** Se necesita espacio libre adicional en el disco para cifrar los archivos en el extremo. Este tamaño varía según las políticas y la capacidad de la unidad.

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

Hardware integrado opcional
○ TPM 1.2 o 2.0

Sistemas operativos

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2) **Nota:** Los OEM y ODM no envían Windows 10 v2004 (actualización de mayo del 2020/20H1 y posteriores) con arquitectura de 32 bits. Para obtener más información, consulte https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2-22H2

Sistemas operativos con Encryption External Media

- El medio externo debe tener aproximadamente 55 MB disponibles, además de una cantidad de espacio libre igual al tamaño del archivo más grande que se vaya a cifrar, para alojar Encryption External Media.
- A continuación, se describen los sistemas operativos admitidos cuando se accede a medios protegidos por Dell.

Sistemas operativos Windows compatibles para el acceso a medios cifrados (32 y 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2) **Nota:** Los OEM y ODM no envían Windows 10 v2004 (actualización de mayo del 2020/20H1 y posteriores) con arquitectura de 32 bits. Para obtener más información, consulte https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2-22H2

Sistemas operativos Mac compatibles para el acceso a medios cifrados (núcleos de 64 bits)
○ macOS High Sierra 10.13.5 - 10.13.6 ○ macOS Mojave 10.14.0 - 10.14.4 ○ macOS Catalina 10.15.5 - 10.15.6

Localización

- Encryption es compatible con la interfaz de usuario multilingüe y se puede configurar en los siguientes idiomas.

Compatibilidad de idiomas	
○ Inglés (EN)	○ Japonés (JA)
○ Español (ES)	○ Coreano (KO)
○ Francés (FR)	○ Portugués brasileño (PT-BR)
○ Italiano (IT)	○ Portugués europeo (PT-PT)

Compatibilidad de idiomas	
○ Alemán (DE)	

SED Manager

- No es compatible con IPv6.
- Recuerde que deberá apagar y reiniciar el equipo después de aplicar las políticas y cuando estén listas para comenzar a aplicarlas.
- Los equipos que cuentan con unidades de cifrado automático no se pueden utilizar con tarjetas HCA. Existen incompatibilidades que impiden el aprovisionamiento del HCA. Dell no vende equipos que tengan unidades de cifrado automático compatibles con el módulo HCA. Esta configuración incompatible será una configuración realizada poscompra.
- Si el equipo marcado para cifrado incluye unidad de cifrado automático, asegúrese de que Active Directory tenga deshabilitada la opción *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*. La Autenticación previa al inicio del sistema no es compatible con esta opción de Active Directory.
- SED Manager no es compatible con configuraciones de varias unidades.
- **NOTA:**

  Debido a la naturaleza de RAID y SED, SED Manager no es compatible con RAID. El problema que presenta *RAID=On* con respecto a SED es que RAID requiere acceso al disco para leer y escribir los datos relacionados con RAID en un sector de alto nivel que no se encuentra disponible desde el inicio en un SED bloqueado, y RAID no puede esperar a leer estos datos hasta que el usuario inicie sesión. Para resolver este problema, cambie el funcionamiento de SATA en el BIOS de *RAID=On* a *AHCI*. Si el sistema operativo no tiene controladores de la controladora AHCI instalados previamente, el sistema operativo se bloqueará cuando se cambie de *RAID=On* a *AHCI*.

- El instalador maestro instala los siguientes requisitos previos si todavía no se encuentra instalado en la computadora. **Cuando utilice el instalador secundario**, debe instalar este componente antes de instalar SED Manager.

Requisito previo
○ Paquete redistribuible Visual C++ 2017 actualización 3 o posterior (x86 o x64)
○ Si no se instalan estas actualizaciones, las aplicaciones y los paquetes de instalación firmados con certificados SHA1 funcionarán, pero se mostrará un error en el terminal durante la instalación o la ejecución de la aplicación

- La configuración de unidades de autocifrado para SED Manager difiere entre las unidades NVMe y las que no son NVMe (SATA), como se indica a continuación.
  - Cualquier unidad NVMe que se use para PBA:
    - Si el dispositivo Dell se fabricó en el 2018 o después, es posible que se puedan aprovechar las opciones RAID ACTIVO o AHCI con unidades NVMe.
    - El modo de arranque del BIOS se debe establecer en Interfaz unificada extensible de firmware (UEFI). Las ROM de funcionamiento heredadas deben estar deshabilitadas.
  - Cualquier unidad distinta de NVMe que se use para PBA:
    - La operación SATA del BIOS se puede establecer en AHCI o RAID ENCENDIDO.
    - El sistema operativo se bloqueará cuando se cambie de RAID Encendido > AHCI si los controladores de la controladora AHCI no están previamente instalados. Para obtener instrucciones sobre cómo cambiar de RAID a AHCI (o viceversa), consulte el artículo de la base de conocimientos 124714.

  Las SED compatibles que cumplen con OPAL necesitan controladores actualizados Intel Rapid Storage Technology, que se pueden encontrar en www.dell.com/support. Dell recomienda el controlador de Intel Rapid Storage Technology más reciente con unidades NVMe.

  NOTA: Los controladores Intel Rapid Storage Technology dependen de la plataforma. Puede encontrar el controlador del sistema en el enlace anterior según el modelo de su computadora.

- Las configuraciones de cifrado de múltiples discos con SED Manager requieren lo siguiente:
  - Todos los discos en el sistema de destino deben ser SED.
  - Todos los discos en el sistema de destino deben estar configurados en el mismo modo de arranque.

- En el modo de arranque UEFI, el sistema operativo se puede instalar en cualquier disco de destino.
- En el modo de inicio heredado, el sistema operativo debe estar instalado en el primer disco (disco #0). Si el sistema operativo no está instalado en el primer disco, el cifrado de múltiples discos se deshabilita.

- Es posible que algunas versiones del BIOS habiliten el SID en bloques de manera predeterminada, lo que puede inhibir SED Manager. Para obtener más información, consulte el artículo 126083 de la base de conocimientos.
- Las actualizaciones de función directas de Windows 10 versión 1607 (Anniversary Update/Redstone 1) a Windows 10 versión 1903 (actualización de mayo del 2019/19H1) no son compatibles con Dell Encryption. Dell recomienda actualizar el sistema operativo a una actualización de funciones más reciente si se desea actualizar a Windows 10 versión 1903. Cualquier intento de actualización directa de Windows 10 versión 1607 a la versión 1903 mostrará un mensaje de error, y la actualización se detendrá.
- **NOTA:** Se necesita una contraseña con autenticación previa al arranque. Dell recomienda establecer una contraseña con longitud mínima de 9 caracteres o más.

- **NOTA:** Se necesita una contraseña para todos los usuarios agregados en el panel *Agregar usuario*. Los usuarios con contraseña sin longitud se bloquearán de la computadora después de la activación.
- **NOTA:** Las computadoras protegidas con SED Manager se deben actualizar a Windows 10 versión 1703 (Creators Update/Redstone 2) o posterior antes de actualizar a Windows 10 versión 1903 (actualización de mayo del 2019/19H1) o posterior. Si se intenta seguir esta ruta de actualización, aparecerá un mensaje de error.
- SED Manager requiere el uso del proveedor de credenciales personalizado de Dell para sincronizar los cambios de contraseñas de Windows y las llaves de cifrado de datos. Si necesita utilizar aplicaciones de terceros que empleen proveedores de credenciales personalizados que se ejecutan en computadoras protegidas con SED Manager, debe iniciar cambios de contraseñas de Windows mediante Data Security Console. Para obtener información sobre cómo cambiar la contraseña en Data Security Console, consulte el capítulo *Contraseña* de la Guía del usuario de Data Security Console.

