# Dell Encryption Enterprise

## Advanced Installation Guide v11.9

January 2023
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

# Introducción

En esta guía se detalla cómo instalar y configurar Encryption, SED Management, Full Disk Encryption, Protección web y firewall de cliente, y BitLocker Manager.

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

## Antes de empezar

1. Instale el Dell Server antes de implementar los clientes. Localice la guía correcta, tal como se indica a continuación, siga las instrucciones y, a continuación, vuelva a esta guía.
   - *Guía de instalación y migración de Security Management Server*
   - *Guía de inicio rápido y guía de instalación de Security Management Server Virtual*
   - Compruebe que las políticas están establecidas de la forma deseada. Explore la ayuda AdminHelp, disponible a través del signo **?** que se encuentra en la esquina superior derecha de la pantalla. AdminHelp es una ayuda a nivel de página diseñada para ayudarlo a definir y modificar las políticas y conocer qué opciones tiene disponibles en Dell Server.
2. Lea detenidamente el capítulo Requisitos de este documento.
3. Implemente los clientes en los usuarios.

## Utilización de esta guía

Use esta guía en el orden siguiente.

- Consulte Requisitos para los requisitos previos del cliente, la información de hardware y software del equipo, las limitaciones, y las modificaciones de registro especiales necesarias para funciones.
- Si es necesario, consulte Configuración previa a la instalación para SED UEFI y BitLocker.
- Si sus clientes están autorizados para utilizar Dell Digital Delivery, consulte Configuración de GPO en la controladora de dominio para habilitar derechos.
- Si se instalarán clientes que utilizan el instalador maestro de , consulte:
  - Instalación interactiva mediante el instalador maestro

    O bien
  - Instalación mediante la línea de comandos con el instalador maestro
- Si instala clientes mediante los instaladores secundarios, los archivos ejecutables de los instaladores secundarios se deben extraer del instalador maestro. Consulte Extracción de instaladores secundarios del instalador maestro y luego regrese aquí.
  - Instale los instaladores secundarios mediante la línea de comandos:
    - Instalación de Encryption: utilice estas instrucciones para instalar Encryption, que es el componente que aplica la política de seguridad, independientemente de que una computadora esté conectada a la red, esté desconectada de esta, se haya perdido o la hayan robado.
    - Instalación del cliente Full Disk Encryption: utilice estas instrucciones para instalar Full Disk Encryption, que es un componente que aplica la política de seguridad, independientemente de que una computadora esté conectada a la red, esté desconectada de esta, se haya perdido o la hayan robado.
    - Instalación de SED Manager: utilice estas instrucciones para instalar el software de cifrado para SED. A pesar de que las SED proporcionan su propio cifrado, no cuentan con una plataforma para administrar el cifrado y las políticas. Con SED Manager, todas las políticas, el almacenamiento y la recuperación de claves de cifrado están disponibles en una única consola, lo cual reduce el riesgo de que las computadoras no estén protegidos en caso de pérdida o acceso no autorizado.
    - Instalación de BitLocker Manager: utilice estas instrucciones para instalar BitLocker Manager, diseñado para mejorar la seguridad de implementaciones de BitLocker y simplificar y reducir el costo de propiedad.

      **NOTA:**

La *mayoría* de los instaladores secundarios se pueden instalar interactivamente, pero no se describen en esta guía.

- Consulte Situaciones frecuentes para obtener las secuencias de comandos de nuestras situaciones más comúnmente usadas.

# 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

## Todos los clientes

Estos requisitos se aplican a todos los clientes. Los requisitos que aparecen en otras secciones se aplican a clientes específicos.

- Durante la implementación se deberán seguir las prácticas recomendadas para TI. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados, para las pruebas iniciales e implementaciones escalonadas para los usuarios.
- La cuenta de usuario que realiza la instalación/actualización/desinstalación debe ser un usuario administrador local o de dominio, que se puede designar temporalmente mediante una herramienta de implementación, como Microsoft SCCM. No son compatibles los usuarios con privilegios elevados que no sean administradores.
- Realice copia de seguridad de todos los datos importantes antes de iniciar la instalación/desinstalación.
- Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Los administradores deben asegurarse de que todos los puertos necesarios estén disponibles.
- Asegúrese de revisar periódicamente dell.com/support para obtener la documentación y la asesoría técnica más recientes.
- La línea de productos Dell Data Security no admite versiones de Windows Insider Preview.

### Requisitos previos

- Se requiere Microsoft .Net Framework 4.5.2 (o posterior) para los clientes del instalador maestro y secundario de . El instalador *no* instala los componentes de Microsoft .Net Framework.
- Para comprobar qué versión de Microsoft .Net tiene instalada, siga estas instrucciones en la computadora en la que se va a realizar la instalación. Consulte estas instrucciones para instalar Microsoft .Net Framework 4.5.2.
- Si se instala Encryption en modo FIPS, se necesita Microsoft .Net Framework 4.6.

### Hardware

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

| **Hardware** |
|---|
| ○ Procesador Intel Pentium o AMD<br>○ 110 MB de espacio disponible en el disco<br>○ 512 MB de RAM<br>**NOTA:** Se necesita espacio libre adicional en el disco para cifrar los archivos en el terminal. El tamaño varía según las políticas habilitadas y la capacidad de la unidad. |

### Localización

- Dell Encryption, SED Manager, PBA Advanced Authentication y BitLocker Manager son interfaces de usuario en varios idiomas que cumplen con las normas del sector y se pueden configurar en los siguientes idiomas.

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

# Cifrado

- El equipo cliente debe tener conectividad de red para activarse.
- Para activar una cuenta de Microsoft Live con Dell Encryption, consulte este artículo de la base de conocimientos 124722.
- Para reducir la duración inicial de cifrado, ejecute el asistente de liberación de espacio en disco de Windows para eliminar los archivos temporales y otros archivos innecesarios.
- Windows Hello empresarial requiere Encryption Enterprise v11.0 o una versión posterior en Windows 10.
- Windows Hello empresarial requiere activación en un servidor Dell que ejecute la versión 11.0 o una posterior.
- 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).
- Encryption no es compatible con las configuraciones de inicio doble, dado que es posible cifrar archivos de sistema del otro sistema operativo, lo cual podría interferir en su funcionamiento.
- 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.
- 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. Consulte Extracción de instaladores secundarios del instalador maestro para obtener instrucciones sobre la extracción.
- Encryption ahora es compatible con el modo de auditoría. El modo de auditoría permite a los administradores implementar Encryption como parte de la imagen corporativa en lugar de utilizar un SCCM de terceros o una solución similar. Para obtener instrucciones acerca de cómo instalar Encryption en una imagen corporativa, consulte el artículo de la base de conocimientos 129990.
- 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.

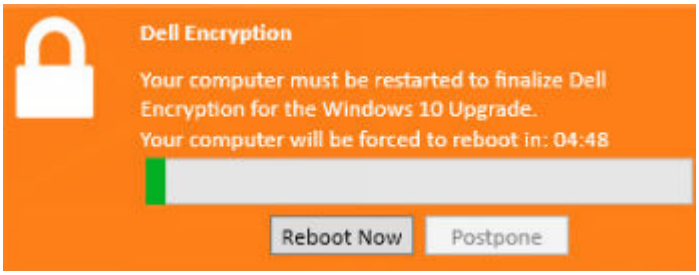
  Si la organización utiliza un proveedor de antivirus que no está en la lista o si observa cualquier problema de compatibilidad, consulte el artículo de la base de conocimientos 126046 o comuníquese con Dell ProSupport para obtener asistencia y validar la configuración de la interoperabilidad entre las soluciones de software y las soluciones de Dell Data Security.

- 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.
- El TPM se usa para sellar la clave de finalidad general. Por lo tanto, si ejecuta Encryption, borre el TPM en el BIOS antes de instalar un sistema operativo nuevo en la computadora de destino.
- No se admite la reinstalación del sistema operativo en el lugar. 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.
- El instalador maestro instala estos componentes si aún no se encuentran instalados en la computadora de destino. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar los clientes.

| **Requisito previo** |
| --- |
| ○ Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 o x64)<br>○ Paquete redistribuible Visual C++ 2017 (x86 o x64)<br>○ A partir de enero de 2020, los certificados de firma SHA1 dejaron de ser válidos y no se pueden renovar. Los dispositivos que ejecutan Windows Server 2008 R2 deben tener instalado Microsoft KB https://support.microsoft.com/help/4474419 y https://support.microsoft.com/help/4490628 para validar los certificados de firma SHA256 en las aplicaciones y los paquetes de instalación.<br>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 |

- Las políticas *Proteger el archivo de hibernación de Windows* y *Evitar la hibernación no protegida* no se admiten en el modo UEFI.
- La activación aplazada permite que la cuenta de usuario de Active Directory que se utiliza durante la activación sea independiente de la cuenta utilizada para iniciar sesión en el extremo. En lugar de que el proveedor de red capture la información de autenticación, el usuario especifica manualmente la cuenta basada en Active Directory cuando se le solicite. Una vez que se ingresan las credenciales, la información de autenticación se envía de forma segura al Dell Server, el cual la valida comparándola con los dominios configurados de Active Directory. Para obtener más información, consulte el artículo de la base de conocimientos 124736.

- 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:




## Hardware

- La siguiente tabla indica el hardware 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)<br>**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.<br>▪ Windows 10 2019 LTSC<br>▪ Windows 10 2021 LTSC<br>○ Windows 11: Enterprise, Pro v21H2-22H2<br>○ La **activación aplazada** incluye compatibilidad con todas las opciones anteriores |

# Encryption External Media

## Sistemas operativos

- 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.
- En la siguiente tabla se indican los sistemas operativos compatibles con el acceso a medios protegidos por Encryption External Media:

| 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)<br>**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.<br>▪ Windows 10 2019 LTSC |

| Sistemas operativos Windows compatibles para el acceso a medios cifrados (32 y 64 bits) |
| --- |
| ▪ Windows 10 2021 LTSC<br>○ Windows 11: Enterprise, Pro v21H2-22H2<br>○ La **activación aplazada** incluye compatibilidad con todas las opciones anteriores |

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

# Cifrado de disco completo

- El cifrado de disco completo requiere activación en un servidor Dell que ejecute la versión 9.8.2 o posterior.
- Full Disk Encryption no es compatible actualmente dentro de equipos host virtualizados.
- Full Disk Encryption requiere un módulo TPM de hardware discreto. PTT y los TPM basados en firmware no son compatibles en este momento.
- Los proveedores de credenciales de terceros no funcionarán con las funciones de FDE instaladas, mientras que todos los proveedores de credenciales de terceros se deshabilitarán cuando se habilite la PBA.
- La computadora cliente debe tener conectividad de red o un código de acceso para activarse.
- La computadora debe contar con una conexión de red con cable para que un usuario con tarjeta inteligente inicie sesión mediante la autenticación previa al arranque por primera vez.
- Las actualizaciones de funciones del sistema operativo no admiten el cifrado de disco completo.
- Se requiere una conexión por cable para que PBA pueda comunicarse con el servidor Dell.
- No puede haber un SED presente en la computadora de destino.
- El cifrado de disco completo no es compatible con BitLocker o BitLocker Manager. No instale el cifrado de disco completo en una computadora donde esté instalado BitLocker o BitLocker Manager.
- Dell recomienda el controlador de Intel Rapid Storage Technology más reciente con unidades NVMe.
- 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 bloquea cuando se cambia 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.
- La administración de Full Disk Encryption no es compatible con las configuraciones de inicio doble, dado que es posible cifrar archivos de sistema del otro sistema operativo, lo cual podría interferir en su funcionamiento.
- No se admite la reinstalación del sistema operativo en el lugar. 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.
- 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 FDE. 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.
- Todos los discos se deben inicializar y formatear antes de habilitar Full Disk Encryption.
- Las configuraciones de cifrado de múltiples discos con Full Disk Encryption requieren lo siguiente:
  - Todos los discos del sistema objetivo deben contar con la siguiente configuración:
    - Unidades no SED
    - Configurados en el mismo modo de arranque
    - Inicializados como tabla de particiones GUID (GPT)

    - Los discos deben ser particiones principales
    - Los discos deben tener una letra de unidad asignada
  - Se requiere reiniciar para cifrar los discos nuevos después de la configuración inicial.
  - Se puede cifrar un máximo de 16 discos.
  - 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.

    Habilite el cifrado de múltiples discos en la consola de administración. Consulte Ajustes de registro a fin de ver los valores del registro de Windows para el cifrado de múltiples discos y el barrido múltiple.

  - Full Disk Encryption 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 Full Disk Encryption, 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.
- El instalador maestro instala estos componentes si aún no se encuentran instalados en la computadora de destino. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar los clientes.

| **Requisito previo** |
| --- |
| ○ Paquete redistribuible Visual C++ 2017 (x86 o x64)<br>○ A partir de enero de 2020, los certificados de firma SHA1 dejaron de ser válidos y no se pueden renovar. Los dispositivos que ejecutan Windows Server 2008 R2 deben tener instalado Microsoft KB https://support.microsoft.com/help/4474419 y https://support.microsoft.com/help/4490628 para validar los certificados de firma SHA256 en las aplicaciones y los paquetes de instalación.<br>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 |

- **NOTA:** Se necesita una contraseña con autenticación previa al arranque. Dell recomienda realizar una configuración mínima de la contraseña para que cumpla con las políticas de seguridad internas.

- **NOTA:** Cuando se usa PBA, la política “Sincronizar todos los usuarios” se debe habilitar si una computadora tiene varios usuarios. Además, todos los usuarios deben tener las contraseñas. Los usuarios con contraseña sin longitud se bloquearán de la computadora después de la activación.
- **NOTA:** Las computadoras protegidas con Full Disk Encryption 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.

**NOTA:** Full Disk Encryption debe estar configurado con algoritmo de cifrado establecido en AES-256 y con el modo de cifrado establecido en CBC.

## Hardware

- La siguiente tabla indica el hardware compatible.

| **Hardware integrado opcional** |
| --- |
| ○ TPM 1.2 o 2.0 |

## Opciones de autenticación con el cliente Full Disk Encryption

- Se requiere hardware específico, para utilizar tarjetas inteligentes y para autenticar en computadoras UEFI. Se requiere una configuración para utilizar tarjetas inteligentes con autenticación previa al arranque. Las tablas siguientes muestran opciones de autenticación disponibles, por sistema operativo, cuando se cumplan los requisitos de hardware y de configuración.

| UEFI | | | | |
|---|---|---|---|---|
| | PBA - en computadoras Dell compatibles | | | |
| | Contraseña | Huellas digitales | Tarjeta inteligente con contacto | Tarjeta SIPR |
| Windows 10 | X[1] | | X[1] | |
| Windows 11 | X[1] | | X[1] | |
| 1. Disponible con computadoras con UEFI compatible. | | | | |

## Modelos de computadoras Dell compatibles con el modo de arranque UEFI

- Para obtener la lista más actualizada de las plataformas compatibles con Full Disk Encryption, consulte el artículo de la base de conocimientos 126855.
- Para obtener una lista de estaciones de acoplamiento y adaptadores compatibles con Full Disk Encryption, consulte el artículo de la base de conocimientos 124241.

## Sistemas operativos

- La tabla siguiente indica los sistemas operativos compatibles.

| Sistemas operativos Windows (de 64 bits) |
|---|
| ○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2)<br>**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.<br>■ Windows 10 2019 LTSC<br>■ Windows 10 2021 LTSC<br>○ Windows 11: Enterprise, Pro v21H2-22H2 |

# Encryption en sistemas operativos de servidor

Encryption de sistemas operativos de servidor está diseñado para que se utilice en computadoras que funcionan en modo servidor, particularmente en servidores de archivos.

- Encryption en sistemas operativos de servidor solo es compatible con Encryption Enterprise y Endpoint Security Suite Enterprise.
- Encryption en sistemas operativos de servidor ofrece:
  - Cifrado de software
  - Cifrado de medios extraíbles
  - Controles de puerto

**NOTA:**

El servidor debe admitir controles de puerto.

Las políticas de sistema de control de puertos afectan a medios extraíbles en servidores protegidos, por ejemplo, mediante el control del acceso y el uso de los puertos USB del servidor por parte de dispositivos USB. La política de puertos USB se aplica a los puertos USB externos. La funcionalidad interna de puerto USB no se ve afectada por la política de puertos USB. Si se deshabilita la política de puertos USB, el teclado y mouse del USB cliente no

funcionarán y el usuario no podrá utilizar la computadora, a menos que se configure una Conexión de escritorio remoto antes de aplicar la política.

- El instalador maestro instala estos componentes si aún no se encuentran instalados en la computadora de destino. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar los clientes.

| **Requisito previo** |
| --- |
| ○ Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 o x64)<br>○ Paquete redistribuible Visual C++ 2017 (x86 o x64)<br>○ A partir de enero de 2020, los certificados de firma SHA1 dejaron de ser válidos y no se pueden renovar. Los dispositivos que ejecutan Windows Server 2008 R2 deben tener instalado Microsoft KB https://support.microsoft.com/help/4474419 y https://support.microsoft.com/help/4490628 para validar los certificados de firma SHA256 en las aplicaciones y los paquetes de instalación.<br>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 |

**Encryption de sistemas operativos de servidor se usa con:**

- Servidores de archivos con unidades locales
- Huéspedes de máquinas virtuales (VM) que ejecutan un sistema operativo de servidor o un sistema operativo que no es de servidor como un servidor de archivos simple
- Configuraciones admitidas:
  - Servidores equipados con RAID 5 o 10 unidades; RAID 0 (división de datos en bloques) y RAID 1 (duplicación) se admiten independientes entre sí.
  - Servidores equipados con unidades RAID de varios TB
  - Servidores equipados con unidades que pueden cambiarse sin apagar el equipo
  - Server Encryption se valida con los proveedores de antivirus líderes del sector. Se aplican exclusiones no modificables para estos proveedores de antivirus con el fin de evitar incompatibilidades entre la detección del antivirus y el cifrado. Si su organización utiliza un proveedor antivirus que no se encuentra incluido, consulte el artículo de la base de conocimientos 126046 o comuníquese con Dell ProSupport para obtener asistencia.

**Encryption de sistemas operativos de servidor no se usa con:**

- Security Management Servers/Security Management Server Virtuals o los servidores que ejecutan bases de datos para Security Management Servers/Security Management Server Virtual.
- Encryption Personal.
- SED Manager, PBA Advanced Authentication o BitLocker Manager.
- Servidores que forman parte de sistemas de archivos distribuidos (DFS).
- Migración hacia o desde Encryption en un sistema operativo de servidor. La actualización de External Media Edition a Encryption de sistemas operativos de servidor requiere que el producto anterior se desinstale por completo antes de instalar Encryption en sistemas operativos de servidor.
- Hosts de VM (un host de VM suele contener varios huéspedes de VM).
- Controladoras de dominio
- Servidores de Exchange
- Servidores que alojen bases de datos (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Servidores que utilicen alguna de las siguientes tecnologías:
  - Sistemas de archivo resistentes
  - Fluid File Systems
  - Espacios de almacenamiento Microsoft
  - Soluciones de almacenamiento de red SAN/NAS
  - Dispositivos conectados iSCSI
  - Software de desduplicación
  - Desduplicación de hardware
  - RAID divididos (varios volúmenes a través de un único RAID)
  - SED (RAID y distinto de RAID)
  - Microsoft Storage Server 2012
- Encryption en sistema operativo de servidor no es compatible con las configuraciones de inicio doble, dado que es posible cifrar archivos de sistema del otro sistema operativo, lo cual podría interferir en su funcionamiento.

- No se admite la reinstalación del sistema operativo en el lugar. Para volver a instalar el sistema operativo, realice un respaldo de la computadora de destino, borre la computadora, instale el sistema operativo y, a continuación, recupere los datos cifrados siguiendo los procedimientos de recuperación. Para obtener más información acerca de la recuperación de los datos cifrados, consulte *Recovery Guide*.

## Sistemas operativos

La tabla siguiente indica los sistemas operativos compatibles.

| **Sistemas operativos (32 y 64 bits)** |
| --- |
| • Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2)<br><br>**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.<br><br>○ Windows 10 2019 LTSC<br>○ Windows 10 2021 LTSC<br>• Windows 11: Enterprise, Pro v21H2-22H2<br>• La **activación aplazada** incluye compatibilidad con todas las opciones anteriores |

| **Sistemas operativos de servidor compatibles** |
| --- |
| • Windows Server 2008 R2 SP1: Standard Edition, Essentials Edition, Foundation Edition y Datacenter Edition<br>• Windows Server 2012: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)<br>• Windows Server 2012 R2: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)<br>• Windows Server 2016: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)<br>• Windows Server 2019: Standard Edition, Datacenter Edition<br>• Windows Server 2022: Standard Edition, Datacenter Edition |

| **Sistemas operativos compatibles con el modo de UEFI** |
| --- |
| • Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2)<br><br>**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.<br><br>○ Windows 10 2019 LTSC<br>○ Windows 10 2021 LTSC<br>• Windows 11: Enterprise, Pro v21H2-22H2 |

**NOTA:**

En un equipo compatible con UEFI, después de seleccionar **Reiniciar** en el menú principal, el equipo se reinicia y a continuación muestra una de las dos posibles pantallas de inicio. La pantalla de inicio que aparece la determinan las diferencias en la arquitectura de la plataforma del equipo.

# Encryption External Media

## Sistemas operativos

- 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 detallan los sistemas operativos compatibles 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)<br>**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.<br>○ Windows 10 2019 LTSC<br>○ Windows 10 2021 LTSC<br>• Windows 11: Enterprise, Pro v21H2-22H2<br>• La **activación aplazada** incluye compatibilidad con todas las opciones anteriores |

| Sistemas operativos de servidor compatibles |
| --- |
| • Windows Server 2012 R2 |

| Sistemas operativos Mac compatibles para el acceso a medios cifrados (núcleos de 64 bits) |
| --- |
| • macOS High Sierra 10.13.5 - 10.13.6<br>• macOS Mojave 10.14.0 - 10.14.4<br>• macOS Catalina 10.15.1 - 10.15.4 |

# SED Manager

- La computadora debe tener una conexión de red por cable para que SED Manager se instale correctamente.
- La computadora debe contar con una conexión de red por cable para que un usuario con tarjeta inteligente inicie sesión mediante la autenticación previa al arranque por primera vez.
- Los proveedores de credenciales de terceros no funcionarán con SED Manager instalado, mientras que todos los proveedores de credenciales de terceros se deshabilitarán cuando se habilite la PBA.
- No es compatible con IPv6.
- SED Manager no es compatible actualmente dentro de equipos host virtualizados.
- 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 arranque no es compatible con esta opción de Active Directory.
- Dell recomienda no cambiar el método de autenticación después de haber activado la PBA. En caso de que tenga que cambiar a un método de autenticación diferente, deberá:
  - Quitar todos los usuarios de la PBA.

    O bien
  - Desactivar la PBA, cambiar el método de autenticación y, a continuación, volver a activar la PBA.
- 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.

**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.

- 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.
- El instalador maestro instala estos componentes si aún no se encuentran instalados en la computadora de destino. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar los clientes.

| **Requisito previo** |
| --- |
| ○ Paquete redistribuible Visual C++ 2017 (x86 o x64)<br>○ A partir de enero de 2020, los certificados de firma SHA1 dejaron de ser válidos y no se pueden renovar. Los dispositivos que ejecutan Windows Server 2008 R2 deben tener instalado Microsoft KB https://support.microsoft.com/help/4474419 y https://support.microsoft.com/help/4490628 para validar los certificados de firma SHA256 en las aplicaciones y los paquetes de instalación.<br>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 |

- SED Manager no es compatible con Encryption en sistemas operativos de servidor .
- Las configuraciones de cifrado de múltiples discos con SED Manager requieren lo siguiente:
  - Todos los discos del sistema objetivo deben contar con la siguiente configuración:
    - Unidades SED
    - Los discos deben tener una letra de unidad asignada
  - 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.

    Habilite el cifrado de múltiples discos en la consola de administración. Consulte Ajustes de registro a fin de ver los valores del registro de Windows para el cifrado de múltiples discos y el barrido múltiple.
- **NOTA:** Se necesita una contraseña con autenticación previa al arranque. Dell recomienda realizar una configuración mínima de la contraseña para que cumpla con las políticas de seguridad internas.
- **NOTA:** Cuando se usa PBA, la política “Sincronizar todos los usuarios” se debe habilitar si una computadora tiene varios usuarios. Además, todos los usuarios deben tener las contraseñas. 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.
-

# Hardware

### SED que cumplen con OPAL

- Para obtener la lista más reciente de SED compatibles con Opal admitidos en SED Manager, 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.

## Opciones de autenticación previa al arranque con SED Manager

- Se requiere hardware específico para utilizar tarjetas inteligentes y para autenticar en computadoras UEFI. Se requiere una configuración para utilizar tarjetas inteligentes con autenticación previa al arranque. Las tablas siguientes muestran opciones de autenticación disponibles, por sistema operativo, cuando se cumplan los requisitos de hardware y de configuración.

| **Sin UEFI** | | | | |
|---|---|---|---|---|
| | **PBA** | | | |
| | **Contraseña** | **Huellas digitales** | **Tarjeta inteligente con contacto** | **Tarjeta SIPR** |
| Windows 10 | X[1] | | X[1 2] | |
| Windows 11 | X[1] | | X[1 2] | |
| 1. Disponible cuando se descargan los controladores de autenticación de dell.com/support<br>2. Disponible con SED OPAL compatible | | | | |

| **UEFI** | | | | |
|---|---|---|---|---|
| | **PBA - en computadoras Dell compatibles** | | | |
| | **Contraseña** | **Huellas digitales** | **Tarjeta inteligente con contacto** | **Tarjeta SIPR** |
| Windows 10 | X[1] | | X[1] | |
| Windows 11 | X[1] | | X[1] | |
| 1. Disponible con un SED OPAL compatible en computadoras UEFI compatibles | | | | |

## 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)<br>**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.<br>■ Windows 10 2019 LTSC<br>■ Windows 10 2021 LTSC<br>○ Windows 11: Enterprise, Pro v21H2-22H2 |

## 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. El modo UEFI y PBA Advanced Authentication son compatibles 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) | |

# BitLocker Manager

- Revise Requisitos de Microsoft BitLocker si BitLocker todavía no está implementado en su entorno,
- Asegúrese de que la partición de PBA ya esté configurada. Si se instala BitLocker Manager antes de configurar la partición PBA, BitLocker no se podrá habilitar y BitLocker Manager no funcionará. Consulte Configuración previa a la instalación para establecer una partición de PBA de BitLocker.
- Es necesario un Dell Server para utilizar BitLocker Manager.
- Asegúrese de que hay un certificado de firma disponible en la base de datos. Para obtener más información, consulte el artículo de la base de conocimientos 124931.
- El teclado, el mouse y los componentes de video deben estar conectados directamente al equipo. No use un conmutador KVM para administrar los periféricos, ya que el conmutador KVM puede interferir en la capacidad del equipo para identificar el hardware correctamente.
- Encienda y habilite el Trusted Platform Module (TPM). BitLocker Manager tomará propiedad del TPM y no requerirá un reinicio. Sin embargo, si ya existe propietario del TPM, BitLocker Manager comenzará el proceso de configuración de cifrado (no se requiere reinicio). La cuestión es que el TPM debe ser con propietario y estar habilitado.
- BitLocker Manager utiliza los algoritmos validados FIPS AES aprobados si el modo FIPS está habilitado para la configuración de seguridad GPO “Criptografía del sistema: utilice los algoritmos compatibles con FIPS para el cifrado, el hashing y la firma” en el dispositivo y administre ese dispositivo mediante nuestro producto. BitLocker Manager no fuerza este modo como predeterminado para los clientes cifrados por BitLocker porque Microsoft ahora sugiere que los clientes no utilicen su cifrado validado FIPS debido a varios problemas con la compatibilidad de la aplicación, la recuperación y el cifrado de medios: http://blogs.technet.com.
- BitLocker Manager no es compatible con Encryption de sistemas operativos de servidor.

- Cuando se utiliza una conexión a escritorio remoto con un terminal que aprovecha BitLocker Manager, Dell recomienda ejecutar cualquier sesión de escritorio remoto en modo de consola para evitar que no haya ningún problema de interacción con la interfaz de usuario en la sesión de usuario existente a través del siguiente comando:

  ```
  mstsc /admin /v:<target_ip_address>
  ```

- El instalador maestro instala estos componentes si aún no se encuentran instalados en la computadora de destino. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar los clientes.

| Requisito previo |
| --- |
| ○ Paquete redistribuible Visual C++ 2017 (x86 o x64)<br>○ A partir de enero de 2020, los certificados de firma SHA1 dejaron de ser válidos y no se pueden renovar. Los dispositivos que ejecutan Windows Server 2008 R2 deben tener instalado Microsoft KB https://support.microsoft.com/help/4474419 y https://support.microsoft.com/help/4490628 para validar los certificados de firma SHA256 en las aplicaciones y los paquetes de instalación.<br>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 |

- **NOTA:** Las computadoras protegidas con Bitlocker 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.
- **NOTA:** No se soportan las actualizaciones locales de sistemas operativos a nuevas versiones, como actualizaciones de Windows 10 a Windows 11.

## Hardware

- La siguiente tabla indica el hardware compatible.

| Hardware integrado opcional |
| --- |
| ○ TPM 1.2 o 2.0 |

## Sistemas operativos

- En las siguientes tablas, se indican los sistemas operativos soportados.

| Sistemas operativos Windows |
| --- |
| ○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (actualización de noviembre del 2019/19H2 - actualización de noviembre del 2022/22H2)<br>**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.<br>■ Windows 10 2019 LTSC<br>■ Windows 10 2021 LTSC<br>○ Windows 11: Enterprise, Pro v21H2-22H2 |

| Sistemas operativos Windows Server |
| --- |
| ○ Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)<br>○ Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)<br>○ Windows Server 2016: Standard Edition, Datacenter Edition (64 bits)<br>○ Windows Server 2019: Standard Edition, Datacenter Edition (64 bits)<br>○ Windows Server 2022: Standard Edition, Datacenter Edition |

# 3

# Configuración de registro

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

## Cifrado

- Si un certificado autofirmado se utiliza en Dell Server. En el caso de Windows, la validación de confianza de certificado debe permanecer desactivada en la computadora cliente (la validación de confianza está *desactivada* de manera predeterminada en Dell Server). Antes de *habilitar* la validación de confianza en el equipo cliente, deben cumplirse los siguientes requisitos.
  - Un certificado firmado por una autoridad raíz, por ejemplo, EnTrust o Verisign, deberá importarse al Dell Server.
  - La cadena completa de confianza del certificado deberá ser almacenada en el keystore de Microsoft del equipo cliente.
  - Para *habilitar* la validación de confianza para Encryption, cambie el valor de la siguiente entrada de registro a 0 en la computadora de destino.

