Dell Data Protection | Endpoint Security Suite Enterprise

Guía de instalación avanzada v1.4

Notas, precauciones y avisos

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

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Guía de instalación avanzada de Endpoint Security Suite Enterprise

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción

Esta guía detalla cómo instalar y configurar Advanced Threat Prevention, el cliente Encryption, el cliente SED Management, Advanced Authentication y BitLocker Manager.

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

Antes de empezar

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

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

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

2 Aprovisionamiento de un inquilino para Advanced Threat Prevention. Debe aprovisionar un inquilino en DDP Server antes de que se active la aplicación de las políticas de Advanced Threat Protection.

3 Lea detenidamente el capítulo Requisitos de este documento.

4 Implemente los clientes en los usuarios finales.

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 Contraseña de un solo uso, SED UEFI y BitLocker.
- Si sus clientes están autorizados para utilizar Dell Digital Delivery (DDD), consulte Configuración de GPO en la controladora de dominio para habilitar derechos.
- Si instala clientes mediante el instalador maestro de ESSE, consulte:
  - Instalación interactiva mediante el instalador maestro de ESSE

    O bien
  - Instalación mediante línea de comandos con el instalador maestro de ESSE
- Si instala clientes mediante los instaladores secundarios, los archivos ejecutables del instalador secundario deberán extraerse del instalador maestro de ESSE . Consulte Extracción de instaladores secundarios del instalador maestro de ESSE y luego regrese aquí.
  - Instale los instaladores secundarios mediante la línea de comandos:
    - Instalación de controladores: descargue los controladores y el firmware correspondientes en función de su hardware de autenticación.
    - Instalación del cliente Encryption: utilice estas instrucciones para instalar el cliente Encryption, que es el componente que aplica la política de seguridad, independientemente de que un equipo esté conectado a la red, esté desconectado de esta, perdido o robado.

- Instalación del cliente de Advanced Threat Prevention: utilice estas instrucciones para instalar el cliente Advanced Threat Prevention, que es la próxima generación en protección antivirus que utiliza ciencia algorítmica y aprendizaje automático para identificar, clasificar y prevenir que se ejecuten amenazas cibernéticas, conocidas o desconocidas, o que estas amenazas causen daños a los extremos.
- Instalación de la Protección web y el Servidor de seguridad: utilice estas instrucciones para instalar las características *opcionales* de Protección web y Servidor de seguridad. El Servidor de seguridad del cliente es un servidor de seguridad con estado que comprueba todo el tráfico entrante y saliente contra su lista de reglas. La Protección web supervisa la exploración de web y las descargas para identificar amenazas y hacer cumplir las acciones definidas en la política cuando se detecta una amenaza, según las clasificaciones de los sitios web.
- Instalación de los clientes SED Management y Advanced Authentication: utilice estas instrucciones para instalar 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 Management, todas las políticas, el almacenamiento y la recuperación de claves de cifrado están disponibles en una única consola, reduciendo el riesgo de que los equipos no estén protegidos en caso de pérdida o acceso no autorizado.

  El cliente Advanced Authentication administra varios métodos de autenticación, incluido PBA para SED, Inicio de sesión único (SSO), y credenciales de usuario como huellas digitales y contraseñas. Además, proporciona capacidades de Advanced Authentication para acceder a sitios web y aplicaciones.
- Instalación del cliente BitLocker Manager: utilice estas instrucciones para instalar el cliente 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 las instalaciones no se describen en esta guía. Sin embargo, el instalador secundario del cliente Advanced Threat Prevention se puede instalar solamente a través de la línea de comandos.

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

Cómo ponerse en contacto con Dell ProSupport

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

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

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

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

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 EE Server/VE Server si los clientes del instalador maestro de ESSE tienen derecho a 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 necesita Microsoft .Net Framework 4.5.2 (o posterior) para los clientes de instalador maestro e instalador secundario de ESSE . 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, los lectores de huellas digitales y las tarjetas inteligentes (como se muestra a continuación) no se incluyen en los archivos ejecutables de instaladores secundarios o en el instalador maestro de ESSE . 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. Las instrucciones de instalación para controladores ControlVault se suministran en Actualización del firmware y de los controladores Dell ControlVault.

Todos