Hardware

- Para obtener la lista más reciente de SED compatibles con Opal admitidos en SED Management, consulte el artículo de la base de conocimientos 126855.
- Para obtener la lista más reciente de plataformas compatibles con SED Management, consulte el artículo de la base de conocimientos 126855.
- Para obtener una lista de estaciones de acoplamiento y adaptadores compatibles con SED Manager, consulte el artículo de la base de conocimientos 124241.

Teclados internacionales

En la tabla siguiente se muestran los teclados internacionales compatibles con la autenticación previa al arranque en computadoras UEFI y distintas de UEFI.

Compatibilidad con teclado Internacional: UEFI	
DE-FR: (francés de Suiza)	EN-GB: Inglés (inglés del Reino Unido)
DE-CH: (alemán de Suiza)	EN-CA: Inglés (inglés de Canadá)
EN-US: Inglés (inglés de EE. UU.)	

Compatibilidad con teclado Internacional: Non-UEFI	
Árabe (AR) (con caracteres latinos)	EN-US: Inglés (inglés de EE. UU.)
DE-FR: (francés de Suiza)	EN-GB: Inglés (inglés del Reino Unido)
DE-CH: (alemán de Suiza)	EN-CA: Inglés (inglés de Canadá)

Sistemas operativos

- La siguiente tabla detalla los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2) **Nota:** Los OEM y ODM no envían Windows 10 v2004 (actualización de mayo del 2020/20H1 y posteriores) con arquitectura de 32 bits. Para obtener más información, consulte https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2-22H2

Las funciones de autenticación solo están disponibles cuando se activa la autenticación previa al arranque.

Localización

SED Manager es una interfaz de usuario en varios idiomas que cumple con los requisitos del sector y se puede configurar en los siguientes idiomas. Se admite el modo UEFI y la autenticación previa al arranque en los siguientes idiomas:

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

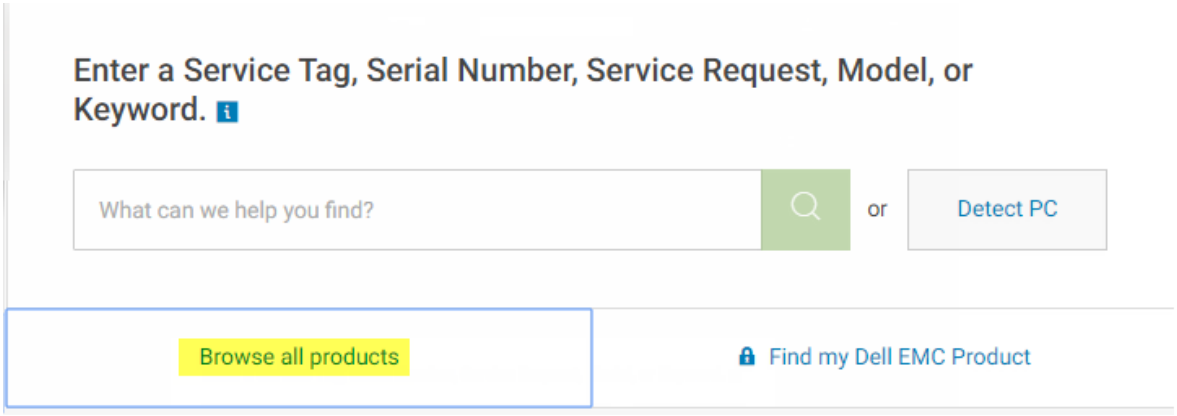
3

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 **Navegar por todos los productos**.



2. Seleccione **Seguridad** en la lista de productos.
3. Seleccione **Dell Data Security**.

   Después de realizar una vez esta selección, el sitio web la recordará.
4. Seleccione el producto Dell.

   Ejemplos:

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise
5. Seleccione **Controladores y descargas**.
6. Seleccione el tipo de sistema operativo del cliente deseado.
7. Seleccione **Dell Encryption** en las coincidencias. 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**.

   Continúe con la instalación de Encryption Personal.

4

Instalación

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

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

NOTA: Si el cifrado basado en políticas se instala antes que Encryption Management Agent, es posible que se produzca una falla en la computadora. Este problema se debe a una falla en la carga del controlador de suspensión de cifrado que administra el entorno PBA. Como solución alternativa, utilice el instalador maestro o asegúrese de que el cifrado basado en políticas se instala después de Encryption Management Agent.

- Consulte *Ayuda de cifrado de Dell* para saber cómo usar las funciones de Encryption. Acceda a la ayuda desde `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- Consulte *Ayuda de Encryption External Media* para saber cómo usar las funciones de Encryption External Media. Acceda a la ayuda desde `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption`.
- Consulte *Ayuda de Encryption Personal* para aprender cómo utilizar las funciones de Advanced Authentication. Acceda a la ayuda desde `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help`.

Importar autorización

La instalación de Encryption Personal requiere una clave de registro en la computadora de destino. Esta clave de registro se agrega a través de la interfaz de línea de comandos durante la instalación o a través de la GUI antes de la instalación.

Para agregar la clave de registro mediante la interfaz de línea de comandos, consulte Instalación por línea de comandos.

Para agregar la clave de registro mediante la GUI:

1. Abra un editor de texto.
2. Agregue el texto a continuación.

   ```
   [HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

   "SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
   XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
   ```

3. Guarde el archivo de texto con la extensión `.reg`.
4. Haga doble clic en el archivo de registro que guardó para importar la autorización de Encryption Personal.

Selección de un método de instalación

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

- Instalación interactiva: RECOMENDADO
- Instalación con la línea de comandos

Instalación interactiva

Para instalar Encryption Personal, el instalador debe encontrar la autorización específica en la computadora. Si falta la autorización correspondiente, no se podrá instalar Encryption Personal.

- El instalador maestro instala varios clientes. En el caso de Encryption Personal, instala Encryption y SED Management.
- Los archivos de registro del instalador maestro están ubicados en `C:\ProgramData\Dell\Dell Data Protection\Installer`.

1. Instale la autorización en el equipo de destino, si fuera necesario. Las instrucciones para agregar el derecho a la computadora se incluyen en el correo electrónico que describe la información de la licencia.
2. Copie DDSSetup.exe en la computadora local.
3. Haga doble clic en DDSSetup.exe para iniciar el instalador.
4. Se muestra un cuadro de diálogo que le informa acerca del estado de los requisitos previos para la instalación. Tardará unos minutos.
5. Haga clic en **Siguiente** en la pantalla de bienvenida.
6. Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.
7. Haga clic en **Siguiente** para instalar Encryption Personal en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\.`
8. La autenticación se instala de forma predeterminada y no se puede anular la selección. Figura como Security Framework en el instalador.

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

   Aparece una ventana de estado. Esta operación tarda varios minutos.
10. Seleccione **Sí, deseo reiniciar ahora mi equipo** y haga clic en **Finalizar**.
11. Una vez que se reinicia el equipo, autentíquese en Windows.

Finalizó la instalación de Encryption Personal y Advanced Authentication.

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

Una vez que finalicen el asistente para la instalación y la configuración de Encryption Personal, inicie la consola del administrador de Encryption Personal.

El resto de esta sección detalla otras tareas de instalación y pueden omitirse. Continúe con los asistentes para la instalación de Advanced Authentication y de Encryption Personal.