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

    "IgnoreCertErrors"=DWORD:00000000

    0 = Falla si se encuentra un error de certificado

    1= Ignora errores

- Para crear un archivo de registro de Encryption Removal Agent, cree la siguiente entrada de registro en el equipo de destino para el descifrado. Consulte (Opcional) Crearción de un archivo de registro de Encryption Removal Agent.

  [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

- 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 o modifique la política *Forzar reinicio al actualizar* en la consola de administración.

  [HKLM\Software\Dell\Dell Data Protection]

  "ShowDecryptAgentRebootPrompt"=DWORD

  1 = habilitado (muestra el indicador)

  0 = deshabilitado (oculta el indicador)

- De forma predeterminada, durante la instalación, aparece el icono del área de notificación. Utilice la siguiente configuración de registro para ocultar el icono del área de notificación de todos los usuarios administrados en una computadora tras la instalación original. Cree o modifique el parámetro de registro:

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=DWORD:1

- 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.

- Encryption muestra el indicador de *duración de cada retraso de actualización de política* durante cinco minutos cada vez. Si el usuario no responde a la indicación, comenzará el siguiente retraso. La indicación de retraso final incluye una cuenta atrás y una barra de progreso, y se visualiza hasta que el usuario responde o el retraso final caduca y se produce el cierre de sesión/reinicio requerido.

  Puede cambiar el comportamiento de la indicación al usuario para iniciar o retrasar el cifrado, para evitar el procesamiento del cifrado cuando el usuario no responda a la indicación. Para ello, establezca el 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])

- Utilice la configuración de registro para que Encryption sondee Dell Server en busca de una actualización de política aplicada. Cree o modifique el parámetro de registro:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  La configuración de registro desaparece automáticamente cuando finaliza.

- Utilice la configuración de registro para permitir que Encryption envíe un inventario optimizado y completo (usuarios activados y no activados) o completo (solo usuarios activados) a Dell Server.
  - Envíe el inventario optimizado al Dell Server:

    Cree o modifique el parámetro de registro:

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

    "OnlySendInvChanges"=REG_DWORD:1

    Si no hay ninguna entrada, el inventario optimizado se enviará al Dell Server.

  - Envíe el inventario completo al Dell Server:

    Cree o modifique el parámetro de registro:

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

    "OnlySendInvChanges"=REG_DWORD:0

    Si no hay ninguna entrada, el inventario optimizado se enviará al Dell Server.

  - Enviar el inventario completo para todos los usuarios activados

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

    "RefreshInventory"=REG_DWORD:1

    Esta entrada se elimina del registro tan pronto como se procese. El valor se guarda en el almacén, así que incluso si la computadora se reinicia antes de que tenga lugar la carga del inventario, Encryption sigue respetando esta solicitud la próxima vez que se cargue correctamente el inventario.

    Esta entrada sustituye el valor de registro OnlySendInvChanges.

- La activación ranurada es una función que le permite repartir activaciones de clientes durante un período establecido para facilitar la carga del Dell Server durante una implementación masiva. Las activaciones se retrasan en función de ranuras generadas algorítmicamente para ofrecer una distribución progresiva de los tiempos de activación.

  Para usuarios que requieran activación a través de VPN, puede que sea necesaria una configuración de activación ranurada para el cliente, para retrasar la activación inicial durante el tiempo suficiente para permitir que el cliente VPN establezca una conexión de red.

  Estas entradas de registro requieren un reinicio del equipo para que las actualizaciones surtan efecto.

  - **Activación ranurada**

    Para habilitar o deshabilitar esta función, cree un DWORD con el nombre **SlottedActivation** en la clave principal:

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

  - **Ranura de activación**

    Para habilitar o deshabilitar esta función, cree una subclave con el nombre **ActivationSlot** en la clave principal:

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

    Ranura de activación: cadena que define el período en el que Encryption intenta la activación con Dell Server. Estos valores se definen en segundos y la sintaxis se define mediante <lowervalue>,<uppervalue>. Un ejemplo sería 120,300. Esto significa que Encryption intenta la activación en un tiempo aleatorio entre 2 minutos y 5 minutos después del inicio de sesión del usuario.

    - **Repetición del calendario**

      Para habilitar o deshabilitar esta función, cree una subclave con el nombre **CalRepeat** en la clave principal:

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

      CalRepeat: un DWORD que define el período en segundos en que se produce el intervalo de ranura de activación. Utilice esta configuración para invalidar el período en segundos en que se produce el intervalo de ranura de activación. Dispone de 25.200 segundos para las activaciones ranuradas durante un período de siete horas. El valor predeterminado es 86.400 segundos, que representa una repetición diaria. El valor decimal sugerido es 600, que representa 10 minutos.

    - **Intervalo de ranura**

      Para habilitar o deshabilitar esta función, cree una subclave con el nombre **SlotInterval** en la clave principal:

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

      Intervalo de ranura: valor de cadena que define los intervalos entre activaciones de ranuras. La configuración sugerida es 45,120. Esto representa el tiempo de activación que se asigna aleatoriamente entre 45 y 120 segundos.

    - **Umbral de fallas**

      Para habilitar o deshabilitar esta función, cree una subclave con el nombre **MissThreshold** en la clave principal:

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

      MissThreshold: valor DWORD que contiene un número entero positivo que define la cantidad de intentos de activación antes de que se requiera el cierre de sesión. Si se alcanza el MissThreshold, cesarán los intentos de activación hasta el siguiente inicio de sesión del usuario no activado. El recuento de MissThreshold siempre es el restablecimiento de cierre de sesión.

      Las claves de registro recopilan datos de usuario de activación ranurada:

      [HKCU/Software/CREDANT/ActivationSlot] (datos por usuario)

      Tiempo aplazado para intentar la activación ranurada, que se establece cuando el usuario inicia sesión en la red por primera vez tras haber habilitado la activación ranurada. La ranura de activación se vuelve a calcular para cada intento de activación.

      [HKCU/Software/CREDANT/SlotAttemptCount] (datos por usuario)

      Número de intentos fallidos o perdidos, cuando la ranura de tiempo llega y se intenta la activación, pero falla. Cuando este número alcanza el valor establecido en ACTIVATION_SLOT_MISSTHRESHOLD, el equipo intenta una activación inmediata al conectarse a la red.

- Para detectar usuarios no administrados en la computadora cliente, establezca el valor de registro en la computadora cliente:

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=DWORD value:1

Detectar usuarios no administrados en este equipo=1

No detectar usuarios no administrados en este equipo=0

- El acceso a medios externos cifrados con Encryption External Media se puede restringir a computadoras con acceso al Dell Server que generó las claves de cifrado con las que se cifraron los medios.

  Esta función se habilita con la configuración del registro:

  [ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

  "EnterpriseUsage"=DWORD:0

  Desactivado (valor predeterminado)=0

  Acceso de archivos restringido para Enterprise=1

  Si se cambia este valor después de cifrar archivos en medios externos, se realizará de nuevo el cifrado de los archivos según el valor actualizado de la clave de registro cuando el medio se conecte a la computadora en la que se actualizó el ajuste del registro.

- Para habilitar la reactivación automática silenciosa en el caso poco frecuente de que un usuario se desactive, el valor de registro se debe establecer en la computadora del cliente.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=DWORD:00000001

  0 =Deshabilitado (valor predeterminado)

  1 =Habilitado

- 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 el registro en la computadora:

  [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.

  Para obtener más información sobre SDUser, consulte el artículo de la base de conocimientos 131035.

- Establezca la entrada de registro EnableNGMetadata si se producen problemas relacionados con actualizaciones de Microsoft en equipos con datos cifrados con clave común o con cifrado, descifrado o descompresión de un número elevado de archivos en una carpeta.

  Establezca la entrada de registro EnableNGMetadata en la siguiente ubicación:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = DWORD:1

  0 =Deshabilitado (valor predeterminado)

  1 =Habilitado

- Puede activar la función de activación sin dominio si se comunica con el equipo de Dell ProSupport y solicita instrucciones para hacerlo.
- 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\

  "DumpPolicies" = DWORD

  Value=1

  **Nota:** Los registros se escriben en C:\ProgramData\Dell\Dell Data Protection\Policy.

- 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

# SED Manager

- Para establecer el intervalo de reintentos cuando Dell Server no esté disponible para comunicarse con SED Manager, agregue el siguiente valor de registro.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Este valor es la cantidad de segundos que SED Manager espera para intentar comunicarse con Dell Server si este no está disponible para comunicarse. El valor predeterminado es 300 segundos (5 minutos).

- Si se utiliza un certificado autofirmado en Dell Server para SED Manager, la validación de confianza de SSL/TLS deberá permanecer deshabilitada en la computadora cliente (la validación de confianza de SSL/TLS está *deshabilitada* de forma predeterminada en SED Manager). Antes de *habilitar* la validación de confianza de SSL/TLS en el equipo cliente, deberán cumplirse los siguientes requisitos.
  - Un certificado firmado por una autoridad raíz, por ejemplo, EnTrust o Verisign, deberá importarse al Dell Server.
  - La cadena completa de confianza del certificado deberá ser almacenada en el keystore de Microsoft del equipo cliente.
  - Para *habilitar* la validación de confianza de SSL/TLS en SED Manager, cambie el valor de la siguiente entrada de registro a 0 en la computadora cliente.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Habilitado

    1 = Deshabilitado

- 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.

- 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

- Para evitar que SED Manager 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

**NOTA:** Este valor puede impedir que el proveedor de credenciales de Dell sincronice correctamente las credenciales, debido a que los proveedores de credenciales de terceros están deshabilitados. Asegúrese de que los dispositivos que utilizan esta clave de registro se pueden comunicar correctamente con el servidor Dell.

- Para establecer el intervalo con el que SED Manager intenta comunicarse con Dell Server cuando este no está disponible para comunicarse, establezca el siguiente valor en la computadora de destino:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD Value:300

  Este valor es la cantidad de segundos que SED Manager espera para intentar comunicarse con Dell Server si este no está disponible para comunicarse. El valor predeterminado es 300 segundos (5 minutos).

- El host de Security Server puede cambiarse desde la ubicación de instalación original, si fuera necesario. La información de host se lee cada vez que se produce un sondeo de la política. Cambie el siguiente valor de registro en el equipo cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- El puerto de Security Server puede cambiarse desde la ubicación de instalación original, si fuera necesario. Este valor se lee cada vez que se produce un sondeo de la política. Cambie el siguiente valor de registro en el equipo cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- La dirección URL de Security Server puede cambiarse desde la ubicación de instalación original, si fuera necesario. Este valor se lee en el cliente cada vez que se produce un sondeo de la política. Cambie el siguiente valor de registro en el equipo cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

- (Solo con autenticación previa al arranque) Si **no** desea que PBA Advanced Authentication cambie los servicios asociados a las tarjetas inteligentes y los dispositivos biométricos a un tipo de inicio “automático”, deshabilite la función de inicio del servicio. La deshabilitación de esta función también suprime los avisos asociados con el mal funcionamiento de los servicios necesarios.

  Cuando está **deshabilitado**, PBA Advanced Authentication no trata de iniciar estos 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.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Habilitado

    1 = Deshabilitado

- Para utilizar tarjetas inteligentes con PBA Authentication de SED, el valor de registro siguiente debe estar establecido en la computadora cliente equipada con un SED.

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

  "MSSmartcardSupport"=DWORD:1

  Establezca la política Método de autenticación en Tarjeta inteligente en la consola de administración y confirme el cambio.

- 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

# Cifrado de disco completo

- En esta sección, se detalla toda la configuración de registro aprobada por Dell ProSupport para computadoras locales, independientemente del motivo de la configuración de registro. Si una configuración de registro coincide con dos productos, aparecerá en cada categoría.
- Estos cambios de registro deben realizarlos únicamente los administradores y es posible que no sean adecuados para todas las situaciones ni que funcionen en todas ellas.
- Para establecer el intervalo de reintentos cuando Dell Server no esté disponible para comunicarse con Full Disk Encryption, agregue el siguiente valor de registro.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Este valor es la cantidad de segundos que Full Disk Encryption espera para intentar contactarse con Dell Server si este no está disponible para comunicarse con Full Disk Encryption. El valor predeterminado es 300 segundos (5 minutos).

- Si se utiliza un certificado autofirmado en Dell Server para Full Disk Encryption, la validación de confianza de SSL/TLS deberá permanecer deshabilitada en la computadora cliente (la validación de confianza de SSL/TLS está *deshabilitada* de forma predeterminada con Full Disk Encryption). Antes de *habilitar* la validación de confianza de SSL/TLS en el equipo cliente, deberán cumplirse los siguientes requisitos.
  - Un certificado firmado por una autoridad raíz, por ejemplo, EnTrust o Verisign, deberá importarse al Dell Server.
  - La cadena completa de confianza del certificado deberá ser almacenada en el keystore de Microsoft del equipo cliente.
  - Para *habilitar* la validación de confianza de SSL/TLS para la administración de Dell Encryption, cambie el valor de la siguiente entrada de registro a 0 en la computadora cliente.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Habilitado

    1 = Deshabilitado

- 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

- El host de Security Server puede cambiarse desde la ubicación de instalación original, si fuera necesario. La información de host se lee en el equipo cliente cada vez que se produce un sondeo de la política. Cambie el siguiente valor de registro en el equipo cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- El puerto de Security Server puede cambiarse desde la ubicación de instalación original, si fuera necesario. Este valor se lee en el cliente cada vez que se produce un sondeo de la política. Cambie el siguiente valor de registro en el equipo cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- (Solo con autenticación previa al arranque) Si **no** desea que PBA Advanced Authentication cambie los servicios asociados a las tarjetas inteligentes y los dispositivos biométricos a un tipo de inicio "automático", deshabilite la función de inicio del servicio. La deshabilitación de esta función también suprime los avisos asociados con el mal funcionamiento de los servicios necesarios.

  Cuando está **deshabilitado**, PBA Advanced Authentication no trata de iniciar estos 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.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Habilitado

    1 = Deshabilitado

- Para evitar que Full Disk Encryption 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

  **NOTA:** Este valor puede impedir que el proveedor de credenciales de Dell sincronice correctamente las credenciales, debido a que los proveedores de credenciales de terceros están deshabilitados. Asegúrese de que los dispositivos que utilizan esta clave de registro se pueden comunicar correctamente con el servidor Dell.

- 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

- Para permitir la instalación de Full Disk Encryption con cifrado basado en políticas, se debe configurar el siguiente valor de registro en la computadora cliente.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  " EnableFDE" = DWORD: 1

0 =Deshabilitado (valor predeterminado)

1 =Habilitado

# BitLocker Manager

- Si se utiliza un certificado autofirmado en el Dell Server para BitLocker Manager, la validación de confianza de SSL/TLS deberá permanecer deshabilitada en la computadora cliente (la validación de confianza de SSL/TLS está *deshabilitada* de forma predeterminada con BitLocker Manager). Antes de *habilitar* la validación de confianza de SSL/TLS en el equipo cliente, deberán cumplirse los siguientes requisitos.
  - Un certificado firmado por una autoridad raíz, por ejemplo, EnTrust o Verisign, deberá importarse al Dell Server.
  - La cadena completa de confianza del certificado deberá ser almacenada en el keystore de Microsoft del equipo cliente.
  - Para *habilitar* la validación de confianza de SSL/TLS para BitLocker Manager, cambie el valor de la siguiente entrada de registro a 0 en la computadora cliente.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Habilitado

    1 = Deshabilitado
  - Para evitar que BitLocker Manager detecte discos extraíbles como discos fijos, agregue la siguiente clave de registro:

    HKLM\Software\Dell\Dell Data Protection\

    "UseEncryptableVolumeType" = DWORD:1

    0 =Deshabilitado (valor predeterminado)

    1 =Habilitado

# 4

# Instalación mediante el instalador maestro

- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Para instalar mediante puertos no predeterminados, utilice los instaladores secundarios en lugar del instalador maestro.
- Los archivos de registro del instalador maestro se encuentran en `C:\ProgramData\Dell\Dell Data Protection\Installer`.

  **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.

- Indique a los usuarios que consulten el siguiente documento y los archivos de ayuda para obtener ayuda sobre la aplicación:
  - 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\EMS`.
  - Consulte la ayuda de *Encryption Enterprise*para obtener información sobre el uso de estas funciones de . Acceda a la ayuda desde `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.
- Los usuarios deben actualizar sus políticas haciendo clic con el botón secundario en el icono de Dell Encryption del área de notificación y seleccionando **Comprobar si existen actualizaciones de políticas** una vez finalizada la instalación.
- El instalador maestro instala todo el conjunto de productos. Existen dos métodos para realizar la instalación con el instalador maestro. Elija una de las siguientes opciones.
  - Instalación interactiva mediante el instalador maestro

  O bien
  - Instalación mediante la línea de comandos con el instalador maestro

# Instalación interactiva mediante el instalador maestro

- El instalador maestro de se puede encontrar en:
  - **En dell.com/support**: si es necesario, obtenga el software en **dell.com/support**
  - **En su cuenta FTP de Dell:** localice el paquete de instalación en Dell-Encryption-8.x.x.xxx.zip
- Utilice estas instrucciones para instalar o actualizar Dell Encryption Enterprise de forma interactiva con el instalador principal de . Este método se puede usar para instalar el conjunto de productos en un equipo al mismo tiempo.

1. Localice el archivo **DDSSetup.exe** en el medio de instalación de Dell. Cópielo al equipo local.
2. Haga doble clic en para iniciar el instalador. Esto puede tardar varios minutos.
3. Haga clic en **Siguiente** en el cuadro de diálogo de bienvenida.
4. Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
5. En *Nombre de servidor Dell local*, ingrese el nombre completo del host del servidor Dell para administrar al usuario objetivo.

   Ingrese los valores de puerto en *Puerto del servidor principal* y en *Puerto del servidor de seguridad* si su organización usa puertos no estándares.

   Haga clic en **Siguiente**.
6. Haga clic en **Siguiente** para instalar el producto en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only`, ya que se pueden producir problemas si lo instala en otras ubicaciones.
7. Seleccione los componentes que va a instalar.

   *Security Framework* instala el esquema de seguridad subyacente, Encryption Management Agent y PBA Authentication.

BitLocker Manager instala el cliente de BitLocker Manager, diseñado para mejorar la seguridad de las implementaciones de BitLocker simplificando y reduciendo el costo de propiedad a través de una administración centralizada de las políticas de cifrado de BitLocker.

*Encryption* instala el componente que aplica la política de seguridad, independientemente de que una computadora esté conectada a la red, esté desconectada de esta, se haya perdido o la hayan robado.

*Encryption External Media* instala el componente que aplica Encryption External Media.

*Full Disk Encryption* instala el componente que aplica Full Disk Encryption.

Haga clic en **Siguiente** una vez haya terminado de realizar las selecciones.

8. Haga clic en **Instalar** para comenzar la instalación. La instalación tarda varios minutos.
9. Seleccione **Sí, deseo reiniciar ahora mi equipo** y haga clic en **Finalizar**.

   La instalación finalizó.

# Instalación mediante la línea de comandos con el instalador maestro

- Los conmutadores se deben especificar en primer lugar en la instalación de una línea de comandos. Otros parámetros se introducen en el argumento que luego pasa al modificador /v.

**Modificadores**

- En la siguiente tabla se describen los switches que se pueden utilizar con el instalador maestro de .

  **NOTA:** Si su organización requiere el uso de proveedores de credenciales de terceros, debe instalar o actualizar Encryption Management Agent con el parámetro FEATURE=BLM o FEATURE=BASIC.

| Modificador | Descripción |
|---|---|
| /s | Instalación silenciosa |
| /z | Envía las variables al archivo .msi dentro de DDSSetup.exe |

**Parámetros**

- En la siguiente tabla se describen los parámetros que se pueden utilizar con el instalador maestro de .

| Parámetro | Descripción |
|---|---|
| SUPPRESSREBOOT | Suprime el reinicio automático al terminar la instalación. Se puede utilizar en modo SILENCIOSO. |
| SERVER | Especifica la dirección URL del Dell Server. |
| InstallPath | Indica la ruta de la instalación. Se puede utilizar en modo SILENCIOSO. |
| FEATURES | Especifica los componentes que se pueden instalar en modo SILENCIOSO.<br>DE = cliente del cifrado de disco solamente<br>EME = Encryption External Media solo<br>BLM = BitLocker Manager<br>SED = SED Manager (Encryption Management Agent/Manager, controladores PBA/GPE) |
| BLM_ONLY=1 | Debe utilizarse cuando se especifica FEATURES=BLM en la línea de comandos para excluir el complemento SED Manager. |

**Ejemplo de línea de comandos**

- Los parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.

- En este ejemplo se instalan todos los componentes mediante el instalador maestro de en puertos estándar, de manera silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com\""
  ```

- En este ejemplo, se instalan SED Manager y Encryption External Media con el instalador maestro, en puertos estándar, de forma silenciosa, con un reinicio suprimido, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=EME-SED,
  SUPPRESSREBOOT=1\""
  ```

- En este ejemplo, se instala SED Manager con el instalador maestro, en puertos estándar, de forma silenciosa, con un reinicio suprimido, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
  ```

- En este ejemplo, se instala SED Manager con el instalador maestro, en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED\""
  ```

- En este ejemplo, se instalan Encryption y BitLocker Manager (sin el complemento SED Manager), con el instalador maestro, en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
  ```

- En este ejemplo, se instalan BitLocker Manager (con el complemento SED Manager) y Encryption External Media, con el instalador maestro, en puertos estándar, de forma silenciosa, con un reinicio suprimido, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
  SUPPRESSREBOOT=1\""
  ```

- En este ejemplo, se instalan BitLocker Manager (con el complemento SED Manager) y Encryption External Media, con el instalador maestro, en puertos estándar, de forma silenciosa, con un reinicio suprimido, en la ubicación predeterminada de C:\Program Files\Dell\Dell Data Protection\ y se configura para utilizar el Dell Server especificado.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
  SUPPRESSREBOOT=1\""
  ```

5

# Desinstalación del instalador maestro

- Dell recomienda utilizar el Desinstalador de Data Security para eliminar la suite de Data Security.
- Cada componente se debe desinstalar por separado, seguido de la desinstalación del instalador maestro de . 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 de (y, por consiguiente, los clientes) tanto para la desinstalación como la instalación.
- Este capítulo le remite a otros capítulos que contienen 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. Desinstale Encryption.
  2. Desinstale SED Manager.
  3. Desinstalar Full Disk Encryption
  4. Desinstale BitLocker Manager.
- Continúe con la Desinstalación del instalador maestro.

## Desinstalar el instalador maestro de

Ahora que todos los clientes individuales se han desinstalado, podrá desinstalar el instalador maestro.

### Desinstalación con la línea de comandos

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

  ```
  "DDSSetup.exe" /s /x
  ```

  Reinicie el equipo cuando finalice.

# 6

# Instalación mediante los instaladores secundarios

- Para instalar o actualizar cada cliente individualmente, en primer lugar es necesario extraer los archivos ejecutables secundarios del instalador principal de , como se muestra en Extracción de instaladores secundarios del instalador principal.
- Para los ejemplos de comandos incluidos en esta sección, se asume que los comandos se ejecutan desde `C:\extracted`.
- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio en la línea de comandos, en comillas de escape.
- Utilice estos instaladores para instalar los clientes mediante instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.
- El reinicio se ha suprimido en los ejemplos de línea de comandos. No obstante, es posible que se requiera un reinicio.

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

- Archivos de registro: Windows crea archivos de registro de instalación de instaladores secundarios únicos 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 `C:\<any directory>\<any log file name>.log`.

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

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

| Modificador | Significado |
|---|---|
| /v | Envía las variables al archivo .msi en setup.exe. El contenido siempre debe ingresarse entre comillas de texto sin formato. |
| /s | Modo silencioso |
| /x | Modo de desinstalación |

**NOTA:**

Con /v, están disponibles las opciones predeterminadas de Microsoft. Para obtener una lista de las opciones, consulte este artículo.

| 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 |

| Opción | Significado |
|---|---|
| /qn | Sin interfaz de usuario |
| /norestart | Se elimina el reinicio |

- Indique a los usuarios que consulten el siguiente documento y los archivos de ayuda para obtener ayuda sobre la aplicación:
  - Consulte *Dell Encrypt Help* (Ayuda de cifrado de Dell) para saber cómo usar las funciones de Encryption. Acceda a la ayuda en `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
  - Consulte *Encryption External Media Help* (Ayuda de Encryption External Media) para saber cómo usar las funciones de Encryption External Media. Acceda a la ayuda en `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
  - Consulte la ayuda de *Encryption Enterprise* para obtener información sobre el uso de las funciones de PBA Authentication . Acceda a la ayuda en `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.

# Instalación de controladores

- Los controladores y el firmware para ControlVault, las lectoras de huellas digitales y las tarjetas inteligentes no se incluyen en los archivos ejecutables de instaladores secundarios ni en el instalador maestro de . Los controladores y el firmware deben actualizarse, y pueden descargarse desde http://www.dell.com/support seleccionando su modelo de equipo. Descargue los controladores y el firmware correspondientes en función de su hardware de autenticación.
  - ControlVault
  - Controlador de huellas digitales NEXT Biometrics
  - Controlador de lector de huellas digitales Validity 495
  - Controlador de tarjeta inteligente O2Micro

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

# Instalar Encryption

- Revise los Requisitos de Encryption si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, por ejemplo, EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de certificado.
- Los usuarios deben actualizar sus políticas haciendo clic con el botón secundario en el icono de Dell Encryption del área de notificación y seleccionando *Comprobar si existen actualizaciones de políticas* una vez finalizada la instalación.
- El instalador de Encryption se puede encontrar en:
  - **En dell.com/support**: si es necesario, obtenga el software en dell.com/support y, a continuación, extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption`.
  - **En su cuenta FTP de Dell:** localice el paquete de instalación en Encryption-Enterprise-10.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption`.
  - **NOTA:** En los registros de Dell Encryption no se especifica si la falla se produjo por falta de almacenamiento en disco.

## Instalación con la línea de comandos

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

| Parámetros |
|---|
| SERVERHOSTNAME=<ServerName> (FQDN del Dell Server para la reactivación) |

| Parámetros |
| --- |
| POLICYPROXYHOSTNAME=<RGKName> (FQDN de la política de proxy predeterminada) |
| MANAGEDDOMAIN=<MyDomain> (dominio que utilizará el dispositivo) |
| DEVICESERVERURL=<DeviceServerName/SecurityServerName> (URL utilizada para la activación; normalmente, incluye nombre del servidor, puerto y xapi) |
| GKPORT=<NewGKPort> (puerto del equipo selector) |
| MACHINEID=<MachineName> (nombre de equipo) |
| RECOVERYID=<RecoveryID> (Id. de recuperación) |
| REBOOT=ReallySuppress (Null permite los reinicios automáticos, ReallySuppress deshabilita el reinicio) |
| HIDEOVERLAYICONS=1 (0 habilita los íconos de superposición, 1 deshabilita los íconos de superposición) |
| HIDESYSTRAYICON=1 (0 habilita el icono en el área de notificación, 1 deshabilita el icono en el área de notificación) |
| ENABLE_FDE_LM=1 (permite la instalación de Dell Encryption en una computadora con Full Disk Encryption activo) |
| EME=1 (instalación en modo de Encryption External Media) |

Para obtener una lista de modificadores basic .msi y las opciones de visualización que se pueden utilizar en líneas de comandos, consulte instalación mediante instaladores secundarios.

- La siguiente tabla indica parámetros opcionales adicionales relacionados con la activación.

| Parámetros |
| --- |
| SLOTTEDACTIVATON=1 (0 deshabilita las activaciones retrasadas/programadas, 1 habilita las activaciones retrasadas/programadas) |
| SLOTINTERVAL=45,120 (programa activaciones mediante la notación x,x, donde el primer valor representa el límite inferior de la programación y el segundo valor representa el límite superior, en segundos) |
| CALREPEAT=600 (DEBE coincidir con el límite superior de SLOTINTERVAL o superarlo. Número de segundos que Encryption espera para generar un intento de activación basado en SLOTINTERVAL). |

**Ejemplo de línea de comandos**

**NOTA:** Reemplace `DEVICESERVERURL=https://server.organization.com:8081/xapi` (sin la barra diagonal final) si la versión de Security Management Server es anterior a la 7.7.

- En el siguiente ejemplo se instala Dell Encryption con los parámetros predeterminados (Encryption, Encrypt for Sharing, sin diálogo, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- En el ejemplo siguiente se instala Encryption y Encrypt for Sharing, se oculta el ícono del área de notificación de Dell Encryption, se ocultan los íconos superpuestos, sin diálogo, sin barra de progreso, se elimina el reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

**Ejemplo de línea de comandos para instalar Encryption External Media solamente**

- Instalación silenciosa, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Instalación silenciosa, sin reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
  ```

- **NOTA:**

  Aunque el cuadro “Acerca de” en el cliente muestra la información sobre el número de versión del software, no muestra si se instaló Encryption (instalación completa) o solo Encryption External Media. Para encontrar esta información, vaya a `C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log` y localice la siguiente entrada:

  [<date/timestamp> DeviceInfo: < >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

**Ejemplo de línea de comandos para convertir Encryption External Media a Encryption (instalación completa)**

**NOTA:** La conversión de Encryption External Media a Encryption (instalación completa) no es compatible con las actualizaciones.

