Encryption

Requisitos del sistema v10.1

Notas, precauciónes y advertencias

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

PRECAUCIÓN: Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

ADVERTENCIA: Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

2018 - 11

Rev. A01

Contenido

1

Introducción

En este documento se especifican los requisitos de Dell Encryption.

Para tener acceso a la documentación de Dell Encryption, consulte www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

Cómo ponerse en contacto con Dell ProSupport

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.

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 puede ser designado temporalmente mediante una herramienta de implementación como Microsoft SMS o Dell KACE. No son compatibles los usuarios con privilegios elevados que no sean administradores.
- Realice copia de seguridad de todos los datos importantes antes de iniciar la instalación/desinstalación.
- Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Asegúrese de que el puerto exterior 443 esté disponible para comunicarse con el Servidor de administración de seguridad/Servidor virtual de administración de seguridad si los clientes del instalador maestro tienen autorización para utilizar Dell Digital Delivery (DDD). La funcionalidad de autorización no funcionará si el puerto 443 (por algún motivo) está bloqueado. DDD no se utiliza si se realiza la instalación con instaladores secundarios.
- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.

Todos los clientes: Requisitos previos

- Se requiere Microsoft .Net Framework 4.5.2 (o posterior) para los clientes de instalador maestro e instalador secundario de . El instalador *no* instala el componente de Microsoft .Net Framework.

  Todos los equipos enviados desde la fábrica de Dell vienen con la versión completa de Microsoft .Net Framework 4.5.2 (o posterior) previamente instalada. Sin embargo, si no está instalando en hardware de Dell o si está actualizando el cliente en hardware de Dell más antiguo, deberá comprobar qué versión de Microsoft .Net tiene instalada y actualizar la versión **antes de instalar el cliente**, con el fin de evitar errores durante la instalación/actualización. Para comprobar qué versión de Microsoft .Net tiene instalada, siga estas instrucciones en el equipo en el que se va a realizar la instalación: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar Microsoft .Net Framework 4.5.2, vaya a https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Los controladores y el firmware para ControlVault, las lectoras de huellas digitales y las tarjetas inteligentes (como se muestra a continuación) no se incluyen en los archivos ejecutables de instaladores secundarios ni del 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

Todos los clientes: Hardware

- La siguiente tabla indica el hardware del equipo compatible.

Hardware

- Procesador Intel Pentium o AMD
- 110 MB de espacio disponible en el disco
- 512 MB de RAM

NOTA: Se necesita espacio libre adicional en el disco para cifrar los archivos en el extremo. Este tamaño varía según las políticas y el tamaño de la unidad.

Todos los clientes: localización

- Los clientes Encryption y BitLocker Manager son compatibles con la Interfaz de usuario multilingüe (MUI) y están localizados en los idiomas siguientes.

Compatibilidad de idiomas

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

Cliente Encryption

- El equipo cliente debe tener conectividad de red para activarse.
- 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.
- Desactive el modo de suspensión durante el barrido de cifrado inicial para evitar que un equipo que no se esté utilizando entre en suspensión. El cifrado se interrumpirá si el equipo entra en modo de suspensión (tampoco podrá realizar el descifrado).
- El cliente Encryption no es compatible con las configuraciones de inicio dual, dado que es posible cifrar archivos de sistema del otro sistema operativo, que podrían interferir con esta operación.
- El instalador maestro no es compatible con las actualizaciones de los componentes anteriores a v8.0. Extraiga los instaladores secundarios del instalador maestro y actualice los componentes individualmente.
- El cliente Encryption ahora es compatible con el modo de auditoría. El modo de auditoría permite a los administradores implementar el cliente Encryption como parte de la imagen corporativa, en lugar de utilizar un SCCM de terceros o soluciones similares para implementar el cliente Encryption. Para obtener instrucciones acerca de la forma de instalar el cliente de Cifrado en una imagen corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.
- El cliente Encryption se ha probado y es compatible con McAfee, el cliente de Symantec, Kaspersky y Malwarebytes. Se aplican exclusiones no modificables para estos proveedores de antivirus con el fin de evitar incompatibilidades entre la detección del antivirus y el cifrado. El cliente Encryption también se ha probado con el kit de herramientas Microsoft Enhanced Mitigation Experience Toolkit.

  Si su empresa utiliza un proveedor antivirus que no se encuentra incluido, consulte http://www.dell.com/support/article/us/en/19/SLN288353 o comuníquese con Dell ProSupport para obtener asistencia.
- El TPM se utiliza para sellar la GPK. Por lo tanto, si ejecuta el cliente Encryption, borre el TPM en el BIOS antes de instalar un sistema operativo nuevo en el equipo cliente.
- La actualización en el lugar del sistema operativo no es compatible con la instalación del cliente Encryption. Desinstale y descifre el cliente Encryption, actualice al nuevo sistema operativo y, a continuación, vuelva a instalar el cliente Encryption.