Instalación con la línea de comandos

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

- Instale la autorización en el equipo de destino, si fuera necesario.
- **NOTA:** En los registros de Dell Encryption no se especifica si la falla se produjo por falta de almacenamiento en disco.
- Modificadores:

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

Modificador	Significado
/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
ENTITLEMENT=1:PE:{ingrese aquí la clave de derecho de Encryption Personal}

Parámetros
NOTA: Este parámetro **solo** se puede utilizar con Encryption Personal

- Ejemplo de instalación con la línea de comandos

  El reinicio se ha suprimido en los ejemplos de línea de comandos. No obstante, es posible que se requiera un reinicio.

  El cifrado basado en políticas no puede comenzar hasta que no se reinicie la computadora.

  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 el Encryption client (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`) y, luego, se transfiere la clave de habilitación directamente al instalador.

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- En el ejemplo siguiente, se instala Encryption Personal y Advanced Authentication (instalación silenciosa, sin reinicio e instalados en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- En el ejemplo siguiente, se instala Encryption Personal y Advanced Authentication (instalación silenciosa, sin reinicio e instalados en la ubicación alternativa `C:\Program Files\Dell\My_New_Folder`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

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

  Finalizó la instalación de Encryption Personal y Advanced Authentication.

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

  Una vez que finalicen el asistente para la instalación y la configuración de Encryption Personal, inicie la consola del administrador de Encryption Personal.

  El resto de esta sección detalla otras tareas de instalación y pueden omitirse. Continúe con los asistentes para la instalación de Advanced Authentication y Personal Edition.

5

Asistentes de instalación de Advanced Authentication y de Encryption Personal

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, aparece el asistente de activación de Advanced Authentication. Haga clic en **Siguiente**.
3. Escriba y vuelva a introducir una Contraseña de administrador de cifrado (EAP) nueva. Haga clic en **Siguiente**.

   Nota: La Contraseña de administrador de cifrado debe tener un mínimo de ocho caracteres y un máximo de 127 caracteres.
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 Advanced Authentication.

   Después de que haya terminado el asistente de activación de Advanced Authentication, continúe con el paso siguiente.
6. Inicie el asistente para la instalación de Encryption Personal desde el ícono de Dell Encryption en el área de notificación (es posible que se inicie por sí mismo).

   Este Asistente para la instalación lo 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, a continuación, 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 8 y 127 caracteres y confírmela. La contraseña debe incluir caracteres alfabéticos, numéricos y especiales. Esta contraseña puede ser igual a la EAP que estableció para Advanced Authentication, pero no están relacionadas. **Anote y guarde esta contraseña en un lugar seguro**. Haga clic en **Siguiente**.

   Nota: La Contraseña de administrador de cifrado debe tener un mínimo de ocho caracteres y un máximo de 127 caracteres.
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 almacenamiento extraíble están disponibles, la copia de seguridad de las claves de cifrado se ejecuta como un proceso de segundo plano. Sin embargo, si la ubicación no está disponible (por ejemplo, si el dispositivo de almacenamiento extraíble original no está insertado en el 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 > Dell > 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 reinicia 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 queda etiquetada como “De conformidad”.

6

Configurar ajustes de la consola

La configuración predeterminada permite que los administradores y usuarios utilicen Advanced Authentication inmediatamente después de la activación, sin configuración adicional. Los usuarios se agregan automáticamente como usuarios de Advanced Authentication cuando inician sesión en la computadora con sus contraseñas de Windows, pero de forma predeterminada, no se habilita la autenticación multifactor de Windows.

Para configurar las funciones de Advanced Authentication, debe ser un administrador de la computadora.

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

Después de la activación de Advanced Authentication, si fuera necesario, se puede cambiar la contraseña del administrador y la ubicación de las copias de seguridad.

1. Como administrador, inicie la consola de Dell Data Security 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 de administrador, si desea cambiar la contraseña, ingrese una nueva que contenga entre 8 y 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 realiza 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), Advanced Authentication solicita una ubicación para realizar la copia de seguridad de los datos. Es necesario tener acceso a los datos de recuperación para comenzar el cifrado.

Configuración de la autenticación de prearranque (PBA)

La PBA está disponible si su computadora cuenta con una SED. La PBA se configura en la pestaña Encryption. Cuando SED Manager asume la propiedad de la SED, se activa la PBA.

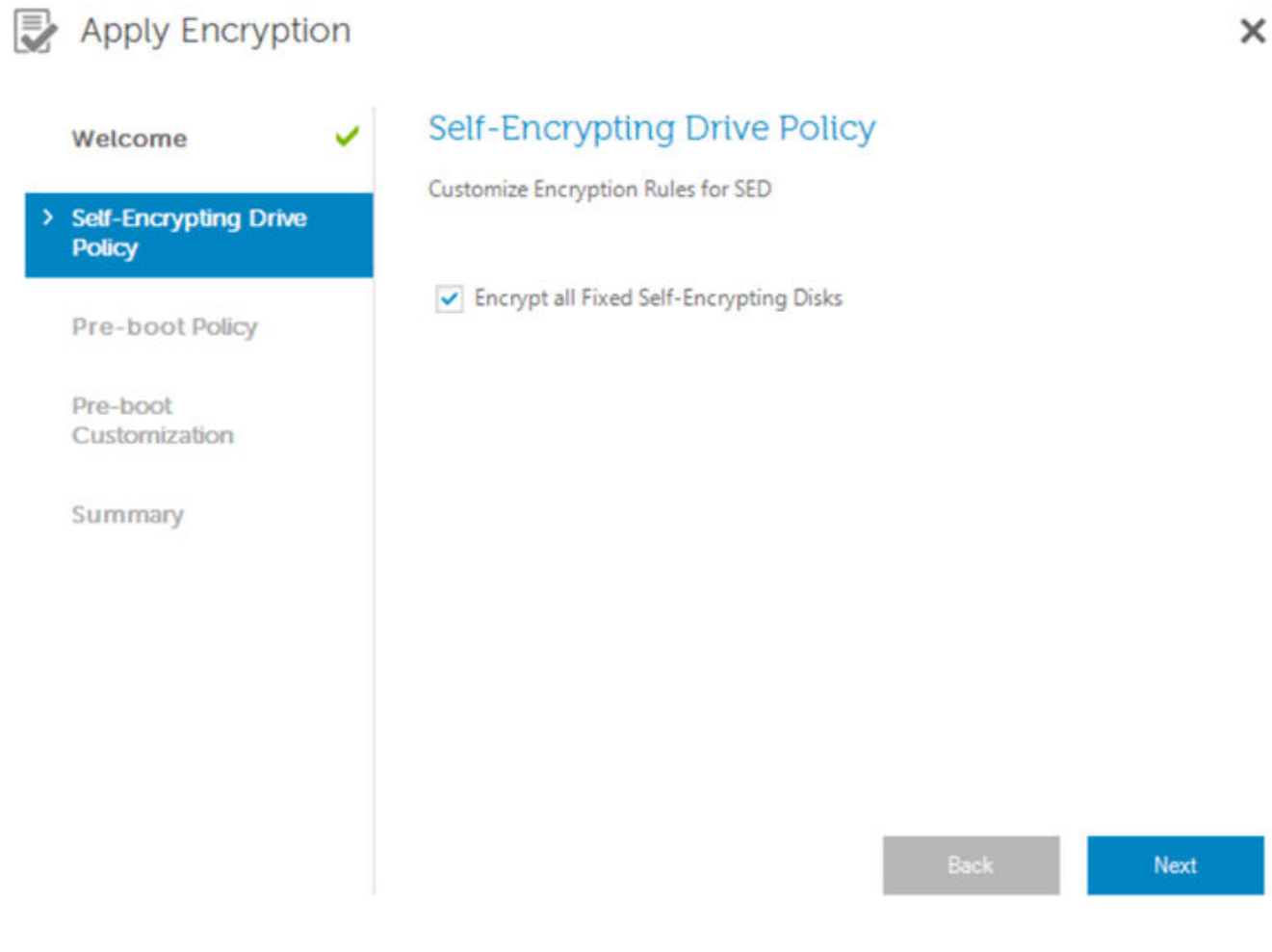
Para habilitar SED Management, haga lo siguiente:

1. En la consola Data Security, haga clic en el mosaico **Configuración del administrador**.
2. Asegúrese de que se puede acceder a la ubicación de copia de seguridad desde el equipo.