- No se necesita el descifrado cuando se convierte Encryption External Media a Encryption (instalación completa).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
  REINSTALLMODE=vamus /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
  ```

- **Ejemplo de línea de comandos para instalar Dell Encryption con Full Disk Encryption**

  **\Encryption**

- En el siguiente ejemplo se instala Dell Encryption con los parámetros predeterminados (Encryption, Encrypt for Sharing, sin diálogo, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  *Luego*:

  **\Encryption Management Agent**

  En el siguiente ejemplo, se instala Full Disk Encryption administrado de forma remota y permite la instalación en una computadora protegida Dell Encryption (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Ejemplo de línea de comandos para instalar Encryption External Media y Full Disk Encryption.**

  **\Encryption**

  En el ejemplo siguiente se instala Encryption External Media con instalación silenciosa, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption.`

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  *Luego*:

  **\Encryption Management Agent**

  En el siguiente ejemplo, se instala remotamente Full Disk Encryption administrado y permite la instalación en una computadora protegida Dell Encryption (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Ejemplo de línea de comandos para instalar Encryption External Media mediante una instalación existente de Full Disk Encryption.**

  En el siguiente ejemplo se habilita la instalación de Encryption External Media mediante una instalación existente de Full Disk Encryption con instalación silenciosa, sin barra de progreso, reinicio automático e instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection.`

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
  norestart /qn"
  ```

- **Ejemplo de línea de comandos para instalar el cliente Remotely Managed Encryption mediante una instalación existente de Full Disk Encryption.**

  En el siguiente ejemplo se habilita la instalación del Dell Encryption mediante una instalación de Full Disk Encryption existente con parámetros predeterminados (cliente Encryption, Encrypt for Sharing, sin diálogo, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`) y los registros de instalación en `C:\Dell`. **Nota:** Para realizar una correcta generación de registros, el directorio `C:\Dell` debe existir antes de realizar la instalación.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
  norestart /qn /l*v C:\Dell\DellEncryptionInstall.log"
  ```

**NOTA:** Algunas versiones anteriores pueden requerir caracteres de escape de \" entre los valores de parámetros. Por ejemplo:

DDPE_XXbit_setup.exe /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn

# Instalar Full Disk Encryption

- Revise los Requisitos de Full Disk Encryption si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, como EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de confianza SSL/TLS.
- Los usuarios inician sesión en PBA mediante sus credenciales de Windows.

## Instalación con la línea de comandos

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

| Parámetros |
|---|
| CM_EDITION=1 (administración remota) |
| INSTALLDIR= (cambia el destino de instalación) |
| SERVERHOST= (securityserver.organization.com) |
| SERVERPORT=8888 |
| SECURITYSERVERHOST= (securityserver.organization.com) |
| SECURITYSERVERPORT=8443 |
| FUNCIÓN=FDE |
| ENABLE_FDE_LM=1 (permite la instalación de Full Disk Encryption en una computadora con Dell Encryption activo) |

Para obtener una lista de modificadores basic .msi y las opciones de visualización que se pueden utilizar en líneas de comandos, consulte instalación mediante instaladores secundarios.

**Ejemplo de línea de comandos**

**Encryption Management Agent**

- En el ejemplo siguiente se instala Full Disk Encryption administrado de forma remota (instalación silenciosa, sin reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management Agent**
- En el siguiente ejemplo, se instala Full Disk Encryption administrado de forma remota y permite la instalación en una computadora protegida Dell Encryption (instalación silenciosa, sin reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

- **Ejemplo de línea de comandos para instalar Full Disk Encryption y Encryption External Media.**

  **Cifrado**

En el ejemplo siguiente se instala Encryption External Media con instalación silenciosa, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

*Luego*:

**Encryption Management Agent**

En el siguiente ejemplo, se instala Full Disk Encryption administrado de forma remota y permite la instalación en una computadora protegida Dell Encryption (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

# Instalar Encryption en sistema operativo de servidor

Existen dos métodos disponibles para instalar Encryption en un sistema operativo de servidor. Seleccione uno de los siguientes métodos:

- Instalar Encryption en un sistema operativo de servidor de manera interactiva

  Encryption en sistema operativo de servidor puede instalarse de forma interactiva solo en computadoras que ejecutan sistemas operativos de servidor. La instalación en equipos que ejecutan sistemas operativos que no son del servidor debe realizarse mediante la línea de comandos, con el parámetro SERVERMODE=1 especificado.

- Instalar Encryption en un sistema operativo de servidor con línea de comandos

**Cuenta de usuario virtual**

- Como parte de la instalación, se crea una **cuenta de usuario de servidor virtual** para el uso exclusivo de Encryption en sistema operativo de servidor. La contraseña y la autenticación de DPAPI se deshabilitan para que solo el usuario de servidor virtual pueda acceder a las claves de cifrado.

**Antes de empezar**

- La cuenta de usuario que ejecuta la instalación debe ser un usuario de dominio con permisos de nivel de administrador.
- Para anular este requisito o para ejecutar Encryption en un sistema operativo de servidor en servidores sin dominio o con varios dominios, establezca la propiedad *ssos.domainadmin.verify* en *falso* en el archivo application.properties. El archivo se guarda en las siguientes rutas de acceso de archivos, según el Dell Server que se esté utilizando:

  Security Management Server *<installation dir>*/Security Server/conf/application.properties

  Security Management Server Virtual - /opt/dell/server/security-server/conf/application.properties

- El servidor debe admitir controles de puerto.

  Las políticas de sistema de control de puertos afectan a medios extraíbles en servidores protegidos, por ejemplo, mediante el control del acceso y el uso de los puertos USB del servidor por parte de dispositivos USB. La política de puertos USB se aplica a los puertos USB externos. La funcionalidad interna de puerto USB no se ve afectada por la política de puertos USB. Si se deshabilita la política de puertos USB, el teclado y el mouse USB no funcionarán y el usuario no podrá utilizar la computadora, a menos que se configure una conexión de escritorio remota antes de aplicar la política.

- Para activar correctamente, la computadora debe tener conectividad de red.
- Cuando Trusted Platform Module (TPM) está disponible, se utiliza para sellar la clave de finalidad general en el hardware de Dell. Si un TPM no está disponible, la API de protección de datos de Microsoft (DPAPI) se usa para proteger la clave de finalidad general.

  Cuando se instala un nuevo sistema operativo en un equipo Dell con TPM que ejecuta Server Encryption, deje en blanco el TPM en el BIOS. Consulte este artículo para obtener instrucciones.

- El archivo de registro de instalación se encuentra en el directorio %temp% del usuario, ubicado en `C:\Users\<nombre de usuario>\AppData\Local\Temp`. Para ubicar el archivo de registro correcto, busque el nombre de archivo que empiece

con MSI y termine con una extensión .log. El archivo incluye una fecha y hora que coinciden con el momento en que se ejecutó el instalador.

- Encryption no es compatible en servidores que forman parte de sistemas de archivos distribuidos (DFS).

**Extraiga el instalador secundario**

- Para instalar Encryption en un sistema operativo de servidor, primero debe extraer el instalador secundario, **DDPE_xxbit_setup.exe**, del instalador maestro. Consulte Extracción de instaladores secundarios del instalador maestro.

# Instalar de forma interactiva

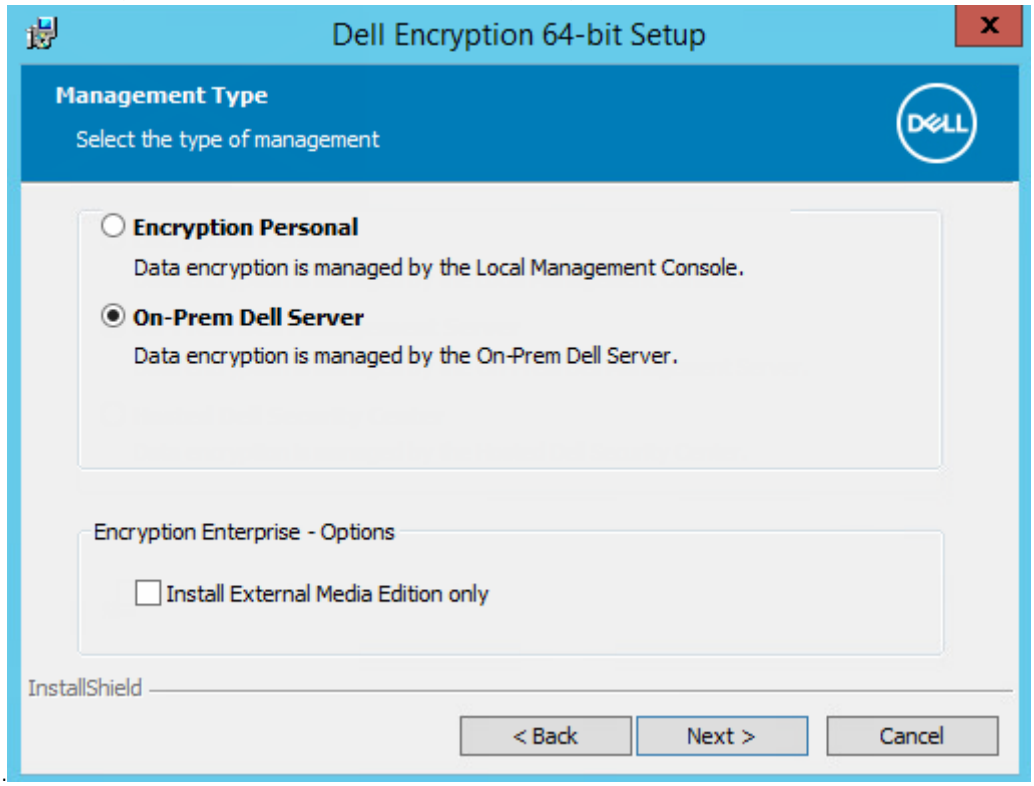
- Utilice estas instrucciones para instalar Encryption en sistema operativo de servidor de forma interactiva. Este instalador incluye los componentes que necesita para el cifrado de software.

1. Ubique **DDPE_XXbit_setup.exe** en la carpeta `C:\extracted\Encryption`. Cópielo al equipo local.
2. Si está instalando Encryption en sistema operativo de servidor, haga doble clic en **DDPE_XXbit_setup.exe** para iniciar el instalador.

   **NOTA:**

   Cuando Encryption en sistema operativo de servidor está instalado en una computadora que ejecuta un sistema operativo de servidor, como Windows Server 2012 R2, el instalador se instala automáticamente en SERVERMODE.

3. En la página de Bienvenida, haga clic en **Siguiente**.
4. Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.
5. Seleccione *Dell Management Server local* y, a continuación, haga clic en **Siguiente**.




6. Haga clic en **Siguiente** para instalar en la ubicación predeterminada.
7. Haga clic en **Siguiente** para omitir el cuadro de diálogo *Tipo de administración*.
8. En *Nombre de Security Management Server*, introduzca/valide el nombre completo del host del Dell Server para administrar el usuario de destino (por ejemplo, *server.organization.com)*.

   Escriba el nombre de dominio en *Dominio administrado* (por ejemplo, organización). Haga clic en **Siguiente**.
9. En el nombre de host y el puerto de Proxy de política, introduzca/valide la información y haga clic en **Siguiente**.
10. En la URL del servidor del dispositivo, introduzca/valide la información y haga clic en **Siguiente**.
11. Haga clic en **Instalar** para comenzar la instalación.

La instalación puede tardar varios minutos.

12. Cuando se complete la configuración, haga clic en **Finalizar**.

    La instalación ha finalizado.

13. Reinicie el equipo. Dell recomienda suspender el reinicio solo si se necesita tiempo para guardar su trabajo y cerrar las aplicaciones. El cifrado no puede comenzar hasta que no se reinicie el equipo.

# Instalar mediante la línea de comandos

**Busque el instalador en `C:\extracted\Encryption`**

- Utilice **DDPE_xxbit_setup.exe** para instalar o actualizar mediante una instalación con secuencia de comandos, utilizando archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.

**Modificadores**

La siguiente tabla indica los modificadores disponibles para la instalación.

| Modificador | Significado |
|---|---|
| /v | Envía las variables al archivo .msi dentro de DDPE_XXbit_setup.exe |
| /a | Instalación administrativa |
| /s | Modo silencioso |

**Parámetros**

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

| Componente | Archivo de registro | Parámetros de línea de comandos |
|---|---|---|
| Todo | /l*v [fullpath] [nombre_archivo].log * | SERVERHOSTNAME=<Security Management Server Name> |
| | | SERVERMODE=1 |
| | | POLICYPROXYHOSTNAME=<RGK Name> |
| | | MANAGEDDOMAIN=<My Domain> |
| | | DEVICESERVERURL=<Activation Server Name> |
| | | GKPORT=<New GK Port> |
| | | MACHINEID=<Machine Name> |
| | | RECOVERYID=<Recovery ID> |
| | | REBOOT=ReallySuppress |
| | | HIDEOVERLAYICONS=1 |
| | | HIDESYSTRAYICON=1 |
| | | EME=1 |

**NOTA:**

Aunque se puede suprimir el reinicio, se requerirá eventualmente. El cifrado no puede comenzar hasta que no se reinicie el equipo.

**Opciones**

La siguiente tabla indica las opciones de presentación que pueden especificarse al final del argumento que se envía al conmutador /v.

| 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 |
| **NOTA:** No utilice **/q** ni **/qn** en la misma línea de comandos. Utilice solamente **!** y después **/qb**. | |

- El parámetro de la línea de comandos, SERVERMODE=1, se ejecuta solo durante nuevas instalaciones. El parámetro se ignora para desinstalaciones.
- Incorpore un valor que contenga uno o más caracteres especiales, como un espacio, en comillas de escape.
- El parámetro DEVICESERVERURL distingue mayúsculas de minúsculas.

**Ejemplo de instalación con la línea de comandos**

- En el siguiente ejemplo se instala Encryption en el modo de sistema operativo de servidor con los parámetros predeterminados (Encryption, instalación silenciosa, Encrypt for Sharing, sin diálogo, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn
  REBOOT="ReallySuppress" SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- En el siguiente ejemplo se instala Encryption en modo de sistema operativo de servidor con un archivo de registro y parámetros predeterminados (Encryption, instalación silenciosa, Encrypt for Sharing, sin diálogo, sin barra de progreso, sin reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`) y se especifica un nombre de archivo de registro personalizado que termina con un número (DDP_ssos-090.log), el cual aumenta si la línea de comandos se ejecuta más de una vez en el mismo servidor. Incluya la ruta de acceso completa en el comando para especificar la ubicación de un registro distinta de la ubicación predeterminada donde se encuentra el archivo ejecutable. Por ejemplo, /l*v C:\Logs\DDP_ssos-090.log crea registros de instalación en C:\Logs.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /
  norestart/qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
  xapi/" /l*v DDP_ssos-090.log /norestart/qn"
  ```

Reinicie la computadora después de la instalación. Dell recomienda suspender el reinicio solo si se necesita tiempo para guardar su trabajo y cerrar las aplicaciones. El cifrado no puede comenzar hasta que no se reinicie el equipo.

# Activar

- Asegúrese de que el nombre de la computadora del servidor sea el nombre del terminal que se muestra en la consola de administración.
- Un usuario interactivo con credenciales de administrador de dominios debe iniciar sesión en el servidor al menos una vez para la activación inicial. El usuario conectado puede ser de cualquier tipo: de dominio o no de dominio, escritorio remoto conectado o usuario interactivo en el servidor, pero la activación requiere credenciales de administrador de dominios.
- Tras el reinicio después de la instalación, se muestra el cuadro de diálogo Activación. El administrador debe introducir credenciales de administrador de dominios con un nombre de usuario con el formato de Nombre principal de usuario (UPN). Encryption de sistemas operativos de servidor no se activa automáticamente.
- Durante la activación inicial, se crea una cuenta de usuario de servidor virtual. Después de la activación inicial, se reinicia el equipo para que pueda comenzar la activación del dispositivo.
- Durante la fase de activación de dispositivo y de autenticación, se asigna a la computadora una Id. de máquina exclusiva, se crean y se unen las claves de cifrado y se establece una relación entre el paquete de claves de cifrado y el usuario del servidor virtual. El paquete de claves de cifrado asocia estas y las políticas con el usuario del servidor virtual nuevo para crear una relación irrompible entre los datos cifrados, el equipo determinado y el usuario del servidor virtual. Después de la activación del dispositivo, el usuario del servidor virtual aparece en la consola de administración como SERVIDOR-USUARIO@<*fully qualified server name*>. Para obtener más información sobre la activación, consulte Activación en un sistema operativo de servidor.

**NOTA:**

Si cambia el nombre del servidor después de la activación, el nombre para mostrar no cambiará en la consola de administración. Sin embargo, si Encryption de sistemas operativos de servidor se activa de nuevo después de que se cambia el nombre del servidor, el nuevo nombre del servidor aparecerá en la consola de administración.

Se muestra un cuadro de diálogo de activación después de cada reinicio para solicitar al usuario que active Encryption en un sistema operativo de servidor. Para completar la activación, siga estos pasos:

1. Inicie sesión en el servidor ya sea en el servidor o a través Remote Desktop Connection.
2. Introduzca el nombre de usuario de un administrador de dominio en formato UPN y la contraseña, y haga clic en **Activar**. Este es el mismo cuadro de diálogo Activación que aparece cada vez que se reinicia un sistema no activado.

   El Dell Server emite una clave de cifrado para la Id. de máquina, crea la **cuenta de usuario de servidor virtual**, crea una clave de cifrado para la cuenta de usuario, empaqueta las claves de cifrado, y crea la relación entre el paquete de cifrado y la cuenta de usuario de servidor virtual.

3. Haga clic en **Cerrar**.

   Después de la activación, comienza el cifrado.

4. Después de que haya terminado el barrido de cifrado, reinicie el equipo para procesar todos los archivos que estaban anteriormente en uso. Este es un paso importante por motivos de seguridad.

   **NOTA:**

   Si la política *Proteger credenciales de Windows* está habilitada, Encryption de sistemas operativos de servidor cifra los archivos de `\Windows\system32\config`, que incluyen las credenciales de Windows. Los archivos en `\Windows\system32\config` se cifran, incluso si la política *Cifrado de SDE habilitado* está deshabilitada. De manera predeterminada, la política *Proteger credenciales de Windows* está seleccionada.

   **NOTA:**

   Después de reiniciar la computadora, la autenticación para la clave de cifrado común *siempre* requiere la clave de máquina del servidor protegido. Dell Server arroja una clave de desbloqueo para acceder a las claves y las políticas de cifrado en el almacén (las claves y las políticas son para el servidor, no para el usuario). Sin la clave de máquina del servidor, la clave de cifrado común no puede desbloquearse y la computadora no puede recibir actualizaciones de política.

### Confirmar la activación

Desde la consola local, abra el cuadro de diálogo **Acerca de** para confirmar que Encryption de sistemas operativos de servidor esté instalado, autenticado y en el modo de servidor. Si el ID de cliente Encryption está en **rojo**, el cifrado aún no se ha activado.

## Usuario de servidor virtual

- En la consola de administración, se puede encontrar un servidor protegido bajo su nombre de máquina. Además, cada servidor protegido tiene su propia cuenta de usuario de servidor virtual. Cada cuenta tiene un nombre de usuario estático exclusivo y un nombre de máquina exclusivo.
- La cuenta de usuario de servidor virtual solo la utiliza Encryption en sistemas operativos de servidor y no afecta el funcionamiento del servidor protegido. El usuario del servidor virtual se asocia al paquete de claves de cifrado y el proxy de políticas.
- Después de la activación, la cuenta de usuario del servidor virtual es la cuenta de usuario activada y asociada con el servidor.
- Después de que se haya activado la cuenta de usuario del servidor virtual, se ignoran todas las notificaciones de inicio/cierre de sesión. En su lugar, durante el arranque, la computadora se autentica automáticamente con el usuario del servidor virtual y, luego, descarga la clave de la máquina del Dell Server.

# Instalar SED Manager y PBA Advanced Authentication

- Revise los Requisitos de SED si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, por ejemplo, EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de confianza SSL/TLS.
- Los usuarios inician sesión en PBA mediante sus credenciales de Windows.
- Los instaladores de SED Manager y PBA Advanced Authentication se pueden encontrar en las siguientes ubicaciones:
  - **En dell.com/support**: si es necesario, obtenga el software en dell.com/support y, a continuación, extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption Management Agent`.
  - **En su cuenta FTP de Dell:** localice el paquete de instalación en Encryption-Enterprise-10.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption Management Agent`.

## Instalación con la línea de comandos

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

| Parámetros |
|---|
| CM_EDITION=1 <remote management> |
| INSTALLDIR=<change the installation destination> |
| SERVERHOST=<securityserver.organization.com> |
| SERVERPORT=8888 |
| SECURITYSERVERHOST=<securityserver.organization.com> |
| SECURITYSERVERPORT=8443 |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

Para obtener una lista de modificadores basic .msi y las opciones de visualización que se pueden utilizar en líneas de comandos, consulte instalación mediante instaladores secundarios.

Mediante los siguientes comandos de ejemplo, se puede instalar o actualizar Encryption Management Agent.

**Ejemplo de línea de comandos**

**\Encryption Management Agent**

- En el siguiente ejemplo, se instala remotamente el SED Manager administrado, Encryption Management Agent y la consola de seguridad local (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

# Instalación de BitLocker Manager

- **NOTA:** Si su organización requiere el uso de proveedores de credenciales de terceros, debe instalar o actualizar Encryption Management Agent con el parámetro FEATURE=BLM o FEATURE=BASIC.

- Revise los Requisitos del cliente BitLocker Manager si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, como por ejemplo, EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de confianza SSL/TLS.
- Los instaladores del cliente BitLocker Manager se pueden encontrar en:
  - **En dell.com\support**: si es necesario, obtenga el software en dell.com/support y, a continuación, extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption Management Agent`.
  - **En su cuenta FTP de Dell:** localice el paquete de instalación en Encryption-Enterprise-10.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro. Después de la extracción, localice el archivo en `C:\extracted\Encryption Management Agent`.

## Instalación con la línea de comandos

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

| Parámetros |
|---|
| CM_EDITION=1 <remote management> |
| INSTALLDIR=<change the installation destination> |
| SERVERHOST=<securityserver.organization.com> |
| SERVERPORT=8888 |
| SECURITYSERVERHOST=<securityserver.organization.com> |
| SECURITYSERVERPORT=8443 |
| FEATURE=BLM <install BitLocker Manager only> |
| FEATURE=BLM,SED <install BitLocker Manager with SED> |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

Para obtener una lista de modificadores basic .msi y las opciones de visualización que se pueden utilizar en líneas de comandos, consulte instalación mediante instaladores secundarios.

**Ejemplo de línea de comandos**

- En el ejemplo siguiente se instala solo BitLocker Manager (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM /norestart /qn"
```

- En el ejemplo siguiente se instala BitLocker Manager con SED (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM,SED /norestart /qn"
```

- **Ejemplo de línea de comandos para instalar BitLocker Manager y Dell Encryption**

  En el ejemplo siguiente se instala solo BitLocker Manager (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`)

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  *Luego:*

  En el siguiente ejemplo se instala el cliente con los parámetros predeterminados (cliente Encryption, Encrypt for Sharing, sin diálogo, sin barra de progreso, reinicio automático, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

# 7

# Desinstalación mediante los instaladores secundarios

- Dell recomienda utilizar el Desinstalador de Data Security para eliminar la suite de Data Security.
- Para desinstalar cada cliente por separado, en primer lugar, es necesario extraer los archivos ejecutables secundarios del instalador maestro de , como se muestra en Extracción de los instaladores secundarios del instalador maestro De forma alternativa, ejecute una instalación administrativa para extraer el .msi.
- Asegúrese de que se utiliza la misma versión de cliente tanto para la desinstalación como para la instalación.
- 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 desinstalación secundarios únicos en el directorio %temp% del usuario, 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 de /qb.

| Modificador | Significado |
|---|---|
| /v | Envía las variables al archivo .msi en setup.exe. El contenido siempre debe ingresarse entre comillas de texto sin formato. |
| /s | Modo silencioso |
| /x | Modo de desinstalación |
| /a | Instalación administrativa (se copian todos los archivos en el .msi) |

**NOTA:**

Con /v, están disponibles las opciones predeterminadas de Microsoft. Para obtener una lista de las opciones, consulte https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

| 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 |

| Opción | Significado |
|---|---|
| /qb!- | Diálogo de progreso sin botón **Cancelar** , se reinicia automáticamente al terminar el proceso |
| /qn | Sin interfaz de usuario |

# Desinstalación de Encryption y Encryption en sistema operativo de servidor

- Para reducir la duración del descifrado, ejecute el asistente de liberación de espacio en disco a fin de eliminar los archivos temporales y otros archivos innecesarios.
- 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 de descifrado debidos a archivos bloqueados.
- Una vez finalizada la desinstalación y estando en curso el descifrado, deshabilite toda la conectividad de red. De lo contrario, se podrán obtener nuevas políticas que vuelvan a habilitar el cifrado.
- Siga el actual proceso para el descifrado de datos, como la emisión de la actualización de una política.
- Encryption y Encryption External Media actualizan Dell Server para cambiar el estado a *Desprotegido* al principio de un proceso de desinstalación de cliente. Sin embargo, en caso de que el cliente no se pueda comunicar con el Dell Server, el estado no se podrá actualizar, independientemente del motivo. En este caso, deberá *Quitar el terminal* manualmente en la consola de administración. Si su empresa utiliza este flujo de trabajo por razones de cumplimiento normativo, Dell recomienda comprobar que se haya configurado el estado *Desprotegido* de la manera esperada, ya sea en la consola de administración o en los informes administrados.

## Proceso

- **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.
- Key Server (y Security Management Server) debe estar configurado antes de la desinstalación si utiliza la opción **Descargar claves del Encryption Removal Agent del servidor**. Consulte Configurar Key Server para la desinstalación de cliente Encryption activado en Security Management Server para obtener instrucciones. No se necesitan acciones si el cliente que vaya a realizar la desinstalación se activa en un Security Management Server Virtual, ya que Security Management Server Virtual no utiliza Key Server.
- Debe usar la utilidad administrativa de Dell (CMGAd) antes de iniciar el Encryption Removal Agent si utiliza la opción **Importar claves de Encryption Removal Agent de un archivo**. Esta utilidad se utiliza para obtener la agrupación de claves de cifrado. Consulte Usar la Utilidad de descarga administrativa (CMGAd) para obtener instrucciones. La utilidad se puede encontrar en el medio de instalación de Dell.
- 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.

## Desinstalación con la línea de comandos

- Una vez que se extrae del instalador maestro de , el instalador de Encryption se puede encontrar 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:<br>3 - Usar el paquete LSARecovery<br>2 - Usar el material de claves forenses descargado con anterioridad<br>1 - Descargar claves del Dell Server<br>0 - No instalar Encryption Removal Agent |
| CMGSILENTMODE | Propiedad para desinstalación silenciosa:<br>1 - Silenciosa: se requiere cuando se ejecuta con variables msiexec que contienen /q o /qn<br>0 - No silenciosa: solo es posible cuando no hay variables msiexec que tengan /q en la sintaxis de la línea de comandos |
| **Propiedades requeridas** | |
| DA_KM_PATH | La ruta completa al paquete de claves. |
| DA_KM_PW | La contraseña configurada en el paquete de claves. |
| DA_SERVER | FQHN para el Security Management Server que aloja la sesión de negociación. |
| DA_PORT | Puerto en el Security Management Server para solicitud (el valor predeterminado es 8050). |
| SVCPN | Nombre de usuario en formato UPN en el que inicia sesión el servicio Key Server en el Security Management Server. |
| DA_RUNAS | Nombre de usuario en formato compatible con SAM en cuyo contexto se realiza la solicitud de búsqueda de clave. Este usuario debe estar en la lista de Key Server en Security Management Server. |
| DA_RUNASPWD | Contraseña para el usuario de runas. |
| FORENSIC_ADMIN | Cuenta de administrador forense del Dell Server, que se puede utilizar para solicitudes de administración forense relacionadas con desinstalaciones o claves. |
| FORENSIC_ADMIN_PWD | La contraseña para la cuenta del administrador forense. |
| **Propiedades opcionales** | |
| SVCLOGONUN | Nombre de usuario en formato UPN para inicio de sesión del servicio Encryption Removal Agent como parámetro. |
| SVCLOGONPWD | Contraseña para el inicio de sesión como usuario. |

- En el siguiente ejemplo se desinstala Encryption de forma silenciosa y se descargan las claves de cifrado desde Security Management Server.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  DA_SERVER=server.organization.com DA_PORT=8050 SVCPN=administrator@organization.com
  DA_RUNAS=domain\username DA_RUNASPWD=password /qn"
  ```

  Comando MSI:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

Reinicie el equipo cuando finalice.

- En el siguiente ejemplo se desinstala Encryption de forma silenciosa y se descargan las claves de cifrados mediante una cuenta de administrador forense.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn
  CMG_DECRYPT=1 CMGSILENTMODE=1 FORENSIC_ADMIN=forensicadmin@organization.com
  FORENSIC_ADMIN_PWD=tempchangeit REBOOT=REALLYSUPPRESS
  ```

  Reinicie el equipo cuando finalice.

- En el siguiente ejemplo, se desinstala Encryption de forma silenciosa mediante claves predescargadas que se encuentran en C:\Users\administrator\Desktop\Admin\ usando la contraseña del administrador forense y se escriben registros en C:\SheildUninstall.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1 DA_KM_PATH=C:
  \Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v c:
  \ShieldUninstall.log /qn /norestart"
  ```

  Comando de MSI

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1
  DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
  c:\ShieldUninstall.log /qn /norestart
  ```

**NOTA:**

Dell recomienda las siguientes acciones cuando se utiliza una contraseña de administrador forense en la línea de comandos:

1. Cree una cuenta de administrador forense en la consola de administración para realizar la desinstalación silenciosa.
2. Use una contraseña temporal para esa cuenta que sea exclusiva para esa cuenta y ese período.
3. Una vez finalizada la desinstalación silenciosa, elimine la cuenta temporal de la lista de administradores o cambie la contraseña.