  De manera adicional, no se admite la reinstalación del sistema operativo. Para volver a instalar el sistema operativo, realice una copia de seguridad del equipo de destino, borre el equipo, instale el sistema operativo y, a continuación, recupere los datos cifrados siguiendo los procedimientos de recuperación establecidos.

Requisitos previos del cliente Encryption

- El instalador maestro instala Microsoft Visual C++ 2012 actualización 4 si todavía no está instalado en el equipo. **Cuando utiliza el instalador secundario**, debe instalar este componente antes de instalar el cliente Encryption.

Requisito previo
– Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 y x64)
– Paquete redistribuible Visual C++ 2015 actualización 3 o posterior (x86 y x64)

Hardware del cliente Encryption

- La siguiente tabla indica el hardware compatible.

Hardware integrado opcional
– TPM 1.2 o 2.0

Sistemas operativos del cliente Encryption

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows Embedded Standard 7 con plantilla de compatibilidad de aplicaciones (no admite cifrado de hardware)
– Windows 8: Enterprise, Pro
– Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
– Windows Embedded 8.1 Industry Enterprise (no admite cifrado de hardware)
– Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)
– VMware Workstation 12.5 y superior

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

Sistemas operativos Medios externos de cifrado

- La siguiente tabla indica los sistemas operativos compatibles con el acceso a medios protegidos por Medios externos de cifrado.

NOTA:
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 Medios externos de cifrado.

Sistemas operativos Windows compatibles para el acceso a medios protegidos de Medios externos de cifrado (32 y 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows 8: Enterprise, Pro, Consumer

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

- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)

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

- macOS Sierra 10.12.4 y 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Cliente Server Encryption

Server Encryption está diseñado para que se utilice en equipos que funcionan en modo servidor, particularmente en servidores de archivos.

- Server Encryption solo es compatible con Encryption Enterprise y Endpoint Security Suite Enterprise.
- Server Encryption ofrece lo siguiente:
  - Cifrado de software
  - Cifrado de medios extraíbles
  - Control de puertos

  NOTA:
  El servidor debe admitir controles de puerto.

  Las políticas de sistema de control de puertos de servidor afectan a medios extraíbles en servidores protegidos, por ejemplo, controlando el acceso y 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.

Server Encryption está para su uso en:

- 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 de varios TB RAID
  - 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 empresa utiliza un proveedor antivirus que no se encuentra incluido, consulte el artículo SLN298707 de la base de conocimiento o póngase en contacto con Dell ProSupport para obtener asistencia.

No compatible

Server Encryption no se puede usar en:

- Servidor de administración de seguridads/Servidor virtual de administración de seguridads o los servidores que ejecutan bases de datos para Servidor de administración de seguridads/Servidor virtual de administración de seguridad.
- Server Encryption no es compatible con Encryption Personal.
- Server Encryption no es compatible con el cliente BitLocker Manager ni con SED Management.

- Server Encryption no es compatible en servidores que forman parte de sistemas de archivos distribuidos (DFS).
- La migración a o desde Server Encryption no es compatible. Las actualizaciones de Medios externos de cifrado a Server Encryption requieren que se desinstale completamente el producto o productos previos antes de la instalación de Server Encryption.
- 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)
  - Unidades SED (RAID y NO RAID)
  - Inicio de sesión automático (Windows 7, 8/8.1) para quioscos
  - Microsoft Storage Server 2012
- Server Encryption no es compatible con las configuraciones de inicio dual, dado que es posible cifrar archivos de sistema del otro sistema operativo, que podrían interferir con esta operación.
- 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* (Guía de recuperación).

Hardware del cliente Server Encryption

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

Sistemas operativos del cliente Server Encryption

La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos (32 y 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/ Redstone 4)

Sistemas operativos de servidor compatibles

- Windows Server 2008 R2 SP1: Standard Edition, Essentials Edition, Foundation Edition y Datacenter Edition
- Windows Server 2012: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)
- Windows Server 2012 R2: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)
- Windows Server 2016: Standard Edition, Essentials Edition y Datacenter Edition (Server Core no es compatible)

Sistemas operativos compatibles con el modo de UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/ Redstone 4)

NOTA:

En un equipo compatible con UEFI, después de seleccionar **Reiniciar** desde 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.

Sistemas operativos Medios externos de cifrado

La siguiente tabla indica los sistemas operativos compatibles con el acceso a medios protegidos por Medios externos de cifrado.

NOTA:

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 Medios externos de cifrado.

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/ Redstone 4)

Sistemas operativos de servidor compatibles

- Windows Server 2012 R2

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

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14