   Si aparece el mensaje *No se encuentra la ubicación del respaldo* y la ubicación del respaldo está en una unidad USB, es posible que su unidad no esté conectada o esté conectada a una ranura diferente a la que utilizó durante el respaldo. Si se muestra el mensaje y la ubicación de copia de seguridad se encuentra en una unidad de red, no se podrá acceder a esta unidad desde el equipo. Si es necesario cambiar la ubicación de copia de seguridad, desde la pestaña **Configuración del administrador**, seleccione **Cambiar ubicación de copia de seguridad** para cambiar la ubicación a la ranura actual o a una

unidad accesible. Transcurridos unos segundos tras la reasignación de la ubicación, se podrá continuar con el proceso de habilitación del cifrado.

3. Haga clic en la pestaña **Cifrado** y, a continuación, en **Cifrar**.
4. En la página de Bienvenida, haga clic en **Siguiente**.
5. Seleccione **Cifrar todos los discos de autocifrado fijos** para habilitar el cifrado de varios discos.



6. En la página Política de prearranque, cambie o confirme los siguientes valores y haga clic en **Siguiente**.

Intentos de inicio de sesión de usuario sin caché	Número de veces que un usuario desconocido puede intentar iniciar sesión (un usuario que no ha iniciado sesión en el equipo anteriormente [no se han guardado sus credenciales en la memoria caché]).
Intentos de inicio de sesión de usuario en caché	Número de veces que un usuario conocido puede intentar iniciar sesión.
Intentos en responder a preguntas de recuperación	Número de veces que el usuario puede intentar escribir la respuesta correcta.
Habilitar contraseña para eliminar cifrado	Seleccionar para habilitar
Introducir contraseña para eliminar cifrado	Una palabra o código de hasta 100 caracteres utilizado como mecanismo de seguridad a prueba de errores. Si ingresa esta palabra o este código en el campo de nombre de usuario o contraseña durante la autenticación previa al arranque, se inicia un borrado de cifrado con el cual se eliminan las claves del almacenamiento seguro. Una vez que este proceso se invoca, la unidad se

	puede recuperar. Deje el campo en blanco si no desea tener una contraseña para eliminar cifrado disponible en caso de emergencia. Deje el campo en blanco si no desea tener una contraseña para eliminar cifrado disponible en caso de emergencia.
Recordarme	Habilita o deshabilita la posibilidad de que los usuarios puedan seleccionar la opción Recordarme en la pantalla de inicio de sesión de PBA.

7. En la página Personalización de prearranque, ingrese el texto personalizado que aparecerá en la pantalla de autenticación previa al arranque (PBA) y haga clic en **Siguiente.**

Texto de título de prearranque	Este texto aparece en la parte superior de la pantalla de PBA. Si deja este campo vacío, no se mostrará ningún título. El texto no hace salto de línea, por lo que es posible que los textos de más de 17 caracteres aparezcan cortados.
Texto de información de soporte	Texto que se muestra en la pantalla de información sobre asistencia de PBA. Personalice el mensaje para incluir detalles acerca de cómo comunicarse con un help desk o el administrador de seguridad. Si no ingresa un texto en este campo, el usuario no tendrá información de contacto de soporte a su disposición. El ajuste de texto se produce a nivel de las palabras y no de los caracteres. Si una palabra tiene más de 50 caracteres aproximadamente, no se ajustará y no se mostrará una barra de deslizamiento, lo cual cortará el texto.
Texto de aviso legal	Este texto se muestra antes de que se permita al usuario iniciar sesión en el dispositivo. Por ejemplo: “Al hacer clic en Aceptar, acepta el cumplimiento de la política de uso aceptable del equipo”. Si no introduce texto en este campo, no se mostrará texto o los botones Aceptar/Cancelar. El ajuste de texto se produce a nivel de las palabras y no de los caracteres. Por ejemplo, si hay una sola palabra que tiene más de aproximadamente 50 caracteres, esta no hará salto de línea y no habrá una barra de desplazamiento, por lo tanto el texto se truncará.

8. En la página de Resumen, haga clic en **Aplicar**.
9. Cuando se le solicite, haga clic en **Apagar**.

   Es necesario un apagado completo antes de que pueda darse inicio al proceso de cifrado.

10. Después del apagado, reinicie el equipo.

    Ahora Encryption Management Agent administra la autenticación. Los usuarios deben iniciar sesión en la pantalla de PBA con sus contraseñas de Windows.

Modificación de la configuración de PBA y SED Management

Después de que habilite Encryption por primera vez y configure la política y personalización de prearranque, las siguientes acciones estarán disponibles en la pestaña Encryption:

- Cambiar la política o personalización de prearranque: haga clic en la pestaña **Encryption** y, luego, en **Cambiar**.
- Deshabilite SED Management; por ejemplo, para realizar la desinstalación: haga clic en **Descifrar**.

Después de que habilite SED Management por primera vez y configure la política y personalización del prearranque, las siguientes acciones estarán disponibles en la pestaña Configuración de prearranque:

- Cambiar política o personalización previa al arranque: haga clic en la pestaña **Ajuste previo al arranque** y seleccione **Política de unidad de autocifrado**, **Política previa al arranque** o **Personalización previa al arranque**.

Administrar a los usuarios y la autenticación de usuarios

Agregar usuario

Los usuarios de Windows se convierten automáticamente en usuarios de Encryption Personal al iniciar sesión en Windows o al registrar una credencial.

La computadora debe estar conectada al dominio para agregar un usuario de dominio en la pestaña Agregar usuario de Data Security Console.

1. En el panel izquierdo de la herramienta Configuración del administrador, seleccione **Usuarios**.
2. En la parte superior derecha de la página Usuario, haga clic en **Agregar usuario** para comenzar el proceso de registro para un usuario de Windows existente.
3. Cuando se muestre el cuadro de diálogo Seleccionar usuario, seleccione **Tipos de objeto**.
4. Introduzca un nombre de objeto de usuario en el cuadro de texto y haga clic en **Comprobar nombres**.
5. Haga clic en **Aceptar** cuando termine.

Eliminar usuario

1. En el panel izquierdo de la herramienta Configuración del administrador, seleccione **Usuarios**.
2. Para eliminar un usuario, busque la columna del usuario y haga clic en **Quitar**. (desplácese hasta la parte inferior de la columna del usuario para ver la opción Eliminar).

Cómo quitar todas las credenciales registradas de un usuario

1. Haga clic en el mosaico **Configuración del administrador** y autentique con su contraseña.
2. Haga clic en la pestaña **Usuarios** y busque el usuario que desea eliminar.
3. 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.

7

Desinstalación del 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 Encryption Management Agent.

No es necesario desinstalar el paquete de controladores.

Continúe con Selección de un método de desinstalación.