Es posible que algunos clientes más antiguos requieran que los valores de los parámetros estén entre caracteres de escape \". Por ejemplo:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\"
CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\"
SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\"
DA_RUNASPWD=\"password\" /qn"
```

## Desinstalar Encryption External Media

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

**Desinstalación con la línea de comandos**

Ejecute una línea de comandos similar a la siguiente:

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

Reinicie el equipo cuando finalice.

# Desinstalar Full Disk Encryption

- Para la desactivación de PBA se requiere la conexión de red con el Dell Server.

## Proceso

- Desactive la PBA, lo cual quita todos los datos de PBA de la computadora y desbloquea las claves de Full Disk Encryption.
- Instale Full Disk Encryption.

## Desactivación de la PBA

1. Como administrador de Dell, inicie sesión en la Consola de administración.
2. En el panel izquierdo, haga clic en **Poblaciones** > **Terminales**.
3. Seleccione el tipo de extremo correspondiente.
4. Seleccione *Mostrar* > *Visibles, Ocultos* o *Todos*.
5. Si conoce el nombre de host del equipo, introdúzcalo en el campo Nombre de host (se admiten caracteres comodín). Puede dejar el campo en blanco para que aparezcan todos los equipos. Haga clic en **Buscar**.

   Si desconoce el nombre de host, desplácese por la lista para ubicar al equipo.

   Se muestra un equipo o una lista de equipos, según el filtro de búsqueda.
6. Seleccione el hostname de la computadora que desea.
7. Haga clic en **Políticas de seguridad** en el menú superior.
8. Seleccione **Full Disk Encryption** en el grupo **Cifrado de Windows**.
9. Cambie la política y **Full Disk Encryption** de `On` a ***`Off`***.
10. Haga clic en **Guardar**.
11. En el panel izquierdo, haga clic en **Confirmar políticas**.
12. Haga clic en **Confirmar políticas**.

    Espere a que se propague la política del Dell Server a la computadora de destino para la desactivación.

    Desinstale Full Disk Encryption y PBA Advanced Authentication después de que se desactive PBA.

## Instalar cliente de Full Disk Encryption

**Desinstalación con la línea de comandos**

- Una vez que se extrae del instalador maestro, Full Disk Encryption se puede encontrar en `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - En el siguiente ejemplo, se desinstala Full Disk Encryption de forma silenciosa.

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

    Apague y reinicie el equipo cuando haya terminado.

# Desinstalación de SED Manager

- Para la desactivación de PBA se requiere la conexión de red con el Dell Server.

## Proceso

- Desactivar la PBA, que quita todos los datos de PBA del equipo y desbloquea las claves de SED.
- Desinstale SED Manager.

## Desactivación de la PBA

1. Como administrador de Dell, inicie sesión en la Consola de administración.
2. En el panel izquierdo, haga clic en **Poblaciones** > **Terminales**.
3. Seleccione el tipo de extremo correspondiente.
4. Seleccione *Mostrar* > *Visibles, Ocultos* o *Todos*.

5. Si conoce el nombre de host del equipo, introdúzcalo en el campo Nombre de host (se admiten caracteres comodín). Puede dejar el campo en blanco para que aparezcan todos los equipos. Haga clic en **Buscar**.

   Si desconoce el nombre de host, desplácese por la lista para ubicar al equipo.

   Se muestra un equipo o una lista de equipos, según el filtro de búsqueda.
6. Seleccione el hostname de la computadora que desea.
7. Haga clic en **Políticas de seguridad** en el menú superior.
8. Seleccione **Unidades de cifrado automático** en la página **Categoría de política**.
9. Cambie la **Unidad de cifrado automático (SED)** y la política de *On* a ***Off***.
10. Haga clic en **Guardar**.
11. En el panel izquierdo, haga clic en **Confirmar políticas**.
12. Haga clic en **Confirmar políticas**.

    Espere a que se propague la política del Dell Server a la computadora de destino para la desactivación.

    Desinstale SED Manager y PBA Advanced Authentication después de que se desactive PBA.

## Desinstalación del cliente SED

**Desinstalación con la línea de comandos**

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

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

    Apague y reinicie el equipo cuando haya terminado.

# Desinstalación de BitLocker Manager

## Desinstalación con la línea de comandos

- Una vez se extrae el instalador maestro de , el instalador de BitLocker Manager se puede encontrar en `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- En el siguiente ejemplo se desinstala BitLocker Manager de manera silenciosa.

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

  Reinicie el equipo cuando finalice.

# 8

# Desinstalador de Data Security

## Desinstalar

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: descargar claves desde servidor**.

Ingrese las credenciales totalmente calificadas de un administrador forense y seleccione **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.

# 9

# Situaciones frecuentes

- Para instalar cada cliente individualmente, en primer lugar, se deben extraer los archivos ejecutables secundarios del instalador maestro de , como se muestra en Extracción de instaladores secundarios del instalador maestro.
- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio en la línea de comandos, en comillas de escape.
- Utilice estos instaladores para instalar los clientes mediante instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.
- El reinicio se ha suprimido en los ejemplos de línea de comandos. No obstante, es posible que se requiera un reinicio. El cifrado no puede comenzar hasta que no se reinicie el equipo.
- Archivos de registro: Windows crea archivos de registro de instalación de instaladores secundarios únicos 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 `C:\<any directory>\<any log file name>.log`.

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

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

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

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

- Indique a los usuarios que consulten el siguiente documento y los archivos de ayuda para obtener ayuda sobre la aplicación:
  - Consulte *Dell Encrypt Help* (Ayuda de cifrado de Dell) para saber cómo usar las funciones de Encryption. Acceda a la ayuda de `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help`.
  - Consulte *Encryption External Media Help* (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\EMS`.

- Consulte la ayuda de *Encryption Enterprise* para obtener información sobre el uso de estas funciones de . Puede acceder a esta ayuda en `<Install dir>:\Program Files\Dell\Dell Data Protection\Authentication \Help`.

# Encryption Client

- En el siguiente ejemplo se instala SED Management y Encryption Management Agent (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Luego:

- En el siguiente ejemplo se instala Encryption con los parámetros predeterminados (Encryption y Encrypt for Sharing, sin diálogo, sin barra de progreso, sin reinicio, instalado en la ubicación predeterminada de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Reemplace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sin la barra diagonal final) si la versión de Security Management Server es anterior a la 7.7.

# SED Manager (incluye Advanced Authentication) y cliente Encryption

- El siguiente ejemplo instala controladores para Trusted Software Stack (TSS) para el TPM y revisiones de Microsoft en la ubicación especificada; no crea una entrada en la lista de programas del Panel de control, y suprime el reinicio.

  Estos controladores se deben instalar al instalar el cliente Encryption.

  ```
  setup.exe /S /z"\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
  ```

  Luego:

- En el siguiente ejemplo, se instala remotamente el SED Manager administrado (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Luego:

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

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

  Luego:

- En el siguiente ejemplo se instala el cliente con los parámetros predeterminados (cliente Encryption y Encrypt for Sharing, sin diálogo, sin barra de progreso, sin reinicio, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Reemplace `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sin la barra diagonal final) si la versión de Security Management Server es anterior a la 7.7.

# SED Manager y Encryption External Media

- En el siguiente ejemplo, se instala SED Manager, Encryption Management Agent y la consola de seguridad local (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Luego:

- En el ejemplo siguiente se instala solo Encryption External Media (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  Reemplace `DEVICESERVERURL=https://server.organization.com`**:8081/xapi** (sin la barra diagonal final) si la versión de Security Management Server es anterior a la 7.7.

# BitLocker Manager y Encryption External Media

- BitLocker Manager y Encryption External Media interactúan según la secuencia de cifrado. Si se inserta una unidad de cifrado BitLocker Manager a una computadora con Encryption External Media, la contraseña BitLocker Manager se **debe** ingresar antes de que Encryption External Media pueda leer y cifrar la unidad.
- Si se activa Encryption External Media en una unidad, el cifrado BitLocker Manager se puede aplicar a la misma unidad.
- En el ejemplo siguiente se instala BitLocker Manager (instalación silenciosa, sin reinicio, sin entrada en la lista de programas del Panel de control, instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Luego:

- En el ejemplo siguiente se instala solo Encryption External Media (instalación silenciosa, sin reinicio e instalado en la ubicación predeterminada `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

Reemplace `DEVICESERVERURL=https://server.organization.com`**:8081/xapi** (sin la barra diagonal final) si la versión de Security Management Server es anterior a la 7.7.

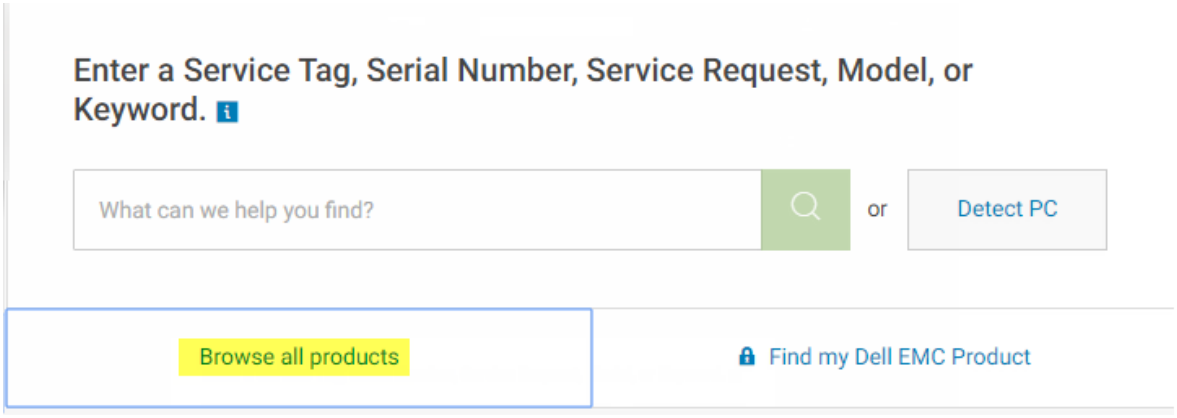
# 10

# 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**.

11

# Configuración previa a la preinstalación para SED UEFI y BitLocker Manager

## Inicialización del TPM

- Debe ser miembro del grupo de administradores locales o de otro equivalente.
- El equipo debe tener un TPM y un BIOS compatibles.
- Siga las instrucciones que se encuentran en http://technet.microsoft.com/en-us/library/cc753140.aspx.

## Configuración previa a la instalación para equipos UEFI

### Habilitación de conectividad de red durante la autenticación previa al arranque de UEFI

Para que la autenticación previa al arranque sea correcta en una computadora con firmware UEFI, PBA tiene que tener conectividad de red. De manera predeterminada, los equipos con firmware UEFI no tienen conectividad de red hasta que se haya cargado el sistema operativo, lo que se produce después del modo PBA.

El siguiente procedimiento habilita la conectividad de red durante PBA para equipos con UEFI habilitado. Como los pasos de configuración varían de un modelo de equipo UEFI a otro, el siguiente procedimiento solo es un ejemplo.

1. Reinicie en la configuración de firmware de UEFI.
2. Pulse F2 continuamente durante el inicio hasta que vea un mensaje en la pantalla superior derecha similar a "preparando el menú de inicio de un solo uso".
3. Si se le solicita, introduzca la contraseña del administrador de BIOS.

   **NOTA:**

   Normalmente, no verá esta indicación si se trata de un equipo nuevo, dado que la contraseña del BIOS aún no ha sido configurada.
4. Seleccione **Configuración del sistema**.
5. Seleccione **NIC integrada**.
6. Seleccione la casilla de verificación **Habilitar la pila de red UEFI**.
7. Seleccione **Habilitado** o **Habilitado con PXE**.
8. Seleccione **Aplicar**

   **NOTA:**

   Los equipos *sin* firmware UEFI no requieren configuración.

### Deshabilitar las ROM de opción heredadas

Asegúrese de que la configuración **Habilitar las ROM de opción heredadas** está deshabilitada en el BIOS.

1. Reinicie el equipo.
2. Mientras se reinicia, pulse **F12** varias veces para que aparezca la configuración de inicio del equipo UEFI.
3. Pulse la flecha Abajo, resalte la opción **Configuración del BIOS** y pulse **Intro**.
4. Seleccione **Configuración** > **General** > **Opciones de arranque avanzadas**.

5. Borre la casilla de verificación **Habilitar las ROM de opción heredadas** y haga clic en **Aplicar**.

# Configuración previa a la instalación para establecer una partición de PBA de BitLocker

- Debe crear la partición de PBA **antes** de instalar BitLocker Manager.
- Encienda y active el TPM **antes** de instalar BitLocker Manager. BitLocker Manager tomará propiedad del TPM (no se requiere un reinicio). Sin embargo, si la propiedad del TMP ya existe, BitLocker Manager comenzará el proceso de configuración de cifrado. La cuestión es que el TPM debe ser con propietario y estar habilitado.
- Es posible que deba particionar el disco de forma manual. Consulte la descripción de Microsoft de la Herramienta de Preparación de BitLocker Drive para obtener más información.
- Use el comando BdeHdCfg.exe para crear la partición de PBA. Con el parámetro predeterminado se indica que la herramienta de la línea de comandos seguirá el mismo proceso que el asistente de instalación de BitLocker.

  ```
  BdeHdCfg -target default
  ```

  **NOTA:**

  Para obtener más opciones disponibles para el comando BdeHdCfg, consulte Referencia de parámetros de BdeHdCfg.exe de Microsoft.

# 12

# Designación del Dell Server a través del registro

- Si sus clientes tienen derechos mediante Dell Digital Delivery, siga estas instrucciones para establecer un registro mediante los objetos de política de grupo con el fin de preestablecer el servidor Dell que se utilizará después de la instalación.
- La estación de trabajo debe ser un miembro de la OU en la que se aplican los objetos de política de grupo, o bien se debe establecer manualmente la configuración del registro en el terminal.
- Asegúrese de que el puerto de salida 443 esté disponible para establecer comunicación desde el Dell Server hacia cloud.dell.com. Si el puerto 443 está bloqueado (por cualquier motivo), no se realiza la adquisición del derecho y se utiliza un derecho desde el pool disponible.

  **NOTA:** Si no establece este valor del registro cuando intenta realizar la instalación a través de Dell Digital Delivery o no especifica un SERVIDOR en el instalador maestro, la dirección URL de activación se establece de forma predeterminada en 199.199.199.199.

### Establecer manualmente la clave de registro

Para los terminales que no están unidos a un dominio o en los que no se puede configurar un objeto de política de grupo, establezca previamente una clave de registro para activarse en un Dell Server específico durante la instalación.

1. En el cuadro de búsqueda de la barra de tareas, escriba **regedit** y, luego, haga clic con el botón secundario y seleccione **Ejecutar como administrador**.
2. Continúe y cree la siguiente clave de registro:

   HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection

   REG_SZ: Server

   Valor: <Dirección IP o FQDN del Dell Server>

3. Instale Encryption mediante Dell Digital Delivery o el instalador maestro.

### Crear el objeto de política de grupo

1. En la controladora de dominio para administrar los clientes, haga clic en **Inicio** > **Herramientas administrativas** > **Administración de políticas de grupo**.
2. Haga clic con el botón secundario en el OU en el que se debe aplicar la política y seleccione **Crear un GPO en este dominio**, y **Vincularlo aquí**.
3. Ingrese el nombre del nuevo GPO, seleccione (ninguno) para GPO de inicio de origen y haga clic en **Aceptar**.
4. Haga clic con el botón derecho del ratón en GPO que fue creado y seleccione **Editar**.
5. Se carga el Editor de administración de políticas de grupo. Acceda a **Configuración de la computadora** > **Preferencias** > **Configuración de Windows** > **Registro**.
6. Haga clic con el botón secundario en el registro y seleccione **Nuevo** > **Elemento de registro**. Complete lo siguiente.

   Acción: Crear

   Subárbol: HKEY_LOCAL_MACHINE

   Ruta de la clave: SOFTWARE\Dell\Dell Data Protection

   Nombre del valor: Servidor

   Tipo de valor: REG_SZ

   Datos de valor: <Dirección IP o FQDN del Dell Server>

7. Haga clic en **Aceptar**.
8. Cierre sesión y vuelva a iniciarla en la estación de trabajo o ejecute `gpupdate /force` para aplicar la política del grupo.

# 13

# Extracción de instaladores secundarios

- Para instalar cada cliente de manera individual, extraiga los archivos secundarios ejecutables del instalador.
- El instalador maestro no es un *desinstalador* maestro. Cada componente se debe desinstalar por separado, seguido de la desinstalación del instalador maestro. 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 que el archivo **DDSSetup.exe** e ingrese:

   ```
   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\.`

# 14

# Configurar Key Server

- En esta sección se explica cómo configurar los componentes a fin de utilizarlos con la autenticación/autorización Kerberos al utilizar un Security Management Server. Security Management Server Virtual no utiliza Key Server.

  Key Server es un servicio que está atento a la conexión de clientes a un socket. Al conectarse un cliente, se negocia, autentica y cifre una conexión segura, con el uso de las interfaces API de Kerberos (si no se puede negociar una conexión segura, se desconecta al cliente).

  Key Server comprueba luego con Security Server (antes, Device Server) para ver si el usuario que ejecuta al cliente tiene permiso de acceso a las claves. Este acceso se concede a través de dominios individuales en la consola de administración.

- Si se va a utilizar la autenticación/autorización Kerberos, entonces el servidor que contiene el componente Key Server deberá formar parte del dominio afectado.
- Como el Security Management Server Virtual no utiliza Key Server, se ve afectada la desinstalación normal. Cuando se desinstala un cliente Encryption que está activado en un Security Management Server Virtual, se utiliza la recuperación de clave forense estándar a través de Security Server, en lugar del método Kerberos de Key Server. Consulte Desinstalación de la línea de comandos para obtener más información.

## Panel Servicios: Agregar usuario de cuenta de dominio

1. En Security Management Server, vaya al panel servicios (Inicio > Ejecutar > services.msc > Aceptar).
2. Haga clic con el botón derecho del mouse en Key Server y seleccione **Propiedades**.
3. Seleccione la pestaña Iniciar sesión y seleccione la opción **Esta cuenta:**.

   En *Esta cuenta:*, agregue el usuario de cuenta de dominio. Este usuario de dominio debe tener al menos derechos de administrador local a la carpeta de Key Server (debe poder escribir en el archivo de configuración de Key Server, y también escribir en el archivo log.txt).

   Introduzca y confirme la contraseña del usuario de dominio.

   Haga clic en **Aceptar**.
4. Reinicie el servicio de Key Server (deje abierto el panel servicios para ejecutar acciones posteriores).
5. Vaya a <Key Server install dir> log.txt a fin de comprobar que el servicio arrancó correctamente.

## Archivo de configuración del Key Server: agregar usuario para la comunicación de Security Management Server

1. Vaya a <Key Server install dir>.
2. Abra `Credant.KeyServer.exe.config` con un editor de texto.
3. Vaya a <add key="user" value="superadmin" /> y cambie el valor de "superadmin" al nombre del usuario correspondiente (también puede dejarlo como "superadmin").

   El formato "superadmin" puede ser cualquier método que pueda autenticarse con Security Management Server. El nombre de la cuenta del SAM, el nombre UPN y también el formato "DOMINIO/Nombre de usuario" son aceptables. Cualquier método que se pueda autenticar con Security Management Server es aceptable porque se requiere la validación de esa cuenta de usuario para obtener autorización de Active Directory.

   Por ejemplo, en un entorno multidominios, si solo se coloca el nombre de la cuenta del SAM, "jdoe", probablemente fallará porque Security Management Server no puede autenticar "jdoe", ya que no puede encontrar "jdoe". En un entorno multidominios, se recomienda el formato UPN, aunque el formato "DOMINIO/Nombre de usuario" también es aceptable. En un entorno de dominio único, es aceptable el nombre de la cuenta del SAM.

4. Vaya a <add key="epw" value="<encrypted value of the password>" /> y cambie "epw" a "password". Luego proceda a cambiar el texto "<encrypted value of the password>" a la contraseña del usuario (paso 3). La contraseña se cifrará nuevamente cuando se reinicie Security Management Server.

   Si se utiliza "superadmin" en el paso 3, y la contraseña del superadministrador no es "changeit", se debe cambiar aquí. Guarde y cierre el archivo.

## Ejemplo de archivo de configuración

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [El puerto TCP que escuchará Key Server. El valor predeterminado es 8050].

<add key="maxConnections" value="2000" /> [cantidad de conexiones activas de sockets que permitirá Key Server]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [URL de Security Server (antes Device Server) (el formato es 8081/xapi para un Security Management Server anterior a la versión 7.7)]

<add key="verifyCertificate" value="false" /> [El valor "verdadero" comprueba los certificados. El valor "falso" no los comprueba, y también cuando se utilizan certificados auto-firmados]

<add key="user" value="superadmin" /> [El nombre de usuario para comunicarse con Security Server. Este usuario debe tener seleccionada la función de administrador en la consola de administración. El formato "superadmin" puede ser cualquier método que pueda autenticarse con Security Management Server. El nombre de la cuenta del SAM, el nombre UPN y también el formato "DOMINIO/Nombre de usuario" son aceptables. Cualquier método que se pueda autenticar con Security Management Server es aceptable porque se requiere la validación de esa cuenta de usuario para obtener autorización de Active Directory. Por ejemplo, en un entorno multidominios, si solo se coloca el nombre de la cuenta del SAM, "jdoe", probablemente fallará porque Security Management Server no puede autenticar "jdoe", ya que no puede encontrar "jdoe". En un entorno multidominios, se recomienda el formato UPN, aunque el formato "DOMINIO/Nombre de usuario" también es aceptable. En un entorno de dominio único, es aceptable el nombre de la cuenta del SAM.]

<add key="cacheExpiration" value="30" /> [Con qué frecuencia (en segundos) debe comprobar Service para ver quiénes tienen permiso de pedir claves. El servicio mantiene una memoria caché y lleva el seguimiento de la antigüedad. Una vez que la información en la memoria caché tenga más antigüedad que el valor, se obtiene una lista nueva. Al conectarse un usuario, Key Server debe descargar los usuarios autorizados desde Security Server. Si no hay información de los usuarios en la memoria caché o si la lista no se ha descargado en los últimos “x” segundos, se volverá a descargar. No se hace sondeo, sino que este valor configura qué tan antigua puede llegar a ser la lista antes de que se actualice, cuando se considere necesario].

<add key="epw" value="encrypted value of the password" /> [Contraseña que se utiliza para comunicarse con Security Management Server. Si la contraseña "superadmin" fue cambiada, se debe cambiar aquí.]

</appSettings>

</configuration>

# Panel Servicios: Reiniciar el servicio Key Server

1. Regrese al panel de servicios de Windows (Inicio > Ejecutar > services.msc > Aceptar).
2. Reinicie el servicio Key Server.
3. Vaya a <Key Server install dir> log.txt a fin de comprobar que el servicio arrancó correctamente.
4. Cierre el panel de servicios.

# Management Console: agregar administrador forense

1. Como un administrador de Dell, inicie sesión en la Management Console.
2. Haga clic en **Poblaciones** > **Dominios**.
3. Seleccione el dominio adecuado.
4. Haga clic en la pestaña **Key Server**.

5. En *Cuenta*, agregue el usuario que realizará las actividades de administrador. El formato es DOMINIO\Nombre de usuario. Haga clic en **Agregar cuenta**.
6. En el menú de la izquierda, haga clic en **Usuarios**. En la casilla de búsqueda, escriba el nombre de usuario que se agregó en el paso 5. Haga clic en **Buscar**.
7. Una vez que haya encontrado al usuario correcto, haga clic en la pestaña **Admin**.
8. Seleccione **Administrador forense** y haga clic en **Actualizar**.

   Los componentes estarán ya configurados para la autenticación/autorización Kerberos.

# 15

# Uso de la Utilidad de descarga administrativa (CMGAd)

- Esta herramienta permite la descarga de un paquete de material de claves para usar en una computadora que no esté conectada a Dell Server.
- Esta utilidad emplea uno de los siguientes métodos para descargar un paquete de materiales de claves según el parámetro de línea de comandos pasado a la aplicación:
  - Modo Forense: se utiliza si se pasa -f en la línea de comandos o si no se utiliza ningún parámetro de línea de comandos.
  - Modo Administración: se utiliza si se pasa -a en la línea de comandos.

    Los archivos de registro se encuentran en `C:\ProgramData\CmgAdmin.log`

## Utilizar el modo Forense

1. Haga doble clic en **`cmgad.exe`** para iniciar la utilidad o abra un símbolo del sistema en el que se encuentre CMGAd y escriba **`cmgad.exe -f`** (o **`cmgad.exe`**).
2. Introduzca la siguiente información (algunos campos pueden estar previamente rellenados).

   URL del servidor de dispositivo: URL completa del servidor de seguridad (servidor de dispositivo). El formato es https://securityserver.domain.com:8443/xapi/. Si la versión de Dell Server es anterior a la versión 7.7, el formato es https://deviceserver.domain.com:8081/xapi (número de puerto diferente, sin la barra final).

   Administrador de Dell: nombre del administrador con credenciales de administrador forense, como jdoe (activado en la consola de administración)

   Contraseña: contraseña de administrador forense

   MCID: Id. de máquina, como por ejemplo, machineID.domain.com

   DCID: primeros ocho dígitos de la Id. de Shield de 16 dígitos

   **NOTA:**

   Normalmente, es suficiente con especificar el MCID *o* DCID. No obstante, si conoce ambos, es útil especificar los dos. Cada parámetro contiene información diferente utilizada por esta utilidad.

   Haga clic en **Siguiente**.

3. En *Frase de contraseña:* introduzca una frase de contraseña para proteger el archivo de descarga. La frase de contraseña debe tener al menos ocho caracteres de longitud, y contener al menos un carácter alfabético y uno numérico. Confirme la frase de contraseña.

   Acepte el nombre y la ubicación predeterminados de donde el archivo se guardará o haga clic en ... para seleccionar otra ubicación.

   Haga clic en **Siguiente**.

   Aparecerá un mensaje, indicando que el material de claves se ha desbloqueado correctamente. Los archivos son ahora accesibles.

4. Haga clic en **Finalizar** cuando haya terminado.

## Utilizar el modo Administrador

Security Management Server Virtual no utiliza el Key Server, así que el modo de administrador no podrá usarse para obtener una agrupación de claves de Security Management Server Virtual. Utilice el modo Forense para obtener la agrupación de claves si el cliente está activado en un Security Management Server Virtual.

1. Abra un símbolo del sistema donde se encuentre CMGAd y escriba **`cmgad.exe -a`**.
2. Introduzca la siguiente información (algunos campos pueden estar previamente rellenados).

   Servidor: nombre de host completo del Key Server, por ejemplo, keyserver.domain.com

   Número de puerto: el puerto predeterminado es 8050.

   Cuenta de servidor: usuario de dominio con el que se ejecuta Key Server. El formato es DOMINIO\Nombre de usuario. El usuario de dominio que ejecuta la utilidad debe estar autorizado para realizar la descarga desde Key Server

   MCID: Id. de máquina, como por ejemplo, machineID.domain.com

   DCID: primeros ocho dígitos de la Id. de Shield de 16 dígitos

   **NOTA:**

   Normalmente, es suficiente con especificar el MCID *o* DCID. No obstante, si conoce ambos, es útil especificar los dos. Cada parámetro contiene información diferente utilizada por esta utilidad.

   Haga clic en **Siguiente**.

3. En *Frase de contraseña*, escriba una frase de contraseña para proteger el archivo de descarga. La frase de contraseña debe tener al menos ocho caracteres de longitud, y contener al menos un carácter alfabético y uno numérico.

   Confirme la frase de contraseña.

   Acepte el nombre y la ubicación predeterminados de donde el archivo se guardará o haga clic en ... para seleccionar otra ubicación.

   Haga clic en **Siguiente**.

   Aparecerá un mensaje, indicando que el material de claves se ha desbloqueado correctamente. Los archivos son ahora accesibles.

4. Haga clic en **Finalizar** cuando haya terminado.

16

# Configurar Encryption en un sistema operativo de servidor

## Habilitación de Encryption en un sistema operativo de servidor

**NOTA:**

Encryption de sistemas operativos de servidor convierte el cifrado de usuario en cifrado común.

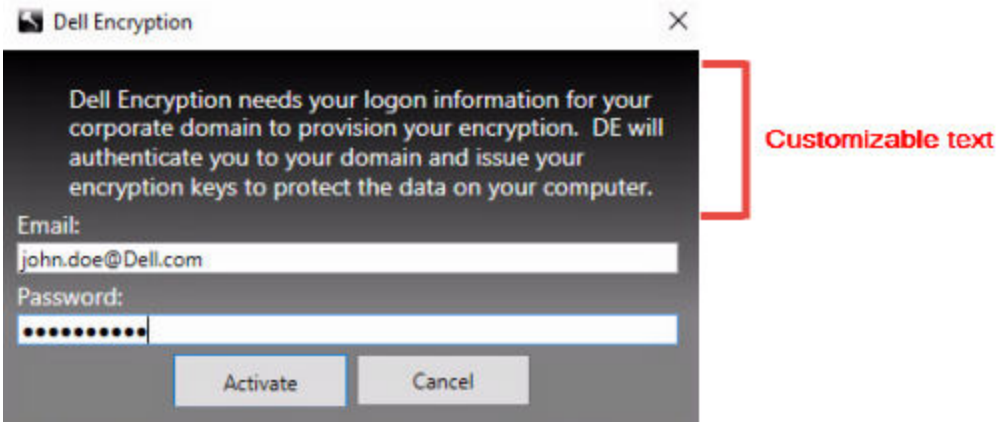
1. Como un administrador de Dell, inicie sesión en la Management Console.
2. Seleccione **Grupo de terminales** (o **Terminal**), busque el terminal o grupo de terminales que se habilitará, seleccione **Políticas de seguridad** y, a continuación, seleccione la categoría de la política **Server Encryption**.
3. Establezca las siguientes políticas:
   - Encryption de servidor: **seleccione** para habilitar Encryption en un sistema operativo de servidor y las políticas relacionadas.
   - Cifrado de SDE habilitado: **seleccione** para activar el cifrado de SDE.
   - Cifrado habilitado: **seleccione** para activar el cifrado común.
   - Credenciales de Windows seguras: esta política está **seleccionada** de manera predeterminada.

     Cuando la política *Credenciales de Windows seguras* está establecida en **Seleccionado** (el valor predeterminado), se cifran todos los archivos de la carpeta \Windows\system32\config, incluidas las credenciales de Windows. Para evitar el cifrado de las credenciales de Windows, establezca la política Credenciales de Windows seguras en **No seleccionado**. El cifrado de las credenciales de Windows se produce independientemente de la configuración de la política *Cifrado de SDE habilitado*.
4. Guarde y confirme las políticas.

## Personalizar cuadro de diálogo Inicio de sesión de activación

Se muestra el cuadro de diálogo Inicio de sesión de activación:

- Cuando un usuario no administrado inicia sesión.
- Cuando el usuario selecciona Activar Dell Encryption en el menú del icono Encryption, ubicado en el área de notificación.



# Establecer políticas de Encryption External Media

La ***computadora de cifrado original*** es la computadora que cifra originalmente un dispositivo extraíble. Cuando la computadora original es un ***servidor protegido***, un servidor con Encryption en un sistema operativo de servidor instalado y activado, y el servidor protegido detecta primero la presencia de un dispositivo extraíble, al usuario se le pide que cifre el dispositivo extraíble.

- Las políticas de Encryption External Media controlan el acceso de medios extraíbles al servidor, autenticación, cifrado, etc.
- Las políticas de Control de puertos afectan a medios extraíbles en servidores protegidos, por ejemplo, mediante el control del acceso y uso de los puertos USB del servidor por parte de dispositivos USB.

Se pueden encontrar las políticas para cifrado de medios extraíbles en la consola de administración en el grupo de tecnología *Server Encryption*.

**Encryption en un sistema operativo de servidor y External Media**

Cuando la política *Medios externos de cifrado de EMS* del servidor protegido está establecida en **Seleccionado**, se cifran los medios externos. Encryption vincula el dispositivo al servidor protegido con la clave de máquina y al usuario con la clave de usuario en roaming del propietario/usuario del dispositivo extraíble. Todos los archivos agregados al dispositivo extraíble se cifrarán a continuación con las mismas claves, independientemente de la computadora a la que esté conectado.

**NOTA:**

Encryption en un sistema operativo de servidor convierte el cifrado de usuario en cifrado común, excepto en dispositivos extraíbles. En dispositivos extraíbles, el cifrado se realiza con la clave de Usuario en roaming asociada a la computadora.