Elija una desinstalación Método

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

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

Desinstalar de forma interactiva

1. Vaya a *Desinstalar un programa* en Windows Control Panel (en el cuadro de búsqueda de la barra de tareas, escriba **Panel de control**, luego seleccione Panel de control en los resultados).
2. Seleccione **Dell Installer** y haga clic con el botón izquierdo del mouse en **Cambiar** para iniciar el asistente para la instalación.
3. Lea la pantalla de bienvenida y, a continuación, haga clic en **Siguiente**.
4. Siga las indicaciones para desinstalar y haga clic en **Finalizar**.
5. Reinicie el equipo y iniciar sesión en Windows.

   El instalador maestro está desinstalado.

Desinstalar desde la línea de comandos

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

  ```
  "DDSSetup.exe" /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

- Dell recomienda utilizar el desinstalador de Data Security para eliminar Encryption Personal.
- 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 Encryption Personal mediante el instalador maestro, antes de la instalación debe 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.

Desinstalar 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.

  NOTA: Antes de desinstalarlo, asegúrese de que todas las plantillas de políticas se establecieron en Deshabilitada e inserte cualquier medio externo cifrado para realizar un descifrado estable.

  En este video se muestra en detalle cómo cambiar las plantillas de políticas en la Local Management Console.
- 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 de servicios.
-

Elija una desinstalación Método

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

- Desinstalar de forma interactiva
- Desinstalar desde la línea de comandos

Desinstalar de forma interactiva

1. Vaya a *Desinstalar un programa* en el panel de control de Windows (en el cuadro de búsqueda de la barra de tareas, escriba **Panel de control** y, a continuación, seleccione **Panel de control** en los resultados).
2. Resalte **Dell Encryption XX-bit** y haga clic con el botón izquierdo en **Cambiar** para iniciar el asistente para la instalación de Encryption Personal.
3. Lea la pantalla de bienvenida y, a continuación, haga clic en **Siguiente**.
4. En la pantalla de instalación de Encryption Removal Agent, puede elegir entre dos opciones:

NOTA: 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**.

5. En *Archivo de copia de seguridad*, ingrese 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.

   Escriba su contraseña de administrador de cifrado. Se trata de la contraseña del Asistente de configuración cuando se instaló el software.

   Haga clic en **Siguiente**.

6. En *Inicio de sesión de servicio de agente de Dell Decryption como*, seleccione **Cuenta del sistema local** y, a continuación, haga clic en **Finalizar**.
7. Haga clic en **Quitar** en la pantalla Quitar el programa.
8. Haga clic en **Finalizar** en la pantalla Configuración completa.
9. 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.

Desinstalar 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\<UserName>\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:\<any directory>\<any log file name>.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 `/qb`.

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

Modificador	Significado
/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 - Silenciosa: se requiere cuando se ejecuta con variables msiexec que contienen /q o /qn 0 - No silenciosa: solo es posible cuando no hay variables msiexec que tengan /q en la sintaxis de la línea de comandos
DA_KM_PW	La contraseña de la cuenta del administrador de dominios.
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 Encryption Management Agent

Elija una desinstalación Método

Existen dos métodos para desinstalar Encryption Management Agent, seleccione **uno** de los siguientes:

- Desinstalar de forma interactiva
- Desinstalar desde la línea de comandos

Desinstalar de forma interactiva

1. Vaya a *Desinstalar un programa* en el panel de control de Windows (en el cuadro de búsqueda de la barra de tareas, escriba **Panel de control** y, a continuación, seleccione **Panel de control** en los resultados).
2. Seleccione **Dell Encryption Management Agent** y haga clic con el botón izquierdo del mouse en **Cambiar** para iniciar el Asistente para la instalación.
3. Lea la pantalla de bienvenida y, a continuación, 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.

Desinstalar desde la línea de comandos

- Una vez extraído del instalador maestro, el instalador de Encryption Management Agent puede encontrarse en `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- En el siguiente ejemplo se desinstala SED Management de forma silenciosa.

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

  Apague y reinicie el equipo cuando haya terminado.

9

Desinstalador de Data Security

Desinstalar Encryption Personal

Dell proporciona el desinstalador de Data Security como un desinstalador maestro. Esta utilidad reúne los productos actualmente instalados y los elimina en el orden adecuado.

Este desinstalador de Data Security está disponible en: `C:\Program Files (x86)\Dell\Dell Data Protection`

Para obtener más información o para usar una interfaz de línea de comandos (CLI), consulte el artículo de la base de conocimientos 125052.

Los registros se generan en `C:\ProgramData\Dell\Dell Data Protection\` para todos los componentes que se eliminan.

Para ejecutar la utilidad, abra la carpeta contenedora, haga clic con el botón secundario en **DataSecurityUninstaller.exe** y seleccione **Ejecutar como administrador**.

Haga clic en **Siguiente**.

Opcionalmente, borre cualquier aplicación desde la extracción y haga clic en **Siguiente**.

Las dependencias necesarias se seleccionan o borran automáticamente.

Para quitar aplicaciones sin tener que instalar el agente de eliminación de cifrado, seleccione **No instalar Agente de eliminación de cifrado** y seleccione **Siguiente**.

Seleccione **Agente de eliminación de cifrado: importar claves desde un archivo** y, luego, seleccione **Siguiente**.

Navegue hasta la ubicación de las claves de recuperación y, luego, ingrese la frase de contraseña del archivo y haga clic en **Siguiente**.

Seleccione **Eliminar** para iniciar la desinstalación.

Haga clic en **Terminar** para finalizar la desinstalación y reinicie la computadora. De forma predeterminada, se selecciona **Reiniciar computadora tras hacer clic en Finalizar**.

La desinstalación y eliminación se han completado.

10

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. Un valor Verdadero significa que todos los datos que no estén cifrados por otras políticas de cifrado basadas en políticas se cifrarán conforme a la política 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
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

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
										no está 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

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
										protección de los directorios podría hacer que el equipo no se inicie y/o requiera que se vuelvan a 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 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.

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
										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 sistema y que el equipo no pueda iniciarse. Nombres de proceso comunes: outlook.exe, winword.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 dónde. “Común” para que todos los usuarios administrados puedan acceder a estos archivos en el punto final donde se crearon (el mismo nivel de acceso que las Carpetas cifradas comunes) y se cifraron con el algoritmo de cifrado Común.

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
										"Usuario" para que solamente el usuario que los creó pueda acceder a estos archivos, solamente en el punto final donde se crearon (el mismo nivel de acceso que las carpetas cifradas por el usuario) y se cifraron con el algoritmo de cifrado 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 que se indican en las variables de entorno TEMP y TMP con la clave de cifrado de datos de Usuario.
Cifrar los archivos temporales de Internet	Verdadero	Falso								El valor Verdadero cifra la ruta que se indica en la variable de entorno CSIDL_INTERNET_CACHE con la clave de cifrado de datos de 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.

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
Cifrar documentos del perfil de usuario	Verdadero								Falso	El valor Verdadero cifra: · El perfil de usuario (`C:\Users\jsmith`) con la clave de cifrado de datos de Usuario · \Usuarios\Público con la clave de cifrado común
Cifrar el archivo de paginación de Windows	Verdadero								Falso	El valor Verdadero cifra el archivo de paginación de Windows. Al realizar un cambio en esta política, se debe reiniciar el equipo.
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 sesión. Esta política también puede impedir el cierre de la sesión de 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 se iniciarán si un usuario no administrado inicia una sesión.

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
Limpieza segura post-cifrado	Sobrescribir tres veces	Sobrescribir una vez							No 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. · "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 cifra únicamente cuando el equipo realiza la hibernación. El cliente desactiva la protección

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
										cuando la computadora sale de la hibernación, brindando protección sin afectar a los usuarios o las aplicaciones mientras la computadora está en uso.
Evitar la hibernación no protegida	Verdadero					Falso		Verdadero	Falso	Al habilitar esta opción, el cliente no permite 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) Una lista de carpetas en el disco duro de extremo que se cifrará con la clave de cifrado de datos de Usuario o se excluirá 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 El algoritmo utilizado para cifrar la información a nivel del usuario individual.

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
										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 dónde. · 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: · "Común" para que todos los usuarios administrados puedan acceder a las carpetas o los archivos cifrados por el usuario en el extremo donde se crearon (el mismo nivel de acceso que las carpetas de cifrado común) y se cifraron con el algoritmo de cifrado Común. · "Usuario" para que solamente el usuario que los creó pueda acceder a estos archivos, solamente en el extremo donde se crearon (el mismo nivel de acceso que las carpetas de cifrado de Usuario) y se cifraron con el algoritmo de cifrado 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
										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 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:

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
										• Id. de equipo (MCID) del equipo actual • · Id. de dispositivo (DCID/SCID) de la instalación del cliente actual Encryption client 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 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 Deshabilitada, no se aplicará ninguna política del sistema de control de puertos, sin importar los valores de otras políticas del sistema de control de puertos. las políticas de PCS requieren un reinicio antes de surtir efecto. **NOTA:** Las operaciones de bloqueo del dispositivo

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
										provocan que los nombres de los dispositivos aparezcan en blanco.
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 Encryption External Media e interacciones con 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

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. 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 Encryption External Media e interacciones con 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.

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
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): 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

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
										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 cifrado de EMS	Verdadero					Falso		Verdadero	Falso	Esta política es la "política maestra" para todas las políticas de almacenamiento 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 Encryption External Media e interacciones con PCS.
Excluir cifrado de CD/DVD de EMS	Falso								Verdadero	Un valor Falso cifra los dispositivos CD/DVD. Esta política interactúa con PCS. Consulte Encryption External Media e interacciones con 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 Encryption External Media e interacciones con PCS.

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
										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 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
Exploración de medios externos de EMS	Verdadero	Falso								Verdadero permite escanear los medios extraíbles cada vez que se inserta. Cuando esta política está configurada en Falso, pero la política de medios externos de cifrado de EMS está configurada

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 Verdadero, solo se cifran los archivos nuevos y modificados. Se realiza una exploración en cada inserción para que todos los archivos agregados a los medios extraíbles sin autenticar puedan capturarse. Los archivos se pueden agregar a los medios si se rechaza la autenticación, pero no se puede acceder a los datos cifrados. Los archivos agregados no se cifrarán en este caso, por lo tanto, la próxima vez que se autentique (para trabajar con datos cifrados), todos los archivos que se hayan agregado se escanean y se cifran.
Acceso de datos cifrados de EMS en un dispositivo no protegido por Shield	Verdadero									El valor Verdadero permite el acceso del usuario a la 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 extraíbles que se desean excluir del cifrado. Se protegerán todos los dispositivos de medios extraíbles 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.

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
										Para buscar el PNPDeviceID para almacenamiento extraíble: 1. Inserte el dispositivo de almacenamiento extraíble en una computadora cifrada. 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 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

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
										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 numéricos de EMS en la	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
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.

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
										Es posible que los dispositivos de almacenamiento que incluyen múltiples conexiones de interfaz, tales como Firewire, USB, eSATA, etc., requieran el uso de reglas de cifrado y de medios externos 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 Encryption External Media.
Acceso bloqueado de EMS a medios no protegidos	Verdadero								Falso	Se bloquea el acceso a cualquier dispositivo de almacenamiento extraíble que tenga menos de 55 MB y, por lo tanto, tenga una capacidad de almacenamiento insuficiente para alojar Encryption External Media (como un disquete de 1,44 MB). Se bloquea todo acceso si EMS y esta política están configurados en Verdadero. Si la política de medios externos de cifrado de EMS 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.

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
										Si la política de medios externos de cifrado de EMS está configurada como Falso, esta política no tendrá efecto y no afectará al acceso a los dispositivos externos 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 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		La cantidad 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		Establecer el valor en Verdadero le permite al usuario ver una opción de menú en el icono del área de notificación que le permite pausar o reanudar

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 cifrado o descifrado (según lo que Encryption esté realizando en ese momento). Permitir a un usuario pausar el cifrado podría autorizar al usuario a evitar que el cliente Encryption client 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 es Verdadero, no se produce el cifrado o descifrado de datos mientras el usuario está trabajando activamente. El cliente procesará la información únicamente cuando la pantalla esté bloqueada. El valor opcional de usuario agrega una opción al ícono del área de notificación que permite al usuario activar o desactivar esta función. Cuando el valor está configurado en Falso, el proceso de cifrado se lleva a cabo en cualquier momento, incluso cuando el usuario esté trabajando. Habilitar esta opción prolongará considerablemente 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.
- cifra todos los datos en los dispositivos de almacenamiento extraíble, e impide el 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.
- indica 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.
- indica 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.
- indica 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.
- indica 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.

11

Extracción de instaladores secundarios

- 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 `DDSSetup.exe` a la computadora local.
2. Abra un símbolo del sistema en la misma ubicación en la que está el archivo `DDSSetup.exe` e ingrese lo siguiente:

   ```
   DDSSetup.exe /s /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.

12

Solución de problemas

Actualización con actualizaciones de características de Windows 10 o Windows 11

Para actualizar Windows 10 o Windows 11 con las actualizaciones de características, siga las instrucciones que se indican en el artículo de la base de conocimientos 125419.

Solución de problemas de Dell 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.
- El archivo de registro de Encryption Removal Agent no se crea hasta después de que el servicio de Encryption Removal Agent se haya ejecutado, lo cual 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**.

Encryption External Media e interacciones con 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: almacenamiento > Almacenamiento de subclase: 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 esté 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 Windows Media Encryption = activado.
- Establecer EMS, Excluir cifrado de CD/DVD = no seleccionado.
- Establecer subclase de almacenamiento: Control de unidad óptica = Solo UDF.

Uso de WSScan

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

NOTA: WSScan debe ejecutarse en modo Sistema con la herramienta PsExec si un archivo de destino es propiedad de la cuenta del sistema.

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 analizar: *Todas las unidades, Unidades fijas*, *Unidades extraíbles* o *CD-ROM/DVD-ROM*.
5. Seleccione el tipo de informe de Encryption: *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 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 en el menú.
3. Si no desea escribir la salida de WSScan en un archivo, desactive la casilla de verificación **Salida a archivo**.
4. Si lo desea, cambie la ruta de acceso y el nombre de archivo predeterminados en *Ruta de acceso*.
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 SDE. **Usuario:** clave de cifrado de usuario. **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 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 (resalte el servicio > haga clic con el botón derecho del mouse > Actualizar) para actualizar el estado.

- **En espera de la desactivación de SDE**: Encryption aún está instalado, configurado o ambos. El descifrado no se inicia hasta que Encryption esté desinstalado.
- **Barrido inicial**: El servicio realiza un barrido inicial, calculando la cantidad de archivos cifrados y los bytes. El barrido inicial se produce una sola vez.
- **Barrido de descifrado**: El servicio descifra archivos y posiblemente solicita 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 el servicio de Encryption Removal Agent para 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 Encryption External Media

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.