Si el usuario no acepta cifrar el dispositivo extraíble, el acceso del usuario al dispositivo puede establecerse como *Bloqueado* si se utiliza en el servidor protegido, como *Solo lectura* mientras se utiliza en el servidor protegido o como *Acceso total*. Las políticas del servidor protegido determinan el nivel de acceso en un dispositivo extraíble no protegido..

Las actualizaciones de política se producen cuando el dispositivo extraíble se vuelve a insertar en el servidor protegido original.

**Autenticación y medios externos**

Las políticas del servidor protegido determinan la funcionalidad de autenticación.

Después del cifrado de un dispositivo extraíble, solo su propietario/usuario puede acceder al dispositivo extraíble en el servidor protegido. Otros usuarios no pueden acceder a los archivos cifrados en el medio extraíble.

La autenticación automática local permite que el medio extraíble protegido se autentique automáticamente cuando se inserta en el servidor protegido cuando el propietario de ese medio inicia sesión. Cuando la autenticación automática está deshabilitada, el propietario/usuario debe autenticarse para acceder al dispositivo extraíble protegido.

Si la computadora de cifrado original de un dispositivo extraíble es un servidor protegido, el propietario/usuario siempre debe iniciar sesión en el dispositivo extraíble cuando lo utilice en computadoras que no sean el equipo original, independientemente de la configuración de la política de Encryption External Media definida en las otras computadoras.

Consulte AdminHelp para obtener más información sobre las políticas de Encryption External Media y el Control de puertos de Server Encryption.

# Suspensión de Encryption en un sistema operativo de servidor

Suspender un servidor cifrado impide el acceso a sus datos cifrados tras el reinicio. El usuario del servidor virtual no puede suspenderse. En lugar de eso, se suspende la clave de máquina del servidor cifrado.

**NOTA:**

La suspensión de un extremo del servidor no suspende inmediatamente al servidor. La suspensión tiene lugar la siguiente vez que se solicite la clave, normalmente la siguiente vez que se reinicie el servidor.

**NOTA:**

Úselo con cuidado. Si se suspende un servidor cifrado, se podría generar inestabilidad según la configuración de la política y si el servidor protegido se suspende mientras está desconectado de la red.

**Requisitos previos**

- Los derechos de administrador de soporte técnico, asignados en la consola de administración, son necesarios para suspender un terminal.
- El administrador debe iniciar sesión en la consola de administración.

  En el panel izquierdo de la consola de administración, haga clic en **Poblaciones** > **Terminales**.

  Busque o seleccione un nombre de host y, a continuación, haga clic en la pestaña **Detalles y acciones**.

  En *Control de dispositivo del servidor*, haga clic en **Suspender** y, a continuación, **Sí**.

  **NOTA:**

  Haga clic en **Restablecer** para permitir que Encryption de sistemas operativos de servidor acceda a los datos cifrados en el servidor después de su reinicio.

17

# Configurar la activación aplazada

El cliente Encryption con activación aplazada difiere de la activación del cliente Encryption de dos maneras:

**Políticas de cifrado basadas en dispositivos**

Las políticas del cliente Encryption se basan en usuarios; las políticas de cifrado con activación aplazada del cliente Encryption se basan en dispositivos. El cifrado de usuario se convierte en cifrado común. Esta diferencia permite al usuario utilizar un dispositivo personal dentro del dominio de la organización sin que esta pierda seguridad, ya que las políticas de cifrado se administran de forma centralizada.

**Activación**

Con el cliente Encryption, la activación es automática. Si se instala con activación aplazada, la activación automática se deshabilita. En su lugar, el usuario elige si desea activar el cifrado y cuándo hacerlo.

**NOTA:**

Antes de que un usuario deje permanentemente una organización y mientras su dirección de correo electrónico siga activa, el usuario debe ejecutar Encryption Removal Agent y desinstalar el cliente Encryption de su equipo personal.

# Personalizar la activación aplazada

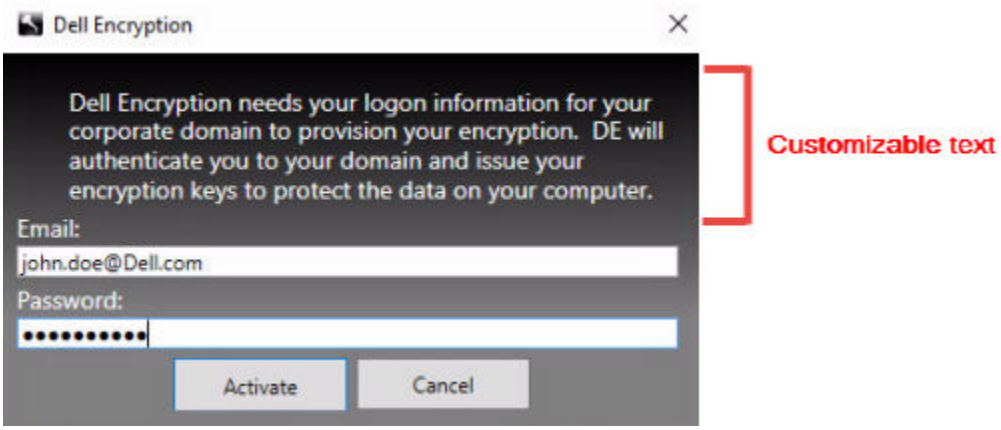
Estas tareas del lado del cliente permiten la personalización de la activación aplazada.

- Agregar una declinación de responsabilidades al cuadro de diálogo de inicio de sesión de la activación
- Deshabilitar la reactivación automática (opcional)

Agregar una declinación de responsabilidades al cuadro de diálogo de inicio de sesión de la activación

El diálogo de inicio de sesión en la activación se muestra:

- Cuando un usuario no administrado inicia sesión.
- Cuando el usuario selecciona Activar Dell Encryption en el menú del icono Encryption, ubicado en el área de notificación.




# Preparar el equipo para la instalación

Si los datos se cifran con un producto de cifrado que no es de Dell, antes de instalar el cliente Encryption, descifre los datos mediante el software de cifrado existente y, a continuación, desinstale dicho software. Si el equipo no se reinicia automáticamente, reinícielo.

**Crear una contraseña de Windows**

Dell recomienda encarecidamente que cree una contraseña de Windows, si es que no cuenta ya con una, para proteger el acceso a los datos cifrados. La creación de una contraseña en su equipo evita que otras personas puedan iniciar sesión en su cuenta de usuario sin su contraseña.

**Desinstalar versiones anteriores del cliente Encryption**

Antes de desinstalar una versión anterior del cliente Encryption, detenga o pause el barrido de cifrado si es necesario.

Si el equipo está ejecutando una versión de Dell Encryption anterior a v8.6, desinstale el cliente Encryption desde la línea de comandos. Para obtener instrucciones, consulte *Desinstalación de los clientes Encryption y Server Encryption*.

**NOTA:**

Si va a instalar la versión más reciente del cliente Encryption inmediatamente tras la desinstalación, no es necesario ejecutar Encryption Removal Agent para descifrar los archivos.

Para actualizar una versión anterior del cliente Encryption instalado con activación aplazada, utilice el Desinstalador de Data Security o los Instaladores secundarios. Estos métodos de desinstalación son posibles incluso si OPTIN está deshabilitado.

**NOTA:**

Si no se han activado usuarios previamente, el cliente Encryption borra el valor OPTIN del almacén de SDE, ya que este proviene de una instalación previa. El cliente Encryption bloquea las activaciones aplazadas si se han activado clientes previamente pero la marca OPTIN no está definida en el almacén de SDE.

# Instalar Encryption con activación aplazada

Para instalar el cliente Encryption con activación aplazada, hágalo con el parámetro OPTIN=1. Para obtener más información sobre la instalación de clientes con el parámetro OPTIN=1, consulte Instalación de Encryption.

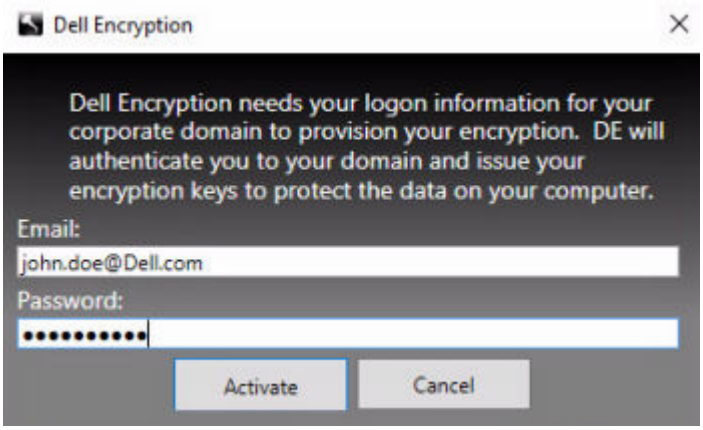
# Activar Encryption con activación aplazada

- La activación asocia a un usuario de dominio con una cuenta de usuario local y un equipo específico.
- Varios usuarios pueden activarse en el mismo equipo, siempre que usen cuentas locales exclusivas y tengan direcciones de correo electrónico de dominio únicas.
- Un usuario puede activar el cliente Encryption solo una vez por cuenta de dominio.

Antes de activar el cliente Encryption:

- Inicie sesión en la cuenta local que utiliza con mayor frecuencia. Los datos asociados a esta cuenta serán los que se cifrarán.
- Conéctese a la red de su organización.

1. Inicie sesión en la estación de trabajo o en el servidor.
2. Introduzca la dirección de correo electrónico y la contraseña del dominio y haga clic en **Activar**.




**NOTA:**

Para la activación no se pueden utilizar direcciones de correo electrónico que no pertenezcan al dominio o que sean personales.

3. Haga clic en **Cerrar**.

   El servidor Dell combina el paquete de claves de cifrado con las credenciales de usuario y el ID exclusivo del equipo (ID de máquina). De esta manera, crea una relación irrompible entre el paquete de claves, el equipo específico y el usuario.

4. Reinicie el equipo para empezar el barrido de cifrado.

   **NOTA:**

   En la consola de administración local, accesible desde el ícono del área de notificación, se muestran las políticas que envía el servidor, no la política vigente.

# Solucionar problemas de la activación aplazada

## Solucionar problemas de activación

**Problema: no se puede obtener acceso a ciertos archivos y carpetas**

La incapacidad de acceder a determinados archivos y carpetas es un síntoma de haber iniciado sesión con una cuenta diferente a aquella con la que el usuario se ha activado.

El diálogo de inicio de sesión en la activación se muestra automáticamente incluso si el usuario se ha activado previamente.

**Posible solución**

Cierre sesión y vuelva a iniciarla con las credenciales de la cuenta activada e intente acceder a los archivos de nuevo.

En el caso de que el cliente Encryption no pueda autenticar al usuario, el diálogo de inicio de sesión en la activación solicita al usuario las credenciales de autenticación y acceso a las claves de cifrado. Para utilizar la función de reactivación automática, AMBAS claves de registro *AutoReactivation* y *AutoPromptForActivation* deben estar habilitadas. Aunque la función esté habilitada de forma predeterminada, se puede deshabilitar manualmente. Para obtener más información, consulte Deshabilitar la reactivación automática.

**Mensaje de error: Error de autenticación del servidor**

El servidor no pudo autenticar la dirección de correo electrónico y la contraseña.

**Posibles soluciones**

- Utilice la dirección de correo electrónico asociada a la organización. Las direcciones de correo electrónico personales no se pueden utilizar para la activación.
- Vuelva a introducir la dirección de correo electrónico y la contraseña, y asegúrese de que no hay errores tipográficos.
- Solicite al administrador la verificación de que la cuenta de correo electrónico está activa y no está bloqueada.
- Solicite al administrador el restablecimiento de la contraseña de dominio del usuario.

  **Mensaje de error: Error de conexión de red**

  El cliente Encryption no se ha podido comunicar con el servidor Dell.

  **Posibles soluciones**

- Conéctese directamente a la red de la organización e intente la activación de nuevo.
- Si es necesario el acceso VPN para conectarse a la red, compruebe la conexión VPN y vuelva a intentarlo.
- Compruebe la URL del Dell Server para asegurarse de que coincida con la proporcionada por el administrador.

  La URL y otros datos que el usuario introduzca en el instalador se guardan en el registro. Compruebe la precisión de los datos en [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] y [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

- Desconecte y vuelva a conectar:

  Desconecte el equipo de la red.

  Vuelva a conectar a la red.

  Reinicie el equipo.

  Intente volver a conectar a la red.

**Mensaje de error: Servidor heredado no compatible**

Encryption no se puede activar con un servidor heredado; la versión del Dell Server debe ser 9.1 o posterior.

**Posible solución**

- Compruebe la URL del Dell Server para asegurarse de que coincida con la proporcionada por el administrador.

  La URL y otros datos que el usuario introduzca en el instalador se guardan en el registro.

- Compruebe la precisión de los datos en [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] y [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

  **Mensaje de error: Usuario de dominio ya activado**

  Un segundo usuario ha iniciado sesión en el equipo local y ha intentado activarse con una cuenta de dominio que ya está activada.

  Un usuario puede activar el cliente Encryption solo una vez por cuenta de dominio.

  **Posible solución**

  Descifre y desinstale el cliente Encryption mientras esté conectado como segundo usuario activado.

  **Mensaje de error: Error de servidor general**

  Se produjo un error en el servidor.

  **Posible solución**

  El administrador debe comprobar los registros del servidor para asegurarse de que los servicios se están ejecutando.

  El usuario debe volver a intentar la activación más tarde.

**Herramientas**

CMGAd

Utilice la utilidad CMGAd antes de iniciar Encryption Removal Agent para obtener un paquete de claves de cifrado. La utilidad CMGAd y sus instrucciones se encuentran en los medios de instalación de Dell (Dell-Offline-Admin-XXbit)

**Archivos de registro**

En `C:\ProgramData\Dell\Dell Data Protection\Encryption`, busque el archivo de registro llamado **CmgSysTray**.

Busque la frase "Manual activation result".

El código de error se encuentra en la misma línea, seguida de " status = "; el estado indica la causa del problema.

# 18

# Solución de problemas

## Todos los clientes: Solución de problemas

- Los archivos de registro del instalador del conjunto maestro se encuentran en `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows crea **archivos de registro de instalación de instaladores secundarios** para el usuario que haya iniciado sesión en %temp%, que se encuentra en `C:\Users\<Nombre de usuario>\AppData\Local\Temp`.
- Windows crea archivos de registro para requisitos previos de cliente, como Visual C++, para el usuario que ha iniciado sesión en %temp%, que se encuentra en `C:\Users\<Nombre de usuario>\AppData\Local\Temp`. Por ejemplo, `C:\Users\<Nombre de usuario>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log`
- Siga las instrucciones disponibles en http://msdn.microsoft.com para verificar la versión de Microsoft .Net instalada en el equipo de destino de la instalación.

  Vaya a https://www.microsoft.com/en-us/download/details.aspx?id=30653para descargar la versión completa de Microsoft .Net Framework 4.5.2 o posterior.
- Consulte este documento si la computadora en la que se va a realizar la instalación tiene (o ha tenido) Dell Access instalado. Dell Access no es compatible con este conjunto de productos.

## Todos los clientes: estado de la protección

En Dell Server versión v9.8.2, se implementó un nuevo método para derivar el estado protegido de un dispositivo. Anteriormente, el área de estado protegido de terminal en el panel de la consola de administración solo denotaría el estado de Encryption por dispositivo.

Para Dell Server v9.8.2, el estado protegido ahora se señala si se cumple alguno de los siguientes criterios:

- Está instalada y activada Advanced Threat Prevention.
- La protección web o el firewall de cliente está instalado y está activada la política de la protección web o la del firewall de cliente.
- El administrador de unidades de autocifrado está instalado y activado, y la PBA está habilitada.
- El cifrado de disco completo está instalado y activado, y la PBA está habilitada.
- BitLocker Manager está instalado, activado y se completó el cifrado.
- Dell Encryption (Mac) está instalado y activado, y *Cifrado mediante FileVault para Mac* se aplicó.
- Dell Encryption (Windows) está instalado, activado y se estableció el cifrado basado en la política para el extremo y los barridos de dispositivo están completos.

## Solución de problemas de Dell Encryption (cliente y servidor)

### Activación remota en un sistema operativo de servidor

Cuando el cifrado está instalado en un sistema operativo de servidor, la activación requiere dos fases de activación: activación inicial y activación del dispositivo.

**Solución de la activación inicial**

La activación inicial falla cuando:

- No se puede construir un UPN válido mediante las credenciales proporcionadas.
- Las credenciales no se encuentran en el almacén de Enterprise.
- Las credenciales que se utilizan para la activación no son las del administrador del dominio.

**Mensaje de error: Nombre de usuario desconocido o contraseña incorrecta**

El nombre de usuario o contraseña no coinciden.

Posible solución: intente volver a iniciar sesión, asegurándose de introducir el nombre de usuario y contraseña de forma exacta.

**Mensaje de error: Se produjo un error en la activación debido a que la cuenta de usuario no tiene derechos de administración del dominio.**

Las credenciales que se utilizan para la activación no tienen derechos de administración del dominio o el nombre de usuario del administrador no estaba en formato UPN.

Posible solución**:** En el diálogo de Activación, ingrese las credenciales en formato UPN de un administrador de dominios.

**Mensajes de error: No se ha podido establecer una conexión con el servidor.**

O bien

```
The operation timed out.
```

Server Encryption no se ha podido comunicar con el puerto 8449 a través de HTTPS con el servidor Dell.

**Posibles soluciones**

- Conéctese directamente con su red e intente la activación de nuevo.
- Si se conectara mediante VPN, intente conectarse directamente a la red y vuelva a intentar la activación.
- Compruebe la URL del Dell Server para asegurarse de que coincida con la URL proporcionada por el administrador. La URL y otros datos que el usuario introduzca en el instalador se guardan en el registro. Compruebe la precisión de los datos en [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] y [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Desconecte el servidor de la red. Reinicie el servidor y vuelva a conectar a la red.

**Mensaje de error: Ha fallado la activación porque el servidor no puede respaldar la solicitud.**

**Posibles soluciones**

- Server Encryption no se puede activar con un servidor heredado; la versión del Dell Server debe ser la versión 9.1 o posterior. Si fuera necesario, actualice el Dell Server a la versión 9.1 o posterior.
- Compruebe la URL del Dell Server para asegurarse de que coincida con la URL proporcionada por el administrador. La URL y otros datos que el usuario introduzca en el instalador se guardan en el registro.
- Compruebe la precisión de los datos en [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] y [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

**Proceso de activación inicial**

El siguiente diagrama muestra una activación inicial correcta.

El proceso de activación inicial de Encryption en los sistemas operativos de servidores requiere un usuario en directo para acceder al servidor. El usuario puede ser de cualquier tipo: con dominio o sin dominio, un usuario interactivo o conectado desde un escritorio remoto, pero este debe tener acceso a las credenciales de administrador del dominio.

El cuadro de diálogo Activación aparece cuando se produce uno de dos flujos de trabajo:

- Un nuevo usuario (no administrado) inicia sesión en el equipo.
- Cuando un nuevo usuario hace clic con el botón secundario en el icono *Encryption* en el área de notificaciones y selecciona *Activar Dell Encryption*.

  El proceso de activación inicial es el siguiente:

1. El usuario inicia sesión.
2. Tras detectar un nuevo usuario (no administrado), se muestra el cuadro de diálogo *Activar*. El usuario hace clic en **Cancelar**.
3. El usuario abre el cuadro Acerca de Server Encryption para confirmar que se está ejecutando en modo Servidor.
4. El usuario hace clic con el botón secundario en el icono *Encryption* en el área de notificaciones y selecciona *Activar Dell Encryption.*
5. El usuario ingresa las credenciales de administrador de dominios en el cuadro de diálogo Activar.

   **NOTA:**

   El requisito de credenciales de administrador de dominios es una medida de seguridad que impide la implementación de Encryption de sistemas operativos de servidor en entornos de servidor no admitidos. Para desactivar el requisito para credenciales de administrador de dominios, consulte Antes de empezar.
6. El Dell Server comprueba las credenciales en el vault de la empresa (Active Directory o equivalente) para comprobar que las credenciales sean las de un administrador de dominio.

7. Un UPN se construye utilizando las credenciales.
8. Con el UPN, el Dell Server crea una cuenta de usuario nueva para el usuario del servidor virtual y almacena las credenciales en el almacén del Dell Server.

   La **cuenta de usuario de servidor virtual** es para uso exclusivo del cliente Encryption. Se utilizará para autenticar con el servidor, para administrar las claves de cifrado común y para recibir las actualizaciones de política.

   **NOTA:**

   La contraseña y la autenticación DPAPI están desactivadas para esta cuenta para que *solo* el usuario de servidor virtual pueda acceder a las claves de cifrado en el equipo. Esta cuenta no se corresponde con ninguna otra cuenta de usuario en el equipo o en el dominio.
9. Cuando la activación se realiza correctamente, el usuario debe reiniciar el equipo y comenzar la segunda parte de dicha activación, autenticación y activación del dispositivo.

**Solución de problemas de la autenticación y activación del dispositivo**

La activación del dispositivo falla cuando:

- Ha fallado la activación inicial.
- No se ha podido establecer la conexión con el servidor.
- No se ha podido validar el certificado de confianza.

Después de la activación, cuando se reinicia la computadora, Encryption para sistemas operativos de servidor inicia sesión automáticamente como el usuario de servidor virtual y solicita la clave de equipo al Dell Server. Esto tiene lugar incluso antes de que cualquier usuario pueda iniciar sesión.

- Abra el cuadro de diálogo Acerca de para confirmar que Encryption para sistemas operativos de servidor está autenticado y en modo Servidor.
- Si la Id. de Encryption client está en rojo, el cifrado aún no se ha activado.
- En la consola de administración, la versión de un servidor con Server Encryption instalado se incluye como *Shield para servidor*.
- Si falla la recuperación de la clave de máquina debido a un error de red, Server Encryption registra notificaciones de red con el sistema operativo.
- Si falla la recuperación de la clave de máquina:
  - El inicio de sesión de usuario de servidor virtual sigue siendo correcto.
  - Configure la política *Reintentar el intervalo tras un error de red* para realizar intentos de recuperación de la clave en un intervalo de tiempo.

    Para obtener detalles acerca de la política *Volver a intentar intervalo tras una falla en la red*, consulte AdminHelp, disponible en la consola de administración.

**Autenticación y activación de dispositivo**

El siguiente diagrama muestra la autenticación correcta y la activación del dispositivo.

1. Cuando se haya reiniciado después de una activación inicial satisfactoria, un equipo con cifrado del servidor se autentica automáticamente mediante la cuenta de usuario de servidor virtual y se ejecuta el cliente Encryption en modo Servidor.
2. La computadora comprueba su estado de activación de dispositivo con el Dell Server:
   - Si el equipo no tiene activación previa de dispositivo, el Dell Server asigna a la computadora un MCID, un DCID y un certificado de confianza, y almacena toda la información en el almacén del Dell Server.
   - Si la computadora tiene activación previa de dispositivo, el Dell Server verifica el certificado de confianza.
3. Después de que el Dell Server asigne el certificado de confianza al servidor, el servidor puede acceder a sus claves de cifrado.
4. La activación del dispositivo es correcta.

   **NOTA:**

   Durante la ejecución en modo Servidor, el cliente Encryption debe tener acceso al mismo certificado que se utilizó en la activación del dispositivo para acceder a las claves de 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 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.

**Uso de la línea de comandos de WSScan**

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r]
[-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

| Modificador | Significado |
|---|---|
| Unidad | Unidad que explorar. Si no se especifica, el valor predeterminado es todas las unidades de disco duro fijas locales. Puede ser una unidad de red asignada. |
| -ta | Explorar todas las unidades |
| -tf | Explorar unidades fijas (valor predeterminado) |
| -tr | Explorar unidades extraíbles |
| -tc | Explorar CDROM/DVDROM |
| -s | Operación silenciosa |
| -o | Ruta de acceso del archivo de salida |
| -a | Anexar a archivo de salida. El comportamiento predeterminado trunca el archivo de salida. |

| Modificador | Significado |
|---|---|
| -f | Informar sobre el especificador de formato (Informar, Fijo, Delimitado) |
| -r | Ejecutar WSScan sin privilegios de administrador. **En este modo, es posible que algunos archivos no se puedan visualizar.** |
| -u | Incluir archivos no cifrados en el archivo de salida.<br>Este conmutador es sensible al orden: "u" debe estar primero, "a" debe estar segundo (u omitirse), "-" o "v" debe estar último. |
| -u- | Solo incluir archivos no cifrados en archivo de salida |
| -ua | Informar también de archivos no cifrados, pero usar todas las políticas de usuario para mostrar el campo "should". |
| -ua- | Informar solo de archivos no cifrados, pero usar todas las políticas de usuario para mostrar el campo "should". |
| -uv | Informar de archivos no cifrados que violen solo la política (Is=No / Should=Y) |
| -uav | Informar de archivos no cifrados que violen solo la política (Is=No / Should=Y), usando todas las políticas de usuario. |
| -d | Especifica qué usar como separador de valores para la salida delimitada |
| -q | Especifica los valores que deben estar entre comillas para la salida delimitada |
| -e | Incluir campos de cifrado ampliados en la salida delimitada |
| -x | Excluir directorio de exploración. Se permiten varias exclusiones. |
| -y | Tiempo de suspensión (en milisegundos) entre directorios. Este modificador produce exploraciones más lentas, pero potencialmente una CPU con más capacidad de respuesta. |

**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.<br>**SysData:** clave de SDE.<br>**Usuario:** clave de cifrado de usuario.<br>**Común:** clave de cifrado común.<br>WSScan no informa archivos cifrados mediante Encrypt for Sharing. |
| KCID | La Id. de equipo clave<br>Como se muestra en el ejemplo anterior, "**7vdlxrsb**"<br>Si se exploró una unidad de red asignada, el informe de exploración no proporciona una KCID. |

| Salida | Significado |
|---|---|
| UCID | La Id. del usuario.<br>Como se muestra en el ejemplo anterior, "**_SDENCR_**"<br>La UCID la comparten todos los usuarios de ese equipo. |
| Archivo | La ruta de acceso del archivo cifrado.<br>Como se muestra en el ejemplo anterior, "**c: \temp\Dell: test.log**" |
| Algoritmo | El algoritmo de cifrado utilizado para cifrar el archivo.<br>Como se muestra en el ejemplo anterior, "**todavía está cifrado según AES256**"<br>RIJNDAEL 128<br>RIJNDAEL 256<br>AES-128<br>AES-256<br>3DES |

# Usar WSProbe

La utilidad de sondeo se debe utilizar con todas las versiones de Encryption con excepción de las políticas de Encryption External Media. Utilice la utilidad de sondeo para:

- Explorar o programar la exploración de un equipo cifrado. La utilidad de sondeo observa la política Prioridad de escaneo de estación de trabajo.
- Deshabilitar temporalmente o volver a habilitar la lista de cifrado de datos de aplicación del usuario actual.
- Agregar o quitar nombres de proceso de la lista de privilegios.
- Solucionar problemas según lo indicado por Dell ProSupport.

### Enfoques sobre el cifrado de datos

Si especifica políticas para cifrar datos en dispositivos Windows, podrá usar cualquiera de los siguientes enfoques:

- El primer enfoque es aceptar el comportamiento predeterminado del cliente. Si especifica carpetas en Carpetas cifradas comunes o Carpetas cifradas por el usuario, o establece Cifrar "Mis documentos", Cifrar carpetas personales de Outlook, Cifrar archivos temporales, Cifrar archivos temporales de Internet, o Cifrar archivo de paginación de Windows en lo seleccionado, los archivos afectados se cifrarán al ser creados, o (después de haber sido creados por un usuario no administrado) al iniciar sesión un usuario administrado. El cliente también explora las carpetas especificadas en, o relacionadas con, estas políticas en busca de posible cifrado/descifrado cuando se cambia el nombre a una carpeta, o cuando el cliente recibe cambios en estas políticas.
- También puede establecer Explorar estación de trabajo al iniciar sesión en Seleccionado. Si está seleccionado Explorar estación de trabajo al iniciar sesión, cuando un usuario inicie sesión, el cliente compara cuántos archivos de carpetas cifradas actualmente, y previamente, están cifrados según las políticas de usuario, y realiza los cambios necesarios.
- Para cifrar archivos que cumplen sus criterios de cifrado pero que se crearon antes de que sus políticas de cifrado entraran en vigor, y si no desea que el rendimiento se vea afectado por una repetida exploración, puede usar esta utilidad para explorar o programar la exploración del equipo.

### Requisitos previos

- El dispositivo Windows con el que desea trabajar debe estar cifrado.
- El usuario con el que desea trabajar debe haber iniciado sesión.

### Usar la utilidad de sondeo

WSProbe.exe se encuentra en el medio de instalación.

### Sintaxis

```
wsprobe [path]
wsprobe [-h]
```

```
wsprobe [-f path]
wsprobe [-u n] [-x process_names] [-i process_names]
```

**Parámetros**

| Parámetro | A |
|---|---|
| path | Opcionalmente, especifique una ruta de acceso concreta en el dispositivo para escanear un posible cifrado/descifrado. Si no especifica una ruta de acceso, esta utilidad explorará todas las carpetas relacionadas con sus políticas de cifrado. |
| -h | Ver la Ayuda de la línea de comandos. |
| -f | Solucionar problemas según lo indicado por Dell ProSupport |
| -u | Deshabilitar temporalmente o volver a habilitar la lista de cifrado de datos de aplicación del usuario. Esta lista solo estará en vigor si está seleccionado Cifrado habilitado para el usuario actual. Especifique 0 para deshabilitarlo o 1 para volver a habilitarlo. La política actual en vigor para el usuario se restablece en el próximo inicio de sesión. |
| -x | Agregar nombres de proceso a la lista de privilegios. Los nombres de proceso del instalador y el equipo de esta lista, más aquellos que agregue usando este parámetro o HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList, se ignorarán si están especificados en la lista de cifrado de datos de aplicación. Separe los nombres de proceso con comas. Si su lista incluye uno o más espacios, ponga la lista entre comillas dobles. |
| -i | Quitar los nombres de proceso previamente agregados a la lista de privilegios (no podrá quitar los nombres de proceso no modificables). Separe los nombres de proceso con comas. Si su lista incluye uno o más espacios, ponga la lista entre comillas dobles. |

## 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. Consulte (Opcional) Creación de un archivo de registro de Encryption Removal Agent para obtener instrucciones.
- **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.

# Solución de problemas de SED

## Uso del código de acceso inicial

- Esta política se utiliza para iniciar sesión en un equipo cuando el acceso a la red no está disponible. Es decir, no hay acceso disponible al Dell Server ni a AD. Utilice la política del *Código de acceso inicial* solo si es absolutamente necesario. Dell no recomienda utilizar este método para iniciar sesión. El uso de la política del *Código de acceso inicial* no proporciona el mismo nivel de seguridad que el método habitual de iniciar sesión con nombre de usuario, dominio y contraseña.

  Además de ser un método menos seguro de inicio de sesión, si un usuario se activa mediante el *Código de acceso inicial*, no quedará registro en el Dell Server de que ese usuario se activó en esta computadora. Por el contrario, no hay manera de generar un Código de respuesta desde el Dell Server para el usuario si falla la contraseña o las respuestas de autoayuda.

- El *Código de acceso inicial* solo se puede utilizar **una** vez, inmediatamente después de la activación. Después de que el usuario final haya iniciado la sesión, el *Código de acceso inicial* ya no volverá a estar disponible. El primer inicio de sesión en el dominio que ocurre tras la introducción del *Código de acceso inicial* se guarda en la memoria caché, y el campo de entrada de *Código de acceso inicial* no se volverá a mostrar.
- El *Código de acceso inicial* se muestra **únicamente** bajo las siguientes condiciones:
  - Un usuario nunca ha sido activado en la PBA.
  - El cliente no tiene conexión a la red o al Dell Server.

**Usar el código de acceso inicial**

1. Configure un valor para la política del **Código de acceso inicial** en la consola de administración.
2. Guarde y confirme la política.
3. Inicie el equipo local.
4. Cuando se muestre la pantalla Código de acceso, introduzca el **Código de acceso inicial**.
5. Haga clic en la **flecha de color azul**.
6. Cuando se muestre la pantalla Aviso legal, haga clic en **Aceptar**.
7. Inicie sesión en Windows con las credenciales de usuario para este equipo. Estas credenciales deben ser parte del dominio.
8. Una vez que inicie sesión, abra Data Security Console y compruebe que se haya creado correctamente el usuario de PBA.

   Haga clic en **Registro** en el menú superior y busque el mensaje *Usuario de PBA creado para <DOMAIN\Username>*, con el cual se indica que el proceso finalizó correctamente.
9. Apague y reinicie el equipo.
10. En la pantalla de inicio de sesión, introduzca el nombre de usuario, dominio y contraseña que se utilizaban previamente para iniciar sesión en Windows.

    Debe utilizar el mismo formato de nombre de usuario que se utilizó cuando se creó el usuario de PBA. De este modo, si utilizó el formato DOMINIO/Nombre de usuario, deberá introducir el DOMINIO/Nombre de usuario para el nombre de usuario.
11. Cuando se muestre la pantalla Aviso legal, haga clic en **Inicio de sesión**.

    Entonces se ejecuta Windows y el equipo se puede usar normalmente.

## Crear un archivo de registro de PBA para la solución de problemas

- Es posible que en ciertas situaciones se requiera un archivo de registro de PBA para solucionar problemas de PBA; por ejemplo:
  - No puede ver el ícono de conexión a la red, aunque sabe que hay conectividad de red. El archivo de registro contiene información de DHCP para resolver el problema.
  - No puede ver el icono de conexión al Dell Server. En el archivo de registro se incluye información para hacer un diagnóstico de los problemas de conectividad.
  - Aparece un error de autenticación aun cuando introduce las credenciales correctas. El archivo de registro, en conjunto con los registros del Dell Server, pueden ayudar a diagnosticar el problema.

**Capturar registros al iniciar en la PBA (PBA heredada)**

1. Cree una carpeta en el nivel raíz de una unidad USB y póngale el nombre **`\CredantSED`**.
2. Cree un archivo con el nombre actions.txt y colóquelo en la carpeta **`\CredantSED`**.

3. En el archivo actions.txt, agregue la línea:

   **get logs**
4. Guarde y cierre el archivo.

   *No inserte la unidad USB cuando el equipo esté apagado*. Si la unidad ya está insertada cuando el equipo esté apagado, desconéctelo.
5. Encienda la computadora y reproduzca el problema. Durante este paso, inserte la unidad USB en el equipo cuyos registros se recopilarán.
6. Una vez insertada la unidad USB, espere entre 5 y 10 segundos y desconecte la unidad.

   En la carpeta **\CredantSED** se creará un archivo credpbaenv.tgz que contendrá los archivos de registro necesarios.

**Capturar registros al iniciar en la PBA (PBA UEFI)**

1. Cree un archivo denominado **PBAErr.log** en el nivel raíz dela unidad USB.
2. Inserte la unidad USB **antes** de encender el equipo.
3. Extraiga la unidad USB **después** de reproducir el problema que requiere los registros.

El archivo PBAErr.log se actualiza y se graba en tiempo real.

# 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**.

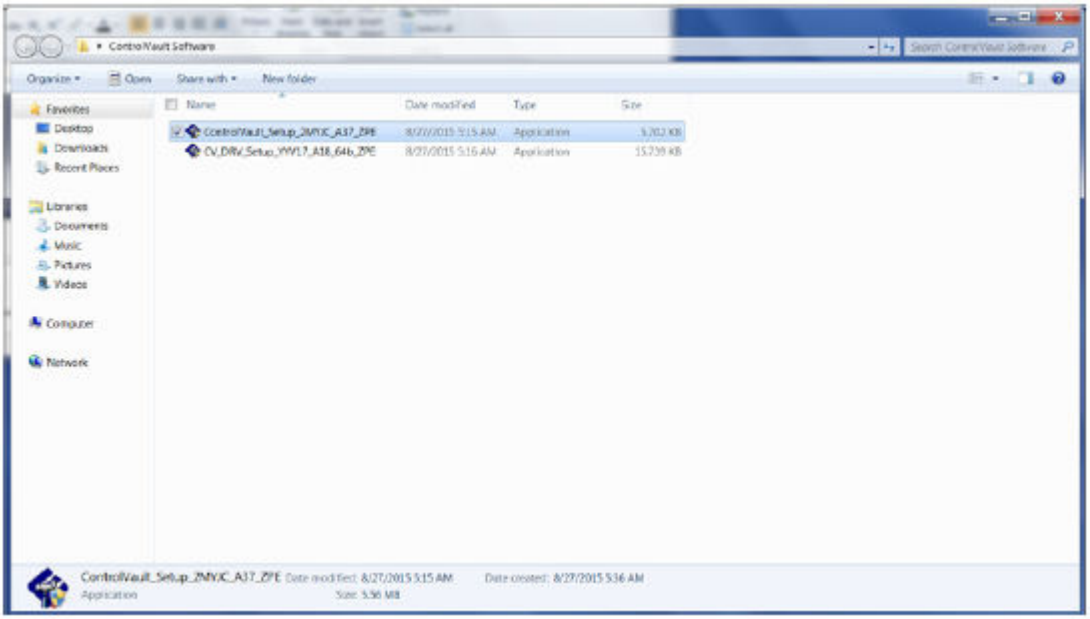
8. Haga doble clic sobre **CVHCI64.MSI** para iniciar el instalador del controlador. [este ejemplo es **CVHCI64.MSI** en este ejemplo (CVHCI para un equipo de 32 bits)].
9. Haga clic en **Siguiente** en la pantalla de bienvenida.
10. Haga clic en **Siguiente** para instalar los controladores en la ubicación 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

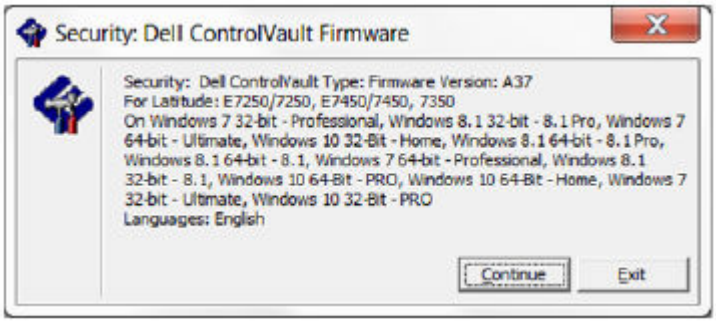
- Device Manager tendrá un dispositivo Dell ControlVault (y otros dispositivos) dependiendo de la configuración del hardware y del sistema operativo.

### Instalación del firmware Dell ControlVault

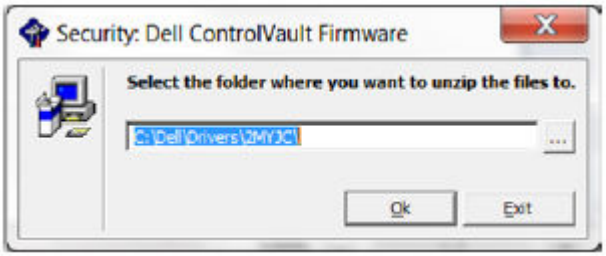
1. Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del firmware.



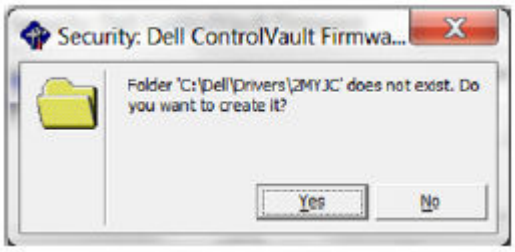
2. Haga doble clic sobre el firmware Dell ControlVault para iniciar el archivo ejecutable autoextraíble.
3. Haga clic en **Continuar** para empezar.



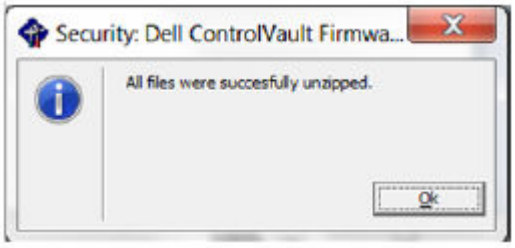

4. Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada de `C:\Dell\Drivers\<New Folder>`.



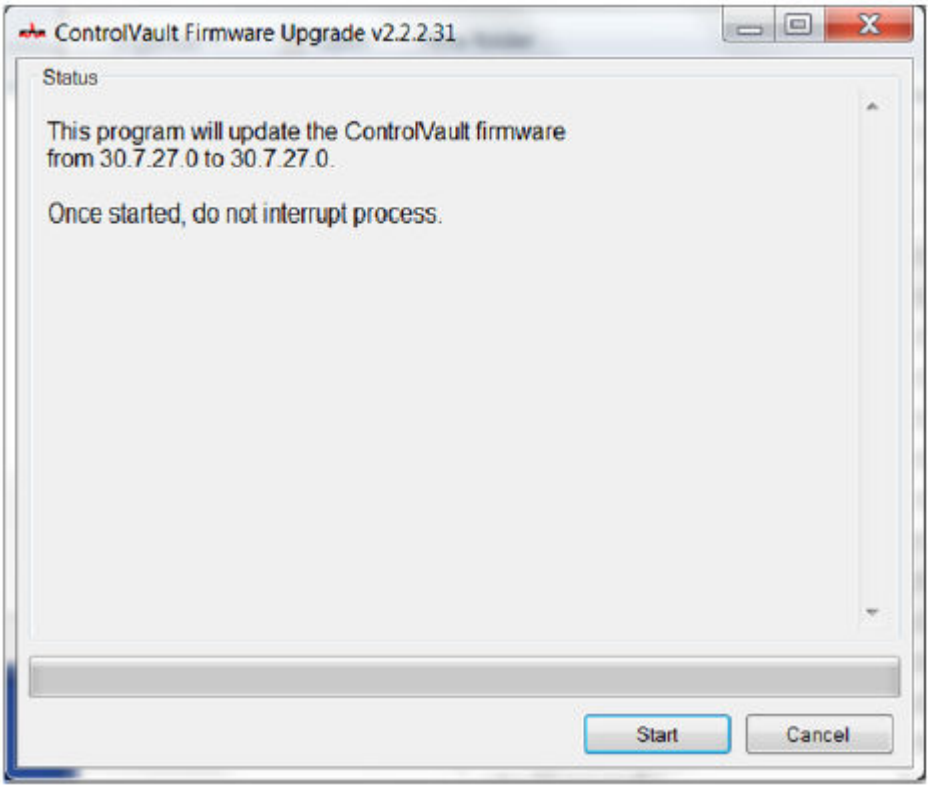

5. Haga clic en **Sí** para permitir la creación de una nueva carpeta.




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.

# Equipos UEFI

## Solución de problemas de conexiones de red

- Para que la autenticación previa al arranque sea correcta en una computadora con firmware UEFI, el modo PBA debe tener conectividad de red. De manera predeterminada, los equipos con firmware UEFI no tienen conectividad de red hasta que se haya cargado el sistema operativo, lo que se produce después del modo PBA. Si el procedimiento de la computadora descrito en Configuración previa a la instalación para computadoras UEFI es correcto y se configura adecuadamente, el ícono de la conexión de red aparecerá en la pantalla de autenticación previa al arranque cuando la computadora esté conectada a la red.

- Compruebe que el cable de red esté conectado a la computadora si el ícono de conexión de red sigue sin aparecer durante la autenticación previa al arranque. Reinicie el equipo para reiniciar el modo PBA si no estaba conectado o estaba suelto.

# TPM y BitLocker

## Códigos de error de TPM y BitLocker

| Constante/Valor | Descripción |
|---|---|
| TPM_E_ERROR_MASK<br>0x80280000 | Se trata de una máscara de error para convertir los errores de hardware de TPM en errores de WIN. |
| TPM_E_AUTHFAIL<br>0x80280001 | Error de autenticación. |
| TPM_E_BADINDEX<br>0x80280002 | El índice a un PCR, DIR u otro registro es incorrecto. |
| TPM_E_BAD_PARAMETER<br>0x80280003 | Uno o más parámetros son erróneos. |
| TPM_E_AUDITFAILURE<br>0x80280004 | Una operación completada correctamente pero ha fallado la auditoría de dicha operación. |
| TPM_E_CLEAR_DISABLED<br>0x80280005 | Se establece el marcador para deshabilitar borrados, por lo que ahora todas las operaciones de borrado requerirán el acceso físico. |
| TPM_E_DEACTIVATED | Activar el TPM. |

| Constante/Valor | Descripción |
|---|---|
| 0x80280006 | |
| TPM_E_DISABLED<br>0x80280007 | Habilitar el TPM. |
| TPM_E_DISABLED_CMD<br>0x80280008 | Se ha deshabilitado el comando de destino. |
| TPM_E_FAIL<br>0x80280009 | Ha fallado la operación. |
| TPM_E_BAD_ORDINAL<br>0x8028000A | El ordinal no se reconoce o no es consistente. |
| TPM_E_INSTALL_DISABLED<br>0x8028000B | La capacidad para instalar un propietario está deshabilitada. |
| TPM_E_INVALID_KEYHANDLE<br>0x8028000C | No puede interpretarse el identificador de claves. |
| TPM_E_KEYNOTFOUND<br>0x8028000D | El identificador de claves apunta a una clave no válida. |
| TPM_E_INAPPROPRIATE_ENC<br>0x8028000E | Combinación de cifrado no aceptable. |
| TPM_E_MIGRATEFAIL<br>0x8028000F | Error al autorizar la migración. |
| TPM_E_INVALID_PCR_INFO<br>0x80280010 | No se puede interpretar la información de PCR. |
| TPM_E_NOSPACE<br>0x80280011 | No hay espacio para cargar la clave. |
| TPM_E_NOSRK<br>0x80280012 | No hay ninguna Clave raíz de almacenamiento (SRK) establecida. |
| TPM_E_NOTSEALED_BLOB<br>0x80280013 | Un blob cifrado no es válido o no fue creado por este TPM. |
| TPM_E_OWNER_SET<br>0x80280014 | El TPM ya tiene un propietario. |
| TPM_E_RESOURCES<br>0x80280015 | El TPM no tiene recursos internos suficientes para realizar la acción solicitada. |
| TPM_E_SHORTRANDOM<br>0x80280016 | Una cadena aleatoria es demasiado corta. |
| TPM_E_SIZE | El TPM no cuenta con el espacio para realizar la operación. |

| Constante/Valor | Descripción |
|---|---|
| 0x80280017 | |
| TPM_E_WRONGPCRVAL<br>0x80280018 | El valor de PCR especificado no coincide con el valor de PRC actual. |
| TPM_E_BAD_PARAM_SIZE<br>0x80280019 | El argumento paramSize para el comando no es correcto |
| TPM_E_SHA_THREAD<br>0x8028001A | No hay ningún subproceso SHA-1 existente. |
| TPM_E_SHA_ERROR<br>0x8028001B | El cálculo no puede continuar por un error en el subproceso SHA-1 existente. |
| TPM_E_FAILEDSELFTEST<br>0x8028001C | El dispositivo de hardware de TPM informó de un error durante la prueba automática interna. Intente reiniciar el equipo para solucionar el problema. Si éste continúa, es posible que deba reemplazar el hardware de TPM o la placa base. |
| TPM_E_AUTH2FAIL<br>0x8028001D | Error al autorizar la segunda clave en una función de 2 claves. |
| TPM_E_BADTAG<br>0x8028001E | El valor de etiqueta enviado para un comando no es válido. |
| TPM_E_IOERROR<br>0x8028001F | Error de E/S al transmitir información al TPM. |
| TPM_E_ENCRYPT_ERROR<br>0x80280020 | El proceso de descifrado tuvo un problema. |
| TPM_E_DECRYPT_ERROR<br>0x80280021 | El proceso de descifrado no se completó. |
| TPM_E_INVALID_AUTHHANDLE<br>0x80280022 | Se usó un identificador no válido. |
| TPM_E_NO_ENDORSEMENT<br>0x80280023 | El TPM no tiene ninguna Clave de aprobación (EK) instalada. |
| TPM_E_INVALID_KEYUSAGE<br>0x80280024 | No se permite el uso de una clave. |
| TPM_E_WRONG_ENTITYTYPE<br>0x80280025 | No se permite el tipo de entidad enviado. |
| TPM_E_INVALID_POSTINIT<br>0x80280026 | El comando se recibió con una secuencia incorrecta, con respecto a TPM_Init y un TPM_Startup subsiguiente. |
| TPM_E_INAPPROPRIATE_SIG<br>0x80280027 | Los datos firmados no pueden incluir información DER adicional. |

| Constante/Valor | Descripción |
|---|---|
| TPM_E_BAD_KEY_PROPERTY<br>0x80280028 | Las propiedades de clave en TPM_KEY_PARMs no son compatibles con este TPM. |
| TPM_E_BAD_MIGRATION<br>0x80280029 | Las propiedades de migración de esta clave no son correctas. |
| TPM_E_BAD_SCHEME<br>0x8028002A | La firma o combinación de cifrado para esta clave no es correcta o no se permite en esta situación. |
| TPM_E_BAD_DATASIZE<br>0x8028002B | El tamaño del parámetro de datos (o blob) no es correcto o no es consistente con la clave especificada. |
| TPM_E_BAD_MODE<br>0x8028002C | Un parámetro de modo no es correcto, como capArea o subCapArea para TPM_GetCapability, phsicalPresence para TPM_PhysicalPresence o migrationType para TPM_CreateMigrationBlob. |
| TPM_E_BAD_PRESENCE<br>0x8028002D | El bit physicalPresence o el bit physicalPresenceLock tiene el valor incorrecto. |
| TPM_E_BAD_VERSION<br>0x8028002E | El TPM no puede realizar esta versión de funcionalidad. |
| TPM_E_NO_WRAP_TRANSPORT<br>0x8028002F | El TPM no permite las sesiones de transporte ajustadas. |
| TPM_E_AUDITFAIL_UNSUCCESSFUL<br>0x80280030 | Error al construir la auditoría de TPM y el comando subyacente también devolvió un código de error. |
| TPM_E_AUDITFAIL_SUCCESSFUL<br>0x80280031 | Error al construir la auditoría de TPM y el comando subyacente devolvió un código correcto. |
| TPM_E_NOTRESETABLE<br>0x80280032 | Se intentó restablecer un registro PCR sin el atributo restablecible. |
| TPM_E_NOTLOCAL<br>0x80280033 | Se intentó restablecer un registro PCR que requiere localidad, pero el modificador de localidad no es parte del transporte de comando. |
| TPM_E_BAD_TYPE<br>0x80280034 | El blob para hacer identidades no se escribió correctamente. |
| TPM_E_INVALID_RESOURCE<br>0x80280035 | Al guardar el contexto, el tipo de recurso identificado no coincide con el recurso real. |
| TPM_E_NOTFIPS<br>0x80280036 | El TPM intenta ejecutar un comando que solo está disponible en modo FIPS. |
| TPM_E_INVALID_FAMILY<br>0x80280037 | El comando intenta usar una Id. de familia no válida. |
| TPM_E_NO_NV_PERMISSION<br>0x80280038 | El permiso para manipular el permiso no volátil no está disponible. |

| Constante/Valor | Descripción |
|---|---|
| TPM_E_REQUIRES_SIGN<br>0x80280039 | La operación requiere un comando firmado. |
| TPM_E_KEY_NOTSUPPORTED<br>0x8028003A | Operación incorrecta para cargar una clave no volátil. |
| TPM_E_AUTH_CONFLICT<br>0x8028003B | El blob NV_LoadKey requiere autorización tanto del propietario como del blob. |
| TPM_E_AREA_LOCKED<br>0x8028003C | El área no volátil está bloqueada y no se puede escribir en ella. |
| TPM_E_BAD_LOCALITY<br>0x8028003D | La localidad no es la correcta para la operación que se intentó. |
| TPM_E_READ_ONLY<br>0x8028003E | El área no volátil solo es de lectura y no se puede escribir en ella. |
| TPM_E_PER_NOWRITE<br>0x8028003F | No hay ninguna protección en el área no volátil de escritura. |
| TPM_E_FAMILYCOUNT<br>0x80280040 | El valor de conteo de familia no coincide. |
| TPM_E_WRITE_LOCKED<br>0x80280041 | Ya se escribió en el área no volátil. |
| TPM_E_BAD_ATTRIBUTES<br>0x80280042 | Conflicto de atributos en el área no volátil. |
| TPM_E_INVALID_STRUCTURE<br>0x80280043 | La etiqueta y versión de estructura no son válidas ni consistentes. |
| TPM_E_KEY_OWNER_CONTROL<br>0x80280044 | La clave está bajo el control del Propietario de TPM, y solo dicho propietario la puede expulsar. |
| TPM_E_BAD_COUNTER<br>0x80280045 | El identificador de contador no es correcto. |
| TPM_E_NOT_FULLWRITE<br>0x80280046 | La escritura no es una escritura completa del área. |
| TPM_E_CONTEXT_GAP<br>0x80280047 | La separación entre los conteos de contexto guardado es demasiado grande. |
| TPM_E_MAXNVWRITES<br>0x80280048 | Se superó el número máximo de escrituras no volátiles permitidas sin un propietario. |
| TPM_E_NOOPERATOR<br>0x80280049 | No se estableció ningún valor de AuthData. |

| Constante/Valor | Descripción |
|---|---|
| TPM_E_RESOURCEMISSING<br>0x8028004A | El recurso al que apunta el contexto no está cargado. |
| TPM_E_DELEGATE_LOCK<br>0x8028004B | La administración de delegación está bloqueada. |
| TPM_E_DELEGATE_FAMILY<br>0x8028004C | Se intentó administrar una familia diferente a la familia delegada. |
| TPM_E_DELEGATE_ADMIN<br>0x8028004D | La administración de la tabla de delegación no está habilitada. |
| TPM_E_TRANSPORT_NOTEXCLUSIVE<br>0x8028004E | Se ejecutó un comando fuera de una sesión exclusiva de transporte. |
| TPM_E_OWNER_CONTROL<br>0x8028004F | Se intentó guardar el contexto de una clave controlada expulsada por el propietario. |
| TPM_E_DAA_RESOURCES<br>0x80280050 | El comando DAA no tiene recursos disponibles para ejecutar el comando. |
| TPM_E_DAA_INPUT_DATA0<br>0x80280051 | Error en la comprobación de consistencia en el parámetro de DAA inputData0. |
| TPM_E_DAA_INPUT_DATA1<br>0x80280052 | Error en la comprobación de consistencia en el parámetro de DAA inputData1. |
| TPM_E_DAA_ISSUER_SETTINGS<br>0x80280053 | Error en la comprobación de consistencia en el parámetro de DAA issuerSettings. |
| TPM_E_DAA_TPM_SETTINGS<br>0x80280054 | Error en la comprobación de consistencia en el parámetro de DAA tpmSpecific. |
| TPM_E_DAA_STAGE<br>0x80280055 | El proceso atómico indicado por el comando DAA enviado no es el esperado. |
| TPM_E_DAA_ISSUER_VALIDITY<br>0x80280056 | La comprobación de validez del emisor ha detectado una incoherencia. |
| TPM_E_DAA_WRONG_W<br>0x80280057 | Error en la comprobación de consistencia en w. |
| TPM_E_BAD_HANDLE<br>0x80280058 | El identificador no es correcto. |
| TPM_E_BAD_DELEGATE<br>0x80280059 | La delegación no es correcta. |
| TPM_E_BADCONTEXT<br>0x8028005A | El blob de contexto no es válido. |

| Constante/Valor | Descripción |
|---|---|
| TPM_E_TOOMANYCONTEXTS<br>0x8028005B | El TPM administra demasiados contextos. |
| TPM_E_MA_TICKET_SIGNATURE<br>0x8028005C | Error al validar la firma de autoridad de migración. |
| TPM_E_MA_DESTINATION<br>0x8028005D | El destino de migración no está autenticado. |
| TPM_E_MA_SOURCE<br>0x8028005E | El origen de migración no es correcto. |
| TPM_E_MA_AUTHORITY<br>0x8028005F | La autoridad de migración no es correcta. |
| TPM_E_PERMANENTEK<br>0x80280061 | Se intentó revocar el EK, pero el EK no es revocable. |
| TPM_E_BAD_SIGNATURE<br>0x80280062 | El vale CMK no tiene una firma correcta. |
| TPM_E_NOCONTEXTSPACE<br>0x80280063 | No hay espacio en la lista de contextos para ningún contexto adicional. |
| TPM_E_COMMAND_BLOCKED<br>0x80280400 | Se bloqueó el comando. |
| TPM_E_INVALID_HANDLE<br>0x80280401 | No se ha encontrado el identificador especificado |
| TPM_E_DUPLICATE_VHANDLE<br>0x80280402 | El TPM devolvió un identificador duplicado, por lo que se deberá volver a enviar el comando. |
| TPM_E_EMBEDDED_COMMAND_BLOCKED<br>0x80280403 | Se bloqueó el comando dentro del transporte. |
| TPM_E_EMBEDDED_COMMAND_UNSUPPORTED<br>0x80280404 | El comando dentro del transporte no es compatible. |
| TPM_E_RETRY<br>0x80280800 | El TPM está demasiado ocupado para responder al comando de inmediato, pero se podrá reenviar el comando más tarde. |
| TPM_E_NEEDS_SELFTEST<br>0x80280801 | No se ha ejecutado SelfTestFull. |
| TPM_E_DOING_SELFTEST<br>0x80280802 | El TPM está actualmente ejecutando una prueba automática completa. |
| TPM_E_DEFEND_LOCK_RUNNING<br>0x80280803 | El TPM se está defendiendo contra ataques de diccionario y está en un periodo de tiempo de espera. |

| Constante/Valor | Descripción |
|---|---|
| TBS_E_INTERNAL_ERROR<br>0x80284001 | Se ha detectado un error de software interno. |
| TBS_E_BAD_PARAMETER<br>0x80284002 | Uno o más parámetros de entrada son erróneos. |
| TBS_E_INVALID_OUTPUT_POINTER<br>0x80284003 | Un puntero de salida especificado es erróneo. |
| TBS_E_INVALID_CONTEXT<br>0x80284004 | El identificador de contexto especificado no hace referencia a ningún contexto válido. |
| TBS_E_INSUFFICIENT_BUFFER<br>0x80284005 | Un búfer de salida especificado es demasiado pequeño. |
| TBS_E_IOERROR<br>0x80284006 | Error al comunicarse con el TPM. |
| TBS_E_INVALID_CONTEXT_PARAM<br>0x80284007 | Uno o más parámetros de contexto son inválidos. |
| TBS_E_SERVICE_NOT_RUNNING<br>0x80284008 | El servicio TBS no está en ejecución y no se puede iniciar. |
| TBS_E_TOO_MANY_TBS_CONTEXTS<br>0x80284009 | No se puede crear un nuevo contexto porque ya hay demasiados contextos abiertos. |
| TBS_E_TOO_MANY_RESOURCES<br>0x8028400A | No se puede crear un nuevo recurso virtual porque ya hay demasiados recursos virtuales abiertos. |
| TBS_E_SERVICE_START_PENDING<br>0x8028400B | El servicio TBS se inició pero todavía no está en ejecución. |
| TBS_E_PPI_NOT_SUPPORTED<br>0x8028400C | La interfaz de presencia física no es compatible. |
| TBS_E_COMMAND_CANCELED<br>0x8028400D | Se ha cancelado el comando. |
| TBS_E_BUFFER_TOO_LARGE<br>0x8028400E | El búfer de salida o de entrada es demasiado grande. |
| TBS_E_TPM_NOT_FOUND<br>0x8028400F | No se puede encontrar en este equipo un dispositivo de seguridad de TPM compatible. |
| TBS_E_SERVICE_DISABLED<br>0x80284010 | Se ha deshabilitado la configuración del servicio TBS. |
| TBS_E_NO_EVENT_LOG<br>0x80284011 | No hay disponible ningún registro de eventos de TCG. |

| Constante/Valor | Descripción |
|---|---|
| TBS_E_ACCESS_DENIED<br>0x80284012 | El autor de la llamada no dispone de los permisos necesarios para realizar la operación solicitada. |
| TBS_E_PROVISIONING_NOT_ALLOWED<br>0x80284013 | Las marcas especificadas no admiten la acción de aprovisionamiento de TPM. Para realizar el aprovisionamiento correctamente, es necesaria una de entre diversas acciones. La acción de la consola de administración del TPM (tpm.msc) para hacer que el TPM esté listo puede ser de ayuda. Si desea obtener más información, consulte la documentación del método WMI Win32_Tpm 'Aprovisionar'. (Entre las acciones que puede que sean necesarias, se incluyen importar el valor de autorización de propietario de TPM al sistema, llamar al método WMI Win32_Tpm para aprovisionar el TPM, especificar TRUE en 'ForceClear_Allowed' o en 'PhysicalPresencePrompts_Allowed' [tal y como indica el valor devuelto en la información adicional] o habilitar el TPM en el sistema BIOS). |
| TBS_E_PPI_FUNCTION_UNSUPPORTED<br>0x80284014 | La interfaz de presencia física de este firmware no admite el método solicitado. |
| TBS_E_OWNERAUTH_NOT_FOUND<br>0x80284015 | No se encontró el valor OwnerAuth de TPM solicitado. |
| TBS_E_PROVISIONING_INCOMPLETE<br>0x80284016 | El aprovisionamiento de TPM no se completó. Si desea obtener más información sobre cómo completarlo, llame al método WMI Win32_Tpm para aprovisionar el TPM ('Aprovisionar') y compruebe la información devuelta. |
| TPMAPI_E_INVALID_STATE<br>0x80290100 | El búfer de comando no está en el estado correcto. |
| TPMAPI_E_NOT_ENOUGH_DATA<br>0x80290101 | El búfer de comando no contiene suficientes datos para atender la solicitud. |
| TPMAPI_E_TOO_MUCH_DATA<br>0x80290102 | Ya no caben más datos en el búfer de comando. |
| TPMAPI_E_INVALID_OUTPUT_POINTER<br>0x80290103 | Al menos un parámetro de salida era NULL o no era válido. |
| TPMAPI_E_INVALID_PARAMETER<br>0x80290104 | Uno o más parámetros de entrada no son válidos. |
| TPMAPI_E_OUT_OF_MEMORY<br>0x80290105 | No hay suficiente memoria para atender la solicitud. |
| TPMAPI_E_BUFFER_TOO_SMALL<br>0x80290106 | El búfer especificado es demasiado pequeño. |
| TPMAPI_E_INTERNAL_ERROR<br>0x80290107 | Se detectó un error interno. |

| Constante/Valor | Descripción |
|---|---|
| TPMAPI_E_ACCESS_DENIED<br>0x80290108 | El autor de la llamada no dispone de los permisos necesarios para realizar la operación solicitada. |
| TPMAPI_E_AUTHORIZATION_FAILED<br>0x80290109 | La información de autorización especificada no es válida. |
| TPMAPI_E_INVALID_CONTEXT_HANDLE<br>0x8029010A | El identificador de contexto especificado no es válido. |
| TPMAPI_E_TBS_COMMUNICATION_ERROR<br>0x8029010B | Error al comunicarse con el TBS. |
| TPMAPI_E_TPM_COMMAND_ERROR<br>0x8029010C | El TPM devolvió un resultado inesperado. |
| TPMAPI_E_MESSAGE_TOO_LARGE<br>0x8029010D | El mensaje es demasiado largo para la combinación de codificación. |
| TPMAPI_E_INVALID_ENCODING<br>0x8029010E | No se reconoce la codificación en el blob. |
| TPMAPI_E_INVALID_KEY_SIZE<br>0x8029010F | El tamaño de clave no es válido. |
| TPMAPI_E_ENCRYPTION_FAILED<br>0x80290110 | Error en la operación de cifrado. |
| TPMAPI_E_INVALID_KEY_PARAMS<br>0x80290111 | La estructura de parámetros de clave no es válida |
| TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB<br>0x80290112 | Los datos proporcionados que se solicitaron no parecen ser un blob válido de autorización de migración. |
| TPMAPI_E_INVALID_PCR_INDEX<br>0x80290113 | El índice PCR especificado no es válido |
| TPMAPI_E_INVALID_DELEGATE_BLOB<br>0x80290114 | Los datos proporcionados no parecen ser un blob válido de delegación |
| TPMAPI_E_INVALID_CONTEXT_PARAMS<br>0x80290115 | Al menos uno de los parámetros de contexto especificados no es válido. |
| TPMAPI_E_INVALID_KEY_BLOB<br>0x80290116 | Los datos proporcionados no parecen ser un blob válido de claves |
| TPMAPI_E_INVALID_PCR_DATA<br>0x80290117 | Los datos PCR especificados no son válidos.. |
| TPMAPI_E_INVALID_OWNER_AUTH<br>0x80290118 | El formato de los datos de autenticación de propietario no es válido. |

| Constante/Valor | Descripción |
|---|---|
| TPMAPI_E_FIPS_RNG_CHECK_FAILED<br>0x80290119 | El número aleatorio generado no aprobó la comprobación RNG de FIPS. |
| TPMAPI_E_EMPTY_TCG_LOG<br>0x8029011A | El registro de eventos de TCG no contiene datos. |
| TPMAPI_E_INVALID_TCG_LOG_ENTRY<br>0x8029011B | Una entrada del registro de eventos de TCG no es válida. |
| TPMAPI_E_TCG_SEPARATOR_ABSENT<br>0x8029011C | No se encontró un separador de TCG. |
| TPMAPI_E_TCG_INVALID_DIGEST_ENTRY<br>0x8029011D | Un valor implícito en una entrada del registro de TCG no coincidía con los datos con hash. |
| TPMAPI_E_POLICY_DENIES_OPERATION<br>0x8029011E | La directiva de TPM actual bloqueó la operación solicitada. Póngase en contacto con el administrador del sistema para solicitar ayuda. |
| TBSIMP_E_BUFFER_TOO_SMALL<br>0x80290200 | El búfer especificado es demasiado pequeño. |
| TBSIMP_E_CLEANUP_FAILED<br>0x80290201 | No se puede limpiar el contexto. |
| TBSIMP_E_INVALID_CONTEXT_HANDLE<br>0x80290202 | El identificador de contexto especificado no es válido. |
| TBSIMP_E_INVALID_CONTEXT_PARAM<br>0x80290203 | Se especificó un parámetro de contexto no válido. |
| TBSIMP_E_TPM_ERROR<br>0x80290204 | Error al comunicarse con el TPM |
| TBSIMP_E_HASH_BAD_KEY<br>0x80290205 | No se encontró ninguna entrada con la clave especificada. |
| TBSIMP_E_DUPLICATE_VHANDLE<br>0x80290206 | El identificador virtual especificado coincide con un identificador virtual ya en uso. |
| TBSIMP_E_INVALID_OUTPUT_POINTER<br>0x80290207 | El puntero a la ubicación de identificador devuelta era NULL o no era válida |
| TBSIMP_E_INVALID_PARAMETER<br>0x80290208 | Uno o más parámetros no son válidos. |
| TBSIMP_E_RPC_INIT_FAILED<br>0x80290209 | No se puede inicializar el subsistema RPC. |
| TBSIMP_E_SCHEDULER_NOT_RUNNING<br>0x8029020A | El programador de TBS no está en ejecución. |

| Constante/Valor | Descripción |
|---|---|
| TBSIMP_E_COMMAND_CANCELED<br>0x8029020B | Se ha cancelado el comando. |
| TBSIMP_E_OUT_OF_MEMORY<br>0x8029020C | No hay suficiente memoria para atender la solicitud |
| TBSIMP_E_LIST_NO_MORE_ITEMS<br>0x8029020D | La lista especificada está vacía, o la iteración ya alcanzó el final de la lista. |
| TBSIMP_E_LIST_NOT_FOUND<br>0x8029020E | El elemento especificado no se encuentra en la lista. |
| TBSIMP_E_NOT_ENOUGH_SPACE<br>0x8029020F | El TPM no tiene suficiente espacio para cargar el recurso solicitado. |
| TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS<br>0x80290210 | Demasiados contextos de TPM en uso. |
| TBSIMP_E_COMMAND_FAILED<br>0x80290211 | Error en el comando TPM. |
| TBSIMP_E_UNKNOWN_ORDINAL<br>0x80290212 | El TBS no reconoce el ordinal especificado. |
| TBSIMP_E_RESOURCE_EXPIRED<br>0x80290213 | El recurso solicitado ya no está disponible. |
| TBSIMP_E_INVALID_RESOURCE<br>0x80290214 | El tipo de recurso no coincide. |
| TBSIMP_E_NOTHING_TO_UNLOAD<br>0x80290215 | No se pueden descargar los recursos. |
| TBSIMP_E_HASH_TABLE_FULL<br>0x80290216 | No se puede agregar ninguna nueva entrada a la tabla de hash. |
| TBSIMP_E_TOO_MANY_TBS_CONTEXTS<br>0x80290217 | No se puede crear un nuevo contexto de TBS porque ya hay demasiados contextos abiertos. |
| TBSIMP_E_TOO_MANY_RESOURCES<br>0x80290218 | No se puede crear un nuevo recurso virtual porque ya hay demasiados recursos virtuales abiertos. |
| TBSIMP_E_PPI_NOT_SUPPORTED<br>0x80290219 | La interfaz de presencia física no es compatible. |
| TBSIMP_E_TPM_INCOMPATIBLE<br>0x8029021A | TBS no es compatible con la versión de TPM en el sistema. |
| TBSIMP_E_NO_EVENT_LOG<br>0x8029021B | No hay disponible ningún registro de eventos de TCG. |

| Constante/Valor | Descripción |
|---|---|
| TPM_E_PPI_ACPI_FAILURE<br>0x80290300 | Se ha detectado un error general al intentar adquirir las respuestas del BIOS a un comando de presencia física. |
| TPM_E_PPI_USER_ABORT<br>0x80290301 | El usuario no puede confirmar la solicitud de operación TPM. |
| TPM_E_PPI_BIOS_FAILURE<br>0x80290302 | Un error de BIOS impidió que la operación TMP solicitada se ejecutara correctamente (p.ej. una solicitud de operación TPM no válida o un error de comunicación de BIOS con el TPM). |
| TPM_E_PPI_NOT_SUPPORTED<br>0x80290303 | El BIOS no es compatible con la interfaz de presencia física. |
| TPM_E_PPI_BLOCKED_IN_BIOS<br>0x80290304 | La configuración de BIOS actual bloqueó el comando de presencia física. El propietario del sistema puede reconfigurar el sistema BIOS para permitir el comando. |
| TPM_E_PCP_ERROR_MASK<br>0x80290400 | Esta es una máscara de error para convertir errores de proveedor de servicios criptográficos de plataforma en errores de WIN. |
| TPM_E_PCP_DEVICE_NOT_READY<br>0x80290401 | El dispositivo criptográfico de la plataforma no está listo actualmente. Necesita estar totalmente aprovisionado para poder funcionar. |
| TPM_E_PCP_INVALID_HANDLE<br>0x80290402 | El identificador proporcionado al proveedor de servicios criptográficos de plataforma no es válido. |
| TPM_E_PCP_INVALID_PARAMETER<br>0x80290403 | Un parámetro proporcionado al proveedor de servicios criptográficos de plataforma no es válido. |
| TPM_E_PCP_FLAG_NOT_SUPPORTED<br>0x80290404 | Una marca proporcionada al proveedor de servicios criptográficos de plataforma no es compatible. |
| TPM_E_PCP_NOT_SUPPORTED<br>0x80290405 | Este proveedor de servicios criptográficos de plataforma no admite la operación solicitada. |
| TPM_E_PCP_BUFFER_TOO_SMALL<br>0x80290406 | El búfer es demasiado pequeño para contener todos los datos. No se ha escrito ninguna información en el búfer. |
| TPM_E_PCP_INTERNAL_ERROR<br>0x80290407 | Error interno inesperado en el proveedor de servicios criptográficos de plataforma. |
| TPM_E_PCP_AUTHENTICATION_FAILED<br>0x80290408 | Error en la autorización para usar un objeto de proveedor. |
| TPM_E_PCP_AUTHENTICATION_IGNORED<br>0x80290409 | El dispositivo criptográfico de plataforma ha pasado por alto la autorización para el objeto de proveedor destinada a mitigar el ataque por diccionario. |
| TPM_E_PCP_POLICY_NOT_FOUND<br>0x8029040A | No se encontró la directiva a la que se hizo referencia. |
| TPM_E_PCP_PROFILE_NOT_FOUND | No se encontró el perfil al que se hizo referencia. |

| Constante/Valor | Descripción |
|---|---|
| 0x8029040B | |
| TPM_E_PCP_VALIDATION_FAILED<br>0x8029040C | La validación no ha sido correcta. |
| PLA_E_DCS_NOT_FOUND<br>0x80300002 | No se encontró el Conjunto de recopiladores de datos. |
| PLA_E_DCS_IN_USE<br>0x803000AA | El Conjunto de recopiladores de datos o alguna de sus dependencias ya está en uso. |
| PLA_E_TOO_MANY_FOLDERS<br>0x80300045 | No se puede iniciar el Conjunto de recopiladores de datos porque ya hay demasiadas carpetas. |
| PLA_E_NO_MIN_DISK<br>0x80300070 | No hay suficiente espacio en disco para iniciar el Conjunto de recopiladores de datos. |
| PLA_E_DCS_ALREADY_EXISTS<br>0x803000B7 | El Conjunto de recopiladores de datos ya existe. |
| PLA_S_PROPERTY_IGNORED<br>0x00300100 | Se omitirá el valor de la propiedad. |
| PLA_E_PROPERTY_CONFLICT<br>0x80300101 | Conflicto con el valor de la propiedad. |
| PLA_E_DCS_SINGLETON_REQUIRED<br>0x80300102 | La configuración actual de este Conjunto de recopiladores de datos requiere que contenga exactamente un recopilador de datos. |
| PLA_E_CREDENTIALS_REQUIRED<br>0x80300103 | Se requiere una cuenta de usuario para confirmar las propiedades del Conjunto de recopiladores de datos actual. |
| PLA_E_DCS_NOT_RUNNING<br>0x80300104 | El Conjunto de recopiladores de datos no está en ejecución. |
| PLA_E_CONFLICT_INCL_EXCL_API<br>0x80300105 | Se detectó un conflicto en la lista de APIs para excluir o incluir. Evite especificar el mismo API en la lista de excluir y en la de incluir. |
| PLA_E_NETWORK_EXE_NOT_VALID<br>0x80300106 | La ruta ejecutable especificada hace referencia a un recurso compartido de red o a una ruta UNC. |
| PLA_E_EXE_ALREADY_CONFIGURED<br>0x80300107 | La ruta ejecutable especificada ya está configurada para el seguimiento de APIs. |
| PLA_E_EXE_PATH_NOT_VALID<br>0x80300108 | La ruta de acceso ejecutable especificada no existe. Compruebe que sea correcta. |
| PLA_E_DC_ALREADY_EXISTS<br>0x80300109 | El recopilador de datos ya existe. |

| Constante/Valor | Descripción |
|---|---|
| PLA_E_DCS_START_WAIT_TIMEOUT<br>0x8030010A | Se agotó el tiempo de espera para notificar el inicio del Conjunto de recopilador de datos. |
| PLA_E_DC_START_WAIT_TIMEOUT<br>0x8030010B | Se agotó el tiempo de espera para que inicie el recopilador de datos. |
| PLA_E_REPORT_WAIT_TIMEOUT<br>0x8030010C | Se agotó el tiempo de espera para que la herramienta de generación de informes finalice. |
| PLA_E_NO_DUPLICATES<br>0x8030010D | No se permiten elementos duplicados. |
| PLA_E_EXE_FULL_PATH_REQUIRED<br>0x8030010E | Al especificar el archivo ejecutable al que desea darle seguimiento, especifique también la ruta completa al archivo ejecutable, no solo el nombre del archivo. |
| PLA_E_INVALID_SESSION_NAME<br>0x8030010F | El nombre de sesión proporcionado no es válido. |
| PLA_E_PLA_CHANNEL_NOT_ENABLED<br>0x80300110 | El canal del registro de eventos Microsoft-Windows-Diagnosis-PLA/Operational debe estar habilitado para realizar esta operación. |
| PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED<br>0x80300111 | El canal del registro de eventos Microsoft-Windows-TaskScheduler debe estar habilitado para realizar esta operación. |
| PLA_E_RULES_MANAGER_FAILED<br>0x80300112 | Error al ejecutar el Administrador de reglas. |
| PLA_E_CABAPI_FAILURE<br>0x80300113 | Error al intentar comprimir o extraer los datos. |
| FVE_E_LOCKED_VOLUME<br>0x80310000 | El Cifrado de unidad BitLocker está bloqueando esta unidad. Debe desbloquear la unidad desde el Panel de control. |
| FVE_E_NOT_ENCRYPTED<br>0x80310001 | La unidad no está cifrada. |
| FVE_E_NO_TPM_BIOS<br>0x80310002 | El BIOS no se comunicó correctamente con el TPM. Póngase en contacto con el fabricante del equipo para obtener instrucciones de actualización del BIOS. |
| FVE_E_NO_MBR_METRIC<br>0x80310003 | El BIOS no se comunicó correctamente con el Registro de arranque maestro (MBR). Póngase en contacto con el fabricante del equipo para obtener instrucciones de actualización del BIOS. |
| FVE_E_NO_BOOTSECTOR_METRIC<br>0x80310004 | Falta una medida de TPM necesaria. Si hay un CD o DVD de arranque en el equipo, quítelo, reinicie el equipo y vuelva a activar BitLocker. Si el problema persiste, asegúrese de que el registro de arranque maestro esté actualizado. |
| FVE_E_NO_BOOTMGR_METRIC<br>0x80310005 | El sector de arranque de esta unidad no es compatible con Cifrado de unidad BitLocker. Use la herramienta Bootrec.exe |

| Constante/Valor | Descripción |
|---|---|
| | del Entorno de recuperación de Windows para actualizar o reparar el administrador de arranque (BOOTMGR). |
| FVE_E_WRONG_BOOTMGR<br>0x80310006 | El administrador de arranque de este sistema operativo no es compatible con Cifrado de unidad BitLocker. Use la herramienta Bootrec.exe del Entorno de recuperación de Windows para actualizar o reparar el administrador de arranque (BOOTMGR). |
| FVE_E_SECURE_KEY_REQUIRED<br>0x80310007 | Se requiere al menos un protector de clave segura para realizar esta operación. |
| FVE_E_NOT_ACTIVATED<br>0x80310008 | Cifrado de unidad BitLocker no está habilitado en esta unidad. Active BitLocker. |
| FVE_E_ACTION_NOT_ALLOWED<br>0x80310009 | Cifrado de unidad BitLocker no puede realizar la acción solicitada. Esta condición se puede presentar cuando dos solicitudes se emiten al mismo tiempo. Espere un momento e intente la operación de nuevo. |
| FVE_E_AD_SCHEMA_NOT_INSTALLED<br>0x8031000A | El bosque de los servicios de dominio de Active Directory no contiene los atributos y clases requeridos para hospedar la información del Cifrado de unidad BitLocker ni del TPM. Póngase en contacto con el administrador del dominio para comprobar que se instalaron todas las extensiones de esquema de Active Directory para BitLocker necesarias. |
| FVE_E_AD_INVALID_DATATYPE<br>0x8031000B | El tipo de datos obtenidos de Active Directory no era el esperado. Puede que la información de recuperación de BitLocker falte o esté dañada. |
| FVE_E_AD_INVALID_DATASIZE<br>0x8031000C | El tamaño de los datos obtenidos de Active Directory no era el esperado. Puede que la información de recuperación de BitLocker falte o esté dañada. |
| FVE_E_AD_NO_VALUES<br>0x8031000D | El atributo leído de Active Directory no contiene ningún valor. Puede que la información de recuperación de BitLocker falte o esté dañada. |
| FVE_E_AD_ATTR_NOT_SET<br>0x8031000E | No se estableció el atributo. Compruebe que inició sesión con una cuenta de dominio que puede escribir información en objetos de Active Directory. |
| FVE_E_AD_GUID_NOT_FOUND<br>0x8031000F | El atributo especificado no se encuentra en Servicios de dominio de Active Directory. Póngase en contacto con el administrador del dominio para comprobar que se instalaron todas las extensiones de esquema de Active Directory para BitLocker necesarias. |
| FVE_E_BAD_INFORMATION<br>0x80310010 | Los metadatos de BitLocker de la unidad cifrada no son válidos. Puede intentar reparar la unidad para restaurar el acceso. |
| FVE_E_TOO_SMALL<br>0x80310011 | La unidad no se puede cifrar porque no tiene espacio disponible suficiente. Elimine los datos innecesarios de la unidad para crear espacio disponible adicional e inténtelo de nuevo. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_SYSTEM_VOLUME<br>0x80310012 | La unidad no se puede cifrar porque contiene información de arranque del sistema. Cree una partición distinta para usarla como unidad del sistema que contenga la información de arranque y una segunda partición para usarla como unidad del sistema operativo y, a continuación, cifre la unidad del sistema operativo. |
| FVE_E_FAILED_WRONG_FS<br>0x80310013 | La unidad no se puede cifrar porque no se admite el sistema de archivos. |
| FVE_E_BAD_PARTITION_SIZE<br>0x80310014 | El tamaño del sistema de archivos es mayor que el tamaño de partición en la tabla de particiones. Puede que esta unidad esté dañada o que se haya alterado. Para usar la partición con BitLocker, debe volver a formatearla. |
| FVE_E_NOT_SUPPORTED<br>0x80310015 | Esta unidad no se puede cifrar. |
| FVE_E_BAD_DATA<br>0x80310016 | Los datos no son válidos. |
| FVE_E_VOLUME_NOT_BOUND<br>0x80310017 | La unidad de datos especificada no está establecida para desbloquearse automáticamente en el equipo actual y no se puede desbloquear automáticamente. |
| FVE_E_TPM_NOT_OWNED<br>0x80310018 | Debe inicializar el TPM para poder utilizar Cifrado de unidad deBitLocker. |
| FVE_E_NOT_DATA_VOLUME<br>0x80310019 | La operación que se intentó no se puede realizar en una unidad del sistema operativo. |
| FVE_E_AD_INSUFFICIENT_BUFFER<br>0x8031001A | El búfer proporcionado para una función no fue suficiente para contener los datos devueltos. Aumente el tamaño del búfer antes de ejecutar la función de nuevo. |
| FVE_E_CONV_READ<br>0x8031001B | Error en una operación de lectura al convertir la unidad. No se convirtió la unidad. Vuelva a habilitar BitLocker. |
| FVE_E_CONV_WRITE<br>0x8031001C | Error en una operación de escritura al convertir la unidad. No se convirtió la unidad. No se convirtió la unidad. Vuelva a habilitar BitLocker. |
| FVE_E_KEY_REQUIRED<br>0x8031001D | Se requiere al menos un protector de clave de BitLocker. No se puede eliminar la última clave de esta unidad. |
| FVE_E_CLUSTERING_NOT_SUPPORTED<br>0x8031001E | Cifrado de unidad BitLocker no admite configuraciones en clúster. |
| FVE_E_VOLUME_BOUND_ALREADY<br>0x8031001F | La unidad especificada ya está configurada para desbloquearse automáticamente en el equipo actual. |
| FVE_E_OS_NOT_PROTECTED<br>0x80310020 | Cifrado de unidad BitLocker no protege a la unidad del sistema operativo. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_PROTECTION_DISABLED<br>0x80310021 | Se ha suspendido el cifrado de unidad BitLocker en esta unidad. Todos los protectores de clave de BitLocker configurados en la unidad se deshabilitaron y la unidad se desbloqueará automáticamente con una clave sin cifrado. |
| FVE_E_RECOVERY_KEY_REQUIRED<br>0x80310022 | La unidad que intenta bloquear no tiene ningún protector de clave disponible para el cifrado porque la protección de BitLocker está suspendida actualmente. Vuelva a habilitar BitLocker para bloquear esta unidad. |
| FVE_E_FOREIGN_VOLUME<br>0x80310023 | BitLocker no puede usar el TPM para proteger una unidad de datos. La protección de TPM solo se puede usar con la unidad del sistema operativo. |
| FVE_E_OVERLAPPED_UPDATE<br>0x80310024 | No se pueden actualizar los metadatos de BitLocker para la unidad cifrada porque otro proceso los bloqueó para actualizarlos. Intente este proceso de nuevo. |
| FVE_E_TPM_SRK_AUTH_NOT_ZERO<br>0x80310025 | Los datos de autorización de la clave raíz de almacenamiento (SRK) del Módulo de plataforma segura (TPM) no son cero y por tanto no son compatibles con BitLocker. Inicialice el TPM antes de intentar usarlo con BitLocker. |
| FVE_E_FAILED_SECTOR_SIZE<br>0x80310026 | El algoritmo de cifrado de unidad no se puede usar en este tamaño de sector. |
| FVE_E_FAILED_AUTHENTICATION<br>0x80310027 | La unidad no se puede desbloquear con la clave proporcionada. Confirme que proporcionó la clave correcta e inténtelo de nuevo. |
| FVE_E_NOT_OS_VOLUME<br>0x80310028 | La unidad especificada no es la unidad del sistema operativo. |
| FVE_E_AUTOUNLOCK_ENABLED<br>0x80310029 | No se puede desactivar Cifrado de unidad BitLocker en la unidad del sistema operativo hasta que la característica de desbloqueo automático se haya deshabilitado para las unidades de datos fijas y extraíbles asociadas con este equipo. |
| FVE_E_WRONG_BOOTSECTOR<br>0x8031002A | El sector de arranque de la partición del sistema no realiza medidas del Módulo de plataforma segura (TPM). Use la herramienta Bootrec.exe del Entorno de recuperación de Windows para actualizar o reparar el sector de arranque. |
| FVE_E_WRONG_SYSTEM_FS<br>0x8031002B | Las unidades del sistema operativo de Cifrado de unidad BitLocker deben estar formateadas con el sistema de archivos NTFS para poder cifrarse. Convierta la unidad a NTFS y después active BitLocker. |
| FVE_E_POLICY_PASSWORD_REQUIRED<br>0x8031002C | La configuración de la directiva de grupo requiere que se especifique una contraseña de recuperación antes de cifrar la unidad. |
| FVE_E_CANNOT_SET_FVEK_ENCRYPTED<br>0x8031002D | El algoritmo y la clave de cifrado de unidad no se pueden establecer en una unidad cifrada con anterioridad. Para cifrar esta unidad con Cifrado de unidad BitLocker, quite el cifrado anterior y después active BitLocker. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_CANNOT_ENCRYPT_NO_KEY<br>0x8031002E | Cifrado de unidad BitLocker no puede cifrar la unidad especificada porque no hay una clave de cifrado disponible. Agregue un protector de clave para cifrar la unidad. |
| FVE_E_BOOTABLE_CDDVD<br>0x80310030 | Cifrado de unidad BitLocker detectó un medio de arranque (CD o DVD) en el equipo. Quite el medio y reinicie el equipo antes de configurar BitLocker. Quite el medio y reinicie el equipo antes de configurar BitLocker. |
| FVE_E_PROTECTOR_EXISTS<br>0x80310031 | No se puede agregar un protector de clave. Solo se permite un protector de clave de este tipo para la unidad. |
| FVE_E_RELATIVE_PATH<br>0x80310032 | No se encontró el archivo de la contraseña de recuperación porque se especificó una ruta de acceso relativa. Las contraseñas de recuperación deben guardarse en una ruta de acceso completa. Las variables de entorno configuradas en el equipo pueden usarse en la ruta de acceso. |
| FVE_E_PROTECTOR_NOT_FOUND<br>0x80310033 | El protector de clave especificado no se encontró en la unidad. Intente usar otro protector de clave. |
| FVE_E_INVALID_KEY_FORMAT<br>0x80310034 | La clave de recuperación proporcionada está dañada y no se puede usar para obtener acceso a la unidad. Debe usarse un método de recuperación alternativo, como una contraseña de recuperación, un agente de recuperación de datos o una versión de copia de seguridad de la clave de recuperación para recuperar el acceso a la unidad. |
| FVE_E_INVALID_PASSWORD_FORMAT<br>0x80310035 | El formato de la contraseña de recuperación proporcionada no es válido. Las contraseñas de recuperación de BitLocker deben tener 48 dígitos. Compruebe que la contraseña de recuperación tiene el formato correcto e inténtelo de nuevo. |
| FVE_E_FIPS_RNG_CHECK_FAILED<br>0x80310036 | Error en la prueba de comprobación del generador de números aleatorios. |
| FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD<br>0x80310037 | La configuración de directiva de grupo que requiere la compatibilidad con FIPS impide la generación o el uso de una contraseña de recuperación local por parte de Cifrado de unidad BitLocker. En el modo compatible con FIPS, las opciones de recuperación de BitLocker pueden ser una clave de recuperación almacenada en una unidad USB o la recuperación mediante un agente de recuperación de datos. |
| FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT<br>0x80310038 | La configuración de directiva de grupo que requiere la compatibilidad con FIPS impide guardar la contraseña de recuperación en Active Directory. En el modo compatible con FIPS, las opciones de recuperación de BitLocker pueden ser una clave de recuperación almacenada en una unidad USB o la recuperación mediante un agente de recuperación de datos. Compruebe la configuración de la directiva de grupo. |
| FVE_E_NOT_DECRYPTED<br>0x80310039 | La unidad debe estar totalmente descifrada para poder completar esta operación. |
| FVE_E_INVALID_PROTECTOR_TYPE<br>0x8031003A | El protector de clave especificado no se puede usar para esta operación. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_NO_PROTECTORS_TO_TEST<br>0x8031003B | No hay ningún protector de clave en la unidad para poder realizar la prueba de hardware. |
| FVE_E_KEYFILE_NOT_FOUND<br>0x8031003C | No se encuentra la clave de inicio o la contraseña de recuperación de BitLocker en el dispositivo USB. Compruebe que tiene el dispositivo USB correcto y que el dispositivo USB está conectado al equipo en un puerto USB activo, reinicie el equipo e inténtelo de nuevo. Si el problema persiste, póngase en contacto con el fabricante del equipo para obtener instrucciones de actualización del BIOS. |
| FVE_E_KEYFILE_INVALID<br>0x8031003D | La clave de inicio o el archivo de contraseña de recuperación de BitLocker están dañados o no son válidos. Compruebe que dispone de la clave de inicio o el archivo de contraseña de recuperación correctos e inténtelo de nuevo. |
| FVE_E_KEYFILE_NO_VMK<br>0x8031003E | La clave de cifrado de BitLocker no se puede obtener de la clave de inicio ni de la contraseña de recuperación. Compruebe que dispone de la clave de inicio o la contraseña de recuperación correctas e inténtelo de nuevo. |
| FVE_E_TPM_DISABLED<br>0x8031003F | El TPM está deshabilitado. El TPM debe estar habilitado, inicializado y tener la propiedad válida para poder usarse con Cifrado de unidad BitLocker. |
| FVE_E_NOT_ALLOWED_IN_SAFE_MODE<br>0x80310040 | La configuración de BitLocker de la unidad especificada no se puede administrar porque este equipo funciona en modo seguro. Mientras el equipo funcione en modo seguro, Cifrado de unidad BitLocker sólo se podrá usar con fines de recuperación. |
| FVE_E_TPM_INVALID_PCR<br>0x80310041 | El Módulo de plataforma segura (TPM) no pudo desbloquear la unidad porque se cambió la información de arranque del sistema o no se proporcionó un PIN correcto. Compruebe que no se haya alterado la unidad y que los cambios en la información de arranque del sistema hayan sido realizados por un origen de confianza. Después de comprobar que el acceso a la unidad es seguro, use la consola de recuperación de BitLocker para desbloquear la unidad y después suspenda y reanude BitLocker para actualizar la información de arranque del sistema que BitLocker asocia a esta unidad. |
| FVE_E_TPM_NO_VMK<br>0x80310042 | No se puede obtener la clave de cifrado de BitLocker a partir del Módulo de plataforma segura (TPM). |
| FVE_E_PIN_INVALID<br>0x80310043 | No se puede obtener la clave de cifrado de BitLocker a partir del MTP y PIN. |
| FVE_E_AUTH_INVALID_APPLICATION<br>0x80310044 | Se modificó una aplicación de arranque después de haberse habilitado Cifrado de unidad BitLocker. |
| FVE_E_AUTH_INVALID_CONFIG<br>0x80310045 | La configuración de los datos de la configuración de arranque (BCD) se modificó después de haberse habilitado Cifrado de unidad BitLocker. |
| FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED<br>0x80310046 | La configuración de directiva de grupo que requiere la compatibilidad con FIPS prohíbe el uso de claves sin cifrado, lo cual impide suspender BitLocker en esta unidad. Póngase |

| Constante/Valor | Descripción |
| --- | --- |
| | en contacto con el administrador del dominio para obtener más información. |
| FVE_E_FS_NOT_EXTENDED<br>0x80310047 | Cifrado de unidad BitLocker no puede cifrar esta unidad porque el sistema de archivos no se extiende hasta el final de la unidad. Vuelva a crear particiones de esta unidad e inténtelo de nuevo. |
| FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED<br>0x80310048 | No se puede habilitar Cifrado de unidad BitLocker en la unidad del sistema operativo. Póngase en contacto con el fabricante del equipo para obtener instrucciones de actualización del BIOS. |
| FVE_E_NO_LICENSE<br>0x80310049 | Esta versión de Windows no incluye Cifrado de unidad BitLocker. Para usar Cifrado de unidad BitLocker, actualice el sistema operativo. |
| FVE_E_NOT_ON_STACK<br>0x8031004A | No se puede usar Cifrado de unidad BitLocker porque faltan archivos del sistema imprescindibles para BitLocker o están dañados. Use Reparación de inicio de Windows para restaurar estos archivos en el equipo. |
| FVE_E_FS_MOUNTED<br>0x8031004B | La unidad no se puede bloquear mientras se está usando. |
| FVE_E_TOKEN_NOT_IMPERSONATED<br>0x8031004C | El token de acceso asociado con el subproceso actual no es un token suplantado. |
| FVE_E_DRY_RUN_FAILED<br>0x8031004D | No se puede obtener la clave de cifrado de BitLocker. Compruebe que el Módulo de plataforma segura (TPM) esté habilitado y que se haya tomado posesión. Si el equipo no tiene ningún TPM, compruebe que la unidad USB esté insertada y disponible. |
| FVE_E_REBOOT_REQUIRED<br>0x8031004E | Debe reiniciar el equipo antes de continuar con Cifrado de unidad BitLocker. |
| FVE_E_DEBUGGER_ENABLED<br>0x8031004F | No se puede cifrar la unidad mientras la depuración de arranque está activada. Use la herramienta de línea de comandos bcdedit para desactivar la depuración de arranque. |
| FVE_E_RAW_ACCESS<br>0x80310050 | No se realizó ninguna acción ya que el Cifrado de unidad BitLocker está en modo de acceso sin procesar. |
| FVE_E_RAW_BLOCKED<br>0x80310051 | Cifrado de unidad BitLocker no puede ponerse en modo de acceso sin procesar para esta unidad porque la unidad se está usando. |
| FVE_E_BCD_APPLICATIONS_PATH_INCORRECT<br>0x80310052 | La ruta de acceso especificada en los Datos de configuración de arranque (BCD) para una aplicación con integridad protegida del Cifrado de unidad BitLocker no es correcta. Compruebe y ajuste la configuración de BCD e inténtelo de nuevo. |
| FVE_E_NOT_ALLOWED_IN_VERSION<br>0x80310053 | Cifrado de unidad BitLocker se puede usar solo en aprovisionamientos limitados o para la recuperación cuando |

| Constante/Valor | Descripción |
|---|---|
| | el equipo se ejecuta en entornos de preinstalación o recuperación. |
| FVE_E_NO_AUTOUNLOCK_MASTER_KEY<br>0x80310054 | La clave maestra de desbloqueo automático no estaba disponible en la unidad del sistema operativo. |
| FVE_E_MOR_FAILED<br>0x80310055 | El firmware del sistema no pudo habilitar el borrado de la memoria del sistema al reiniciar el equipo. |
| FVE_E_HIDDEN_VOLUME<br>0x80310056 | No se puede cifrar la unidad oculta. |
| FVE_E_TRANSIENT_STATE<br>0x80310057 | Se omitieron las claves de cifrado de BitLocker porque la unidad se encontraba en un estado transitorio. |
| FVE_E_PUBKEY_NOT_ALLOWED<br>0x80310058 | No se permiten protectores basados en claves públicas en esta unidad. |
| FVE_E_VOLUME_HANDLE_OPEN<br>0x80310059 | Cifrado de unidad BitLocker ya está realizando una operación en esta unidad. Complete todas las operaciones antes de continuar. |
| FVE_E_NO_FEATURE_LICENSE<br>0x8031005A | Esta versión de Windows no admite esta característica de Cifrado de unidad BitLocker. Para usar esta característica, actualice el sistema operativo. |
| FVE_E_INVALID_STARTUP_OPTIONS<br>0x8031005B | La configuración de la directiva de grupo para las opciones de inicio de BitLocker tiene conflictos y no se puede aplicar. Póngase en contacto con el administrador del sistema para obtener más información. |
| FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED<br>0x8031005C | La configuración de la directiva de grupo no permite la creación de una contraseña de recuperación. |
| FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED<br>0x8031005D | La configuración de la directiva de grupo requiere la creación de una contraseña de recuperación. |
| FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED<br>0x8031005E | La configuración de la directiva de grupo no permite la creación de una clave de recuperación. |
| FVE_E_POLICY_RECOVERY_KEY_REQUIRED<br>0x8031005F | La configuración de la directiva de grupo requiere la creación de una clave de recuperación. |
| FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED<br>0x80310060 | La configuración de la directiva de grupo no permite el uso de un PIN durante el inicio. Elija otra opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_PIN_REQUIRED<br>0x80310061 | La configuración de la directiva de grupo requiere el uso de un PIN durante el inicio. Elija esta opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED<br>0x80310062 | La configuración de la directiva de grupo no permite el uso de una clave de inicio. Elija otra opción de inicio de BitLocker. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_POLICY_STARTUP_KEY_REQUIRED<br>0x80310063 | La configuración de la directiva de grupo requiere el uso de una clave de inicio. Elija esta opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064 | La configuración de la directiva de grupo no permite el uso de una clave de inicio y PIN. Elija otra opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED<br>0x80310065 | La configuración de la directiva de grupo requiere el uso de una clave de inicio y PIN. Elija esta opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED<br>0x80310066 | La directiva de grupo no permite el uso solo de TPM durante el inicio. Elija otra opción de inicio de BitLocker. |
| FVE_E_POLICY_STARTUP_TPM_REQUIRED<br>0x80310067 | La configuración de la directiva de grupo requiere el uso solo de TPM durante el inicio. Elija esta opción de inicio de BitLocker. |
| FVE_E_POLICY_INVALID_PIN_LENGTH<br>0x80310068 | El PIN proporcionado no cumple los requisitos de longitud mínima o máxima. |
| FVE_E_KEY_PROTECTOR_NOT_SUPPORTED<br>0x80310069 | El protector de clave no es compatible con la versión de Cifrado de unidad BitLocker actualmente en la unidad. Actualice la unidad para agregar el protector de clave. |
| FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED<br>0x8031006A | La configuración de la directiva de grupo no permite la creación de una contraseña. |
| FVE_E_POLICY_PASSPHRASE_REQUIRED<br>0x8031006B | La configuración de la directiva de grupo requiere la creación de una contraseña. |
| FVE_E_FIPS_PREVENTS_PASSPHRASE<br>0x8031006C | La configuración de directiva de grupo que requiere la compatibilidad con FIPS impidió que la contraseña de recuperación generara o usara. Póngase en contacto con el administrador del dominio para obtener más información. |
| FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED<br>0x8031006D | No se puede agregar una contraseña a la unidad del sistema operativo. |
| FVE_E_INVALID_BITLOCKER_OID<br>0x8031006E | Parece que el identificador de objeto (OID) de BitLocker en la unidad no es válido o está dañado. Use manage-BDE para restablecer el OID en esta unidad. |
| FVE_E_VOLUME_TOO_SMALL<br>0x8031006F | La unidad es demasiado pequeña para protegerse con Cifrado de unidad BitLocker. |
| FVE_E_DV_NOT_SUPPORTED_ON_FS<br>0x80310070 | El tipo de unidad de detección seleccionado es incompatible con el sistema de archivos de la unidad. Las unidades de detección de BitLocker To Go deben crearse en unidades con formato FAT. |
| FVE_E_DV_NOT_ALLOWED_BY_GP<br>0x80310071 | La configuración de la directiva de grupo del equipo no permite el tipo de unidad de detección seleccionado. Compruebe que la configuración de la directiva de grupo permite la creación de unidades de detección para usarlas con BitLocker To Go. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED<br>0x80310072 | La configuración de la directiva de grupo no permite el uso de certificados de usuario, por ejemplo, tarjetas inteligentes, con Cifrado de unidad BitLocker. |
| FVE_E_POLICY_USER_CERTIFICATE_REQUIRED<br>0x80310073 | La configuración de la directiva de grupo requiere el uso de un certificado de usuario válido, como una tarjeta inteligente, con Cifrado de unidad BitLocker. |
| FVE_E_POLICY_USER_CERT_MUST_BE_HW<br>0x80310074 | La configuración de la directiva de grupo requiere el uso de un protector de clave basado en tarjeta inteligente con Cifrado de unidad BitLocker. |
| FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED<br>0x80310075 | La configuración de la directiva de grupo no permite el desbloqueo automático de unidades de datos fijas protegidas con BitLocker. |
| FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED<br>0x80310076 | La configuración de la directiva de grupo no permite el desbloqueo automático de unidades de datos extraíbles protegidas con BitLocker. |
| FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED<br>0x80310077 | La configuración de la directiva de grupo no permite configurar Cifrado de unidad BitLocker en unidades de datos extraíbles. |
| FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED<br>0x80310078 | La configuración de la directiva de grupo no permite activar Cifrado de unidad BitLocker en unidades de datos extraíbles. Póngase en contacto con el administrador del sistema si necesita activar BitLocker. |
| FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED<br>0x80310079 | La configuración de la directiva de grupo no permite apagar Cifrado de unidad BitLocker en unidades de datos extraíbles. Póngase en contacto con el administrador del sistema si necesita desactivar BitLocker. |
| FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH<br>0x80310080 | La contraseña no cumple los requisitos de longitud mínima de contraseñas. De forma predeterminada, las contraseñas deben tener una longitud mínima de 8 caracteres. Consulte al administrador del sistema cuál es el requisito de longitud de contraseñas de la organización. |
| FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE<br>0x80310081 | La contraseña no cumple los requisitos de complejidad establecidos por el administrador del sistema. Intente agregar caracteres en mayúsculas y minúsculas, números y símbolos. |
| FVE_E_RECOVERY_PARTITION<br>0x80310082 | No se puede cifrar esta unidad porque está reservada para Opciones de recuperación del sistema de Windows. |
| FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON<br>0x80310083 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos. BitLocker no se puede configurar para desbloquear automáticamente unidades de datos fijas cuando las opciones de recuperación de usuario están deshabilitadas. Si desea que las unidades de datos fijas protegidas con BitLocker se desbloqueen automáticamente después de la validación de claves, pida al administrador del sistema que resuelva el conflicto de configuración antes de habilitar BitLocker. |

| Constante/Valor | Descripción |
| --- | --- |
| FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON<br>0x80310084 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos. BitLocker no se puede configurar para desbloquear automáticamente unidades de datos extraíbles cuando la opción de recuperación de usuario está deshabilitada. Si desea que las unidades de datos extraíbles protegidas con BitLocker se desbloqueen automáticamente después de la validación de claves, pida al administrador del sistema que resuelva el conflicto de configuración antes de habilitar BitLocker. |
| FVE_E_NON_BITLOCKER_OID<br>0x80310085 | El atributo EKU (uso mejorado de clave) del certificado especificado no permite usarlo para el Cifrado de unidad BitLocker. BitLocker no requiere que un certificado tenga el atributo EKU, pero si hay uno configurado, se debe establecer en un identificador de objeto (OID) que coincida con el OID configurado para BitLocker. |
| FVE_E_POLICY_PROHIBITS_SELFSIGNED<br>0x80310086 | Cifrado de unidad BitLocker no se puede aplicar a esta unidad tal como está configurado a causa de la configuración de la directiva de grupo. El certificado que proporcionó para el cifrado de la unidad está autofirmado. La configuración actual de la directiva de grupo no permite el uso de certificados autofirmados. Obtenga un nuevo certificado de la entidad de certificación antes de intentar habilitar BitLocker. |
| FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED<br>0x80310087 | No se puede aplicar Cifrado de BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos. Cuando se deniega el acceso de escritura a unidades no protegidas con BitLocker, el uso de una clave de inicio USB no puede ser obligatorio. Pida al administrador del sistema que resuelva estos conflictos de directiva antes de intentar habilitar BitLocker. |
| FVE_E_CONV_RECOVERY_FAILED<br>0x80310088 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos en cuanto a las opciones de recuperación en unidades del sistema operativo. El almacenamiento de información de recuperación en Servicios de dominio de Active Directory no puede ser obligatorio cuando la generación de contraseñas de recuperación no se permite. Pida al administrador del sistema que resuelva estos conflictos de directiva antes de intentar habilitar BitLocker. |
| FVE_E_VIRTUALIZED_SPACE_TOO_BIG<br>0x80310089 | La virtualización solicitada es demasiado grande. |
| FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON<br>0x80310090 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos en cuanto a las opciones de recuperación en unidades del sistema operativo. El almacenamiento de información de recuperación en Servicios de dominio de Active Directory no puede ser obligatorio cuando la generación de contraseñas de recuperación no se permite. Pida al administrador del sistema que resuelva estos conflictos de directiva antes de intentar habilitar BitLocker. |
| FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON<br>0x80310091 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo |

| Constante/Valor | Descripción |
| --- | --- |
| | tiene conflictos en cuanto a las opciones de recuperación en unidades de datos fijas. El almacenamiento de información de recuperación en Servicios de dominio de Active Directory no puede ser obligatorio cuando la generación de contraseñas de recuperación no se permite. Pida al administrador del sistema que resuelva estos conflictos de directiva antes de intentar habilitar BitLocker. |
| FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON<br>0x80310092 | No se puede aplicar Cifrado de unidad BitLocker a esta unidad porque la configuración de la directiva de grupo tiene conflictos en cuanto a las opciones de recuperación en unidades de datos extraíbles. El almacenamiento de información de recuperación en Servicios de dominio de Active Directory no puede ser obligatorio cuando la generación de contraseñas de recuperación no se permite. Pida al administrador del sistema que resuelva estos conflictos de directiva antes de intentar habilitar BitLocker. |
| FVE_E_NON_BITLOCKER_KU<br>0x80310093 | El atributo Key Usage (KU) del certificado especificado no permite usarlo para el Cifrado de unidad BitLocker. BitLocker no necesita que un certificado tenga un atributo KU, pero si hay uno configurado, debe establecerse para cifrado de clave o para acuerdo de claves. |
| FVE_E_PRIVATEKEY_AUTH_FAILED<br>0x80310094 | No se puede autorizar la clave privada asociada al certificado especificado. No se proporcionó la autorización de la clave privada o, si se hizo, no era válida. |
| FVE_E_REMOVAL_OF_DRA_FAILED<br>0x80310095 | La eliminación del certificado del agente de recuperación de datos debe realizarse con el complemento Certificados. |
| FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME<br>0x80310096 | Esta unidad se cifró con la versión de Cifrado de unidad BitLocker incluida en Windows Vista y Windows Server 2008, que no admite identificadores de organización. Para especificar identificadores de organización para esta unidad, actualice el cifrado de la unidad a la versión más reciente con el comando "manage-bde -upgrade". |
| FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME<br>0x80310097 | La unidad no se puede bloquear porque está desbloqueada automáticamente en este equipo. Quite el protector de desbloqueo automático para bloquear esta unidad. |
| FVE_E_FIPS_HASH_KDF_NOT_ALLOWED<br>0x80310098 | Su tarjeta inteligente no admite la función de derivación de claves de BitLocker SP800-56A para tarjetas inteligentes ECC predeterminada. La configuración de la directiva de grupo que requiere compatibilidad con FIPS impide que BitLocker use ninguna otra función de derivación de claves para el cifrado. Debe usar una tarjeta inteligente compatible con FIPS en entornos restringidos para FIPS. |
| FVE_E_ENH_PIN_INVALID<br>0x80310099 | No se puede obtener la clave de cifrado de BitLocker a partir del TPM y el PIN mejorado. Intente usar un PIN qué solo contenga números. |
| FVE_E_INVALID_PIN_CHARS<br>0x8031009A | El PIN de TPM solicitado contiene caracteres no válidos. |
| FVE_E_INVALID_DATUM_TYPE<br>0x8031009B | La información de administración almacenada en la unidad contenía un tipo desconocido. Si usa una versión anterior |

| Constante/Valor | Descripción |
|---|---|
| | de Windows, intente obtener acceso a la unidad desde la versión más reciente. |
| FVE_E_EFI_ONLY<br>0x8031009C | La característica solo se admite en sistemas EFI. |
| FVE_E_MULTIPLE_NKP_CERTS<br>0x8031009D | Se encontró más de un certificado de protector de clave de red en el sistema. |
| FVE_E_REMOVAL_OF_NKP_FAILED<br>0x8031009E | La eliminación del certificado de protector de clave de red debe realizarse mediante el complemento Certificados. |
| FVE_E_INVALID_NKP_CERT<br>0x8031009F | Se encontró un certificado no válido en el almacén de certificados de protector de clave de red. |
| FVE_E_NO_EXISTING_PIN<br>0x803100A0 | Esta unidad no está protegida con un PIN. |
| FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH<br>0x803100A1 | Escriba el PIN actual correcto. |
| FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100A2 | Debe iniciar sesión con una cuenta de administrador para cambiar el PIN o la contraseña. Haga clic en el enlace para restablecer el PIN o la contraseña como administrador. |
| FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED<br>0x803100A3 | BitLocker ha deshabilitado los cambios de PIN después de demasiadas solicitudes con error. Haga clic en el enlace para restablecer el PIN o la contraseña como administrador. |
| FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII<br>0x803100A4 | El administrador del sistema requiere que las contraseñas contengan únicamente caracteres ASCII imprimibles. Esto incluye letras no acentuadas (A-Z, a-z), números (0-9), espacios, símbolos aritméticos, puntuación común, separadores y los siguientes símbolos: # $ & @ ^ _ ~ . |
| FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A5 | El Cifrado de unidad BitLocker únicamente admite el cifrado solo en espacio utilizado en el almacenamiento con aprovisionamiento fino. |
| FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A6 | El Cifrado de unidad BitLocker no admite la eliminación de espacio disponible en el almacenamiento con aprovisionamiento fino. |
| FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE<br>0x803100A7 | La unidad no admite la longitud de la de clave de autenticación requerida. |
| FVE_E_NO_EXISTING_PASSPHRASE<br>0x803100A8 | Esta unidad no está protegida con una contraseña. |
| FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH<br>0x803100A9 | Escriba la contraseña actual correcta. |
| FVE_E_PASSPHRASE_TOO_LONG | La contraseña no puede superar los 256 caracteres. |

| Constante/Valor | Descripción |
|---|---|
| 0x803100AA | |
| FVE_E_NO_PASSPHRASE_WITH_TPM<br>0x803100AB | No se puede agregar un protector de clave de contraseña porque hay un protector de TPM en la unidad. |
| FVE_E_NO_TPM_WITH_PASSPHRASE<br>0x803100AC | No se puede agregar un protector de clave de TPM porque hay un protector de contraseña en la unidad. |
| FVE_E_NOT_ALLOWED_ON_CSV_STACK<br>0x803100AD | Este comando solo se puede ejecutar desde el nodo del coordinador del volumen CSV especificado. |
| FVE_E_NOT_ALLOWED_ON_CLUSTER<br>0x803100AE | Este comando no se puede ejecutar en un volumen si forma parte de un clúster. |
| FVE_E_EDRIVE_NO_FAILOVER_TO_SW<br>0x803100AF | BitLocker no revirtió al uso de cifrado de software de BitLocker debido a la configuración de directiva de grupo. |
| FVE_E_EDRIVE_BAND_IN_USE<br>0x803100B0 | BitLocker no puede administrar la unidad porque la característica de cifrado de hardware de la unidad ya está en uso. |
| FVE_E_EDRIVE_DISALLOWED_BY_GP<br>0x803100B1 | La configuración de la directiva de grupo no permite el uso de cifrado basado en hardware. |
| FVE_E_EDRIVE_INCOMPATIBLE_VOLUME<br>0x803100B2 | La unidad especificada no admite el uso de cifrado basado en hardware. |
| FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING<br>0x803100B3 | BitLocker no se puede actualizar durante el cifrado o descifrado del disco. |
| FVE_E_EDRIVE_DV_NOT_SUPPORTED<br>0x803100B4 | Los volúmenes de detección no se admiten en volúmenes que usan cifrado de hardware. |
| FVE_E_NO_PREBOOT_KEYBOARD_DETECTED<br>0x803100B5 | No se detectó ningún teclado previo al arranque. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen. |
| FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED<br>0x803100B6 | No se detectó teclado previo al arranque o ambiente de recuperación de Windows. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen. |
| FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE<br>0x803100B7 | La configuración de la política de grupo requiere la creación de un PIN de inicio, pero no hay ningún teclado previo al arranque disponible en este dispositivo. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen. |
| FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE<br>0x803100B8 | La configuración de la política de grupo requiere la creación de una contraseña de recuperación, pero no hay ni teclado previo al arranque ni ambiente de recuperación de Windows disponibles en este dispositivo. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_WIPE_CANCEL_NOT_APPLICABLE<br>0x803100B9 | Actualmente no se está eliminando el espacio disponible. |
| FVE_E_SECUREBOOT_DISABLED<br>0x803100BA | BitLocker no puede usar el arranque seguro para la integridad de la plataforma porque el arranque seguro se ha deshabilitado. |
| FVE_E_SECUREBOOT_CONFIGURATION_INVALID<br>0x803100BB | BitLocker no puede usar el arranque seguro para la integridad de la plataforma porque la configuración del arranque seguro no satisface los requisitos para BitLocker. |
| FVE_E_EDRIVE_DRY_RUN_FAILED<br>0x803100BC | Su equipo no admite el cifrado basado en hardware de BitLocker. Póngase en contacto con el fabricante del equipo para averiguar si hay actualizaciones de firmware. |
| FVE_E_SHADOW_COPY_PRESENT<br>0x803100BD | BitLocker no se puede habilitar en el volumen porque contiene una instantánea de volumen. Quite todas las instantáneas de volumen antes de cifrar el volumen. |
| FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS<br>0x803100BE | Cifrado de unidad BitLocker no se puede aplicar a esta unidad porque la configuración de la directiva de grupo relativa a los datos de la configuración de arranque mejorados contiene datos no válidos. Acuda al administrador del sistema para que arregle esta configuración no válida antes de intentar habilitar BitLocker. |
| FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE<br>0x803100BF | El firmware del equipo no puede admitir el cifrado de hardware. |
| FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED<br>0x803100C0 | BitLocker ha deshabilitado los cambios de contraseña después de demasiadas solicitudes con error. Haga clic en el enlace para restablecer la contraseña como administrador |
| FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100C1 | Debe iniciar sesión con una cuenta de administrador para cambiar la contraseña. Haga clic en el enlace para restablecer la contraseña como administrador |
| FVE_E_LIVEID_ACCOUNT_SUSPENDED<br>0x803100C2 | BitLocker no puede guardar la contraseña de recuperación porque la cuenta Microsoft especificada está suspendida. |
| FVE_E_LIVEID_ACCOUNT_BLOCKED<br>0x803100C3 | BitLocker no puede guardar la contraseña de recuperación porque la cuenta Microsoft especificada está bloqueada. |
| FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES<br>0x803100C4 | Este equipo no está aprovisionado para admitir el cifrado del dispositivo. Habilite BitLocker en todos los volúmenes para cumplir con la directiva de cifrado del dispositivo. |
| FVE_E_DE_FIXED_DATA_NOT_SUPPORTED<br>0x803100C5 | Este equipo no puede admitir el cifrado del dispositivo porque hay volúmenes de datos fijos sin cifrar. |
| FVE_E_DE_HARDWARE_NOT_COMPLIANT<br>0x803100C6 | Este equipo no cumple con los requisitos de hardware necesarios para admitir el cifrado del dispositivo. |
| FVE_E_DE_WINRE_NOT_CONFIGURED<br>0x803100C7 | Este equipo no puede admitir el cifrado del dispositivo porque WinRE no está configurado correctamente. |

| Constante/Valor | Descripción |
|---|---|
| FVE_E_DE_PROTECTION_SUSPENDED<br>0x803100C8 | La protección está habilitada en el volumen, pero se ha suspendido. Probablemente se deba a que se está aplicando una actualización en el sistema. Inténtelo de nuevo después de reiniciar. |
| FVE_E_DE_OS_VOLUME_NOT_PROTECTED<br>0x803100C9 | Este equipo no está aprovisionado para admitir el cifrado del dispositivo. |
| FVE_E_DE_DEVICE_LOCKEDOUT<br>0x803100CA | Se ha desencadenado el bloqueo del dispositivo debido a demasiados intentos de contraseña incorrectos. |
| FVE_E_DE_PROTECTION_NOT_YET_ENABLED<br>0x803100CB | No se habilitó la protección en el volumen. Para habilitarla, una cuenta debe estar conectada. Si ya hay una cuenta conectada y aparece este error, vea el registro de eventos para obtener más información. |
| FVE_E_INVALID_PIN_CHARS_DETAILED<br>0x803100CC | El PIN solo puede incluir números del 0 al 9. |
| FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE<br>0x803100CD | BitLocker no puede usar la protección de reproducción de hardware porque no hay contadores disponibles en su PC. |
| FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH<br>0x803100CE | Error de validación de estado de bloqueo de dispositivo debido a contadores no coincidentes. |
| FVE_E_BUFFER_TOO_LARGE<br>0x803100CF | El búfer de entrada es demasiado grande. |

# 19

# Glosario

Activar: la activación se produce cuando la computadora se registró en el Dell Server y recibió al menos un conjunto de políticas inicial.

Active Directory (AD): es un servicio de directorios creado por Microsoft para las redes de dominio de Windows.

Codificación de datos de aplicaciones: el cifrado de datos de aplicaciones cifra cualquier archivo escrito con una aplicación protegida, utilizando una invalidación de la categoría 2. Esto implica que cualquier directorio que tenga una protección de Categoría 2 o superior, o cualquier ubicación que tenga extensiones específicas protegidas con Categoría 2 o superior, provocará que ADE no cifre esos archivos.

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

Credenciales en memoria caché: las credenciales en memoria caché son aquellas que se agregan a la base de datos de PBA cuando el usuario se autentica correctamente en Active Directory. Esta información sobre el usuario se conserva para que este pueda iniciar sesión cuando no existe la conexión con Active Directory (por ejemplo, cuando utiliza el equipo portátil en su casa).

Cifrado común: la clave Común permite que todos los usuarios administrados del dispositivo tengan acceso a los archivos cifrados que fueron creados en dicho dispositivo.

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

Encryption External Media este servicio incluido en Encryption protege los medios extraíbles y los dispositivos de almacenamiento externo.

Código de acceso de Encryption External Media: este servicio permite la recuperación de dispositivos protegidos de Encryption External Media cuando el usuario olvida su contraseña y ya no puede iniciar sesión. La finalización de este proceso permite al usuario restablecer la contraseña configurada en el soporte.

Encryption: componente en el dispositivo que aplica políticas de seguridad, ya sea que un terminal esté conectado a la red, desconectado de la red, se haya perdido o lo hayan robado. Con la creación de un ambiente informático de confianza para terminales, 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.

Terminal: según el contexto, una computadora, un dispositivo móvil o medios externos.

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

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

Clave de máquina: cuando el cifrado está instalado en un servidor, la clave de máquina protege las claves de políticas y el cifrado de archivos de un servidor. La clave de máquina se guarda en Dell Server. El nuevo servidor intercambia certificados con Dell Server durante la activación y utiliza el certificado para posteriores eventos de autenticación.

Autenticación previa al arranque (PBA): la autenticación previa al arranque sirve como extensión del BIOS o del firmware de arranque y garantiza un entorno a prueba de alteración seguro, externo al sistema operativo como una capa de autenticación confiable. 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.

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

Usuario del servidor: una cuenta de usuario virtual creada por Encryption con el propósito de administrar las claves de cifrado y las actualizaciones de políticas en un sistema operativo de servidor. Esta cuenta de usuario no se corresponde con ninguna otra cuenta de usuario en la computadora o el dominio, y no cuenta con un nombre de usuario ni con una contraseña que puedan utilizarse físicamente. A la cuenta se le asigna un valor de UCID exclusivo en la consola de administración.

System Data Encryption (SDE): el SDE está diseñado para cifrar el sistema operativo y los archivos de programa. Para cumplir con este propósito, SDE debe poder abrir su clave mientras se inicia el sistema operativo. La finalidad de este requisito es evitar que el sistema operativo quede expuesto a alteraciones o ataques perpetrados por piratas informáticos. SDE no está desarrollado para proteger datos de usuario. Los procesos de cifrado común y de usuario están pensados para proteger información de usuarios que se considera confidencial, ya que exigen una contraseña de usuario para efectuar el desbloqueo de las claves de cifrado. Las políticas de SDE no cifran los archivos que necesita el sistema operativo para el proceso de inicio. Las políticas de SDE no requieren de autenticación previa al 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 los directorios cifrados de SDE de los usuarios correspondientes, sin tener en cuenta otros valores de políticas de SDE, como las reglas de cifrado de SDE.

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

Cifrado de usuarios: la clave de Usuario determina que solo los usuarios que crearon los archivos tengan acceso a ellos, y solo en el dispositivo en el que fueron creados. Cuando se ejecuta Dell Data Encryption, el cifrado de usuario se convierte en cifrado común. Existe una excepción para dispositivos de medios extraíbles; cuando se insertan en un servidor con Encryption instalado, los archivos se cifran con la clave de Usuario en roaming.