- Dell no recomienda el uso de dispositivos iPod Shuffle ya que podrían producirse 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 computadoras con Encryption External Media habilitado.
- Debido a que los nombres de las carpetas en los iPod dependen del modelo de iPod, Dell recomienda crear una política de exclusión que cubra todos los nombres de carpeta de todos los modelos de iPod.
- Para garantizar que el cifrado de un iPod mediante Encryption External Media no haga que el dispositivo quede inutilizable, aplique las siguientes reglas en la política de reglas de cifrado de Encryption External Media:

  -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 dell.com/support.
2. Seleccione el modelo del equipo.
3. Seleccione **Controladores y descargas**.
4. Seleccione el **Sistema operativo** del equipo de destino.
5. Seleccione 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

1. Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del controlador.
2. Haga doble clic sobre el controlador Dell ControlVault para iniciar el archivo ejecutable autoextraíble.

   NOTA:

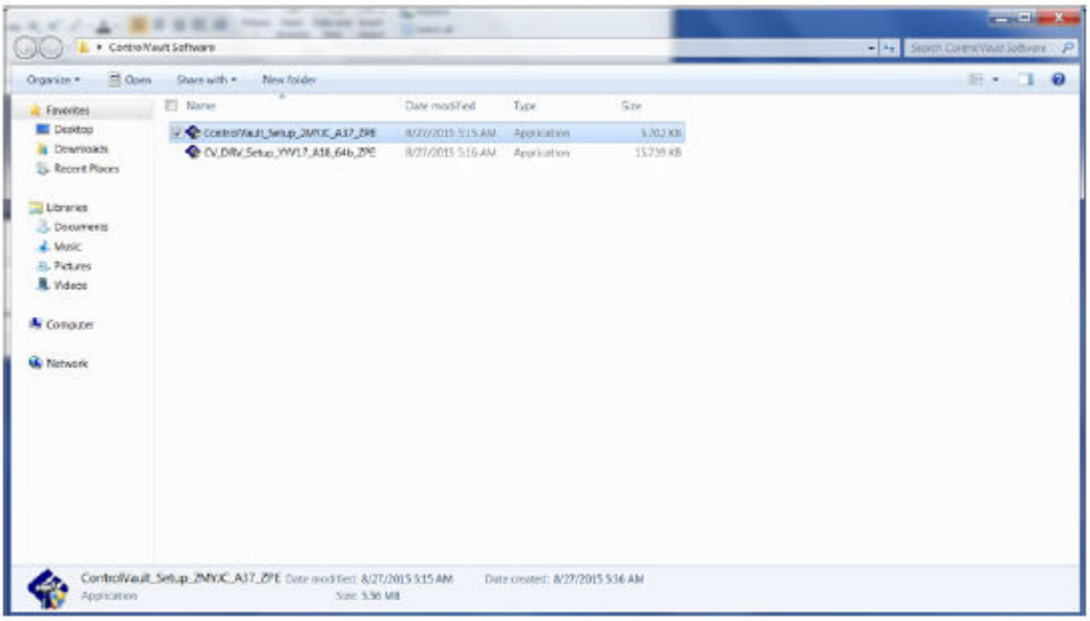
   Asegúrese de instalar primer el controlador. El nombre de archivo del controlador *cuando se creó este documento* era ControlVault_Setup_2MYJC_A37_ZPE.exe.
3. Haga clic en **Continuar** para empezar.
4. Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada de `C:\Dell\Drivers\<New Folder>`.
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. En este caso, la carpeta es **JW22F**.
8. 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)].
9. Haga clic en **Siguiente** en la pantalla de bienvenida.
10. Haga clic en **Siguiente** para instalar los controladores en la ubicación predeterminada de `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Seleccione la opción **Completar** y haga clic en **Siguiente**.
12. Haga clic en **Instalar** para empezar la instalación de los controladores.
13. 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

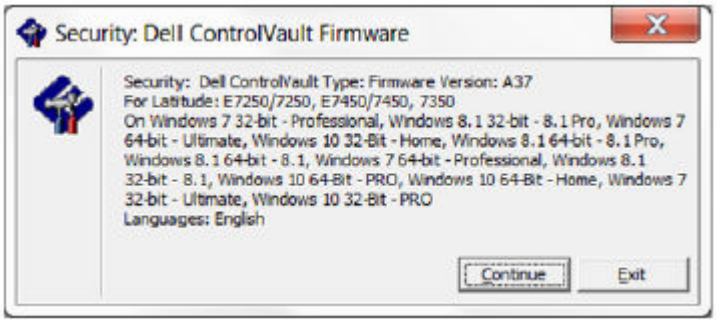
- Device Manager tendrá un dispositivo Dell ControlVault (y otros dispositivos) dependiendo de la configuración del hardware y del sistema operativo.

Instalación del firmware Dell ControlVault

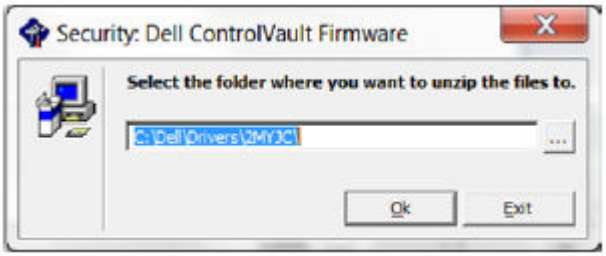
1. Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del firmware.



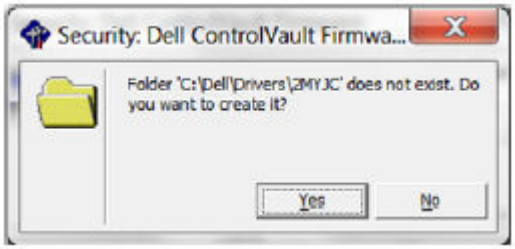
2. Haga doble clic sobre el firmware Dell ControlVault para iniciar el archivo ejecutable autoextraíble.
3. Haga clic en **Continuar** para empezar.



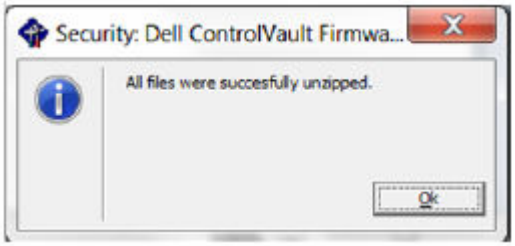
4. Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada de `C:\Dell\Drivers\<New Folder>`.



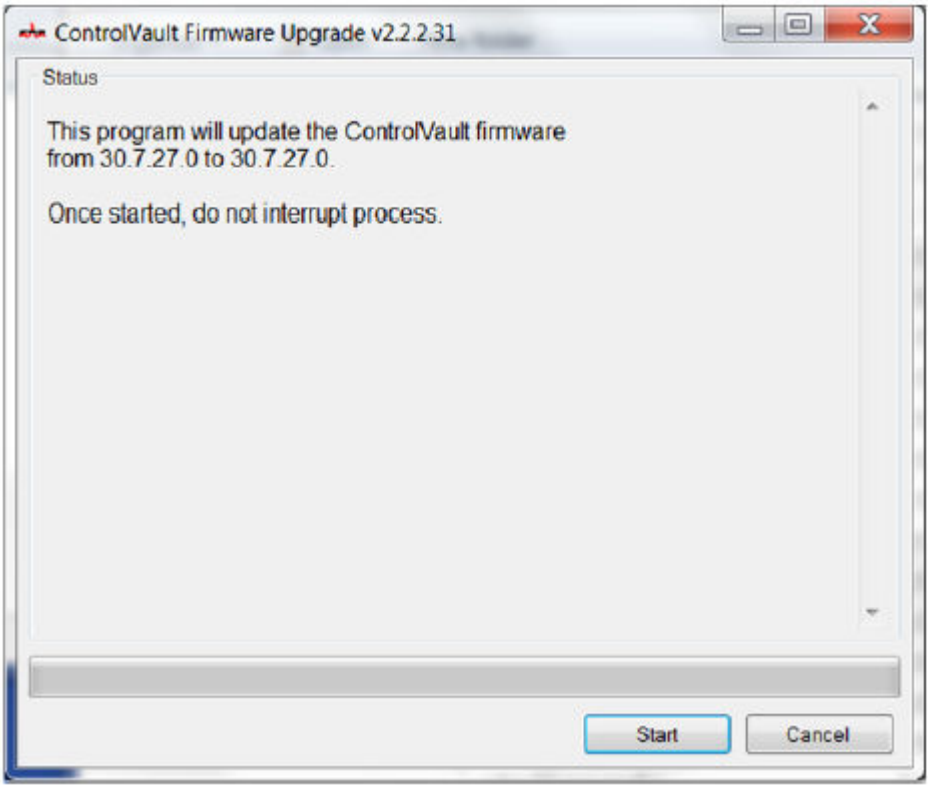
5. Haga clic en **Sí** para permitir la creación de una nueva carpeta.



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.



NOTA:

Si está realizando la actualización desde una versión de firmware más antigua, es posible que deba ingresar 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.

Ajustes de registro

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

Cifrado

(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.
- El archivo de registro de Encryption Removal Agent no se crea hasta después de que el servicio de Encryption Removal Agent se haya ejecutado, lo cual ocurre después de reiniciar el equipo. Se eliminará permanentemente el archivo de registro, una vez que el cliente esté desinstalado y el equipo 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 determinar si una tarjeta inteligente está presente y activa, asegúrese de establecer el siguiente valor:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Si SmartcardEnabled no está presente o tiene un valor de cero, el proveedor de credenciales mostrará solo la opción de contraseña para la autenticación.

  Si SmartcardEnabled tiene un valor distinto de cero, el proveedor de credenciales mostrará opciones para autenticación con contraseña y tarjeta inteligente.

- Con el siguiente valor de registro se indica si Winlogon debe generar una notificación para los eventos de inicio de sesión de tarjetas inteligentes.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0: Deshabilitado

  1: Habilitado

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 de cifrado muestra la indicación *`length of each policy update delay`* 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 cambia el comportamiento predeterminado que se postergará. 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 Encryption está procesando una actualización de 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.

Habilitar/deshabilitar Encrypt for Sharing en el menú contextual del botón secundario

- Para deshabilitar o habilitar la opción *Encrypt for Sharing* en el menú contextual del botón secundario, utilice la siguiente clave de registro.

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 = deshabilita la opción Encrypt for Sharing en el menú contextual del botón secundario

  1 = habilita la opción Encrypt for Sharing en el menú contextual del botón secundario

Habilitar/deshabilitar la notificación para la activación de Encryption Personal

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = desactiva la solicitud de contraseña para la activación de Encryption Personal

  0 = activa la solicitud de contraseña para la activación de Encryption Personal

Habilitar/deshabilitar la solicitud de reinicio después de que Encryption Removal Agent complete la etapa final del descifrado

- Para deshabilitar el mensaje que indica al usuario que reinicie la computadora después de que Encryption Removal Agent finalice su estado final en el proceso de descifrado, modifique el siguiente valor de registro.

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Predeterminado = activado

  1 = habilitado (muestra el indicador)

  0 = deshabilitado (oculta el indicador)

Advanced Authentication

Deshabilitación de Servicios biométricos y tarjetas inteligentes (opcional)

Si no desea que Advanced Authentication 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 desactivado, Authentication no tratará de iniciar estos tres servicios:

- SCardSvr: administra el acceso a las tarjetas inteligentes leídas por el equipo. Si el servicio se detiene, la computadora no puede leer tarjetas inteligentes. Si el servicio se deshabilita, no se pueden iniciar 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 determinar si la PBA está activada, asegúrese de que esté establecido el siguiente valor:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  Un valor de 1 significa que la PBA está activada. Un valor de 0 significa que la PBA no está activada.

  NOTA: La eliminación manual de esta clave puede crear resultados inesperados para los usuarios que sincronizan con PBA, lo que genera la necesidad de una recuperación manual.

- Para determinar si una tarjeta inteligente está presente y activa, asegúrese de establecer el siguiente valor:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Si SmartcardEnabled no está presente o tiene un valor de cero, el proveedor de credenciales mostrará solo la opción de contraseña para la autenticación.

  Si SmartcardEnabled tiene un valor distinto de cero, el proveedor de credenciales mostrará opciones para autenticación con contraseña y tarjeta inteligente.

- Con el siguiente valor de registro se indica si Winlogon debe generar una notificación para los eventos de inicio de sesión de tarjetas inteligentes.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0: Deshabilitado

  1: Habilitado

  Continúe con Glosario.

- Para evitar que SED Management deshabilite proveedores de credenciales de terceros, cree la siguiente clave de registro:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 =Deshabilitado (valor predeterminado)

1 =Habilitado

- Encryption Management Agent ya no genera políticas de manera predeterminada. Para generar las futuras políticas consumidas, cree la siguiente clave de registro:

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

  Value=1

  Nota: Se requiere un reinicio para que este cambio surta efecto.

- Para suprimir todas las notificaciones del sistema desde Encryption Management Agent, se debe configurar el siguiente valor de registro en la computadora cliente.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Habilitado (valor predeterminado)

  1 = Deshabilitado

13

Glosario

Advanced Authentication: el producto Advanced Authentication proporciona opciones de lectores de tarjetas inteligentes. Advanced Authentication ayuda a administrar estos diversos métodos de autenticación, admite inicio de sesión con unidades de cifrado automático, SSO, y administra credenciales y contraseñas de usuario.

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 realizados en la consola de administración local requieren esta contraseña. Además, esta contraseña es la misma que necesita para utilizar el archivo LSARecovery_[hostname].exe a fin de recuperar 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, Encryption utiliza la clave de cifrado del usuario, junto con 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 de cifrado común permite que todos los usuarios administrados tengan acceso a los archivos en el dispositivo en el que se crearon. La clave de cifrado del usuario determina que solo tenga acceso a los archivos la persona que los crea y únicamente en el dispositivo en el que se crearon. La clave de cifrado de roaming del usuario determina que solo tenga acceso a los archivos la persona que los crea en cualquier dispositivo Windows o Mac cifrado.

Barrido de cifrado: el proceso de escanear las carpetas que se van a cifrar para garantizar que los archivos que contienen 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 puede 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 Escanear estación de trabajo durante el inicio de sesión* está habilitada, se realiza un barrido en las carpetas especificadas para el cifrado en cada inicio de sesión del usuario. - Se puede volver a desencadenar un barrido con determinados cambios de política posteriores. Cualquier cambio de política relacionado con la definición de las carpetas de cifrado, los algoritmos de cifrado, el uso de claves de cifrado (común frente a usuario), desencadena un barrido. Además, cambiar entre cifrado activado y desactivado desencadenará un barrido de cifrado.

Autenticación previa al arranque (PBA): la autenticación previa al arranque 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 que sirve como una capa confiable de autenticación. 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. El cifrado de clave común y de usuario está pensado para datos de usuario confidenciales porque requieren una contraseña de usuario para desbloquear 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 de SDE activa el descifrado automático de todos los archivos y directorios cifrados de SDE de los usuarios correspondientes, sin tener en cuenta los otros valores de política de SDE, como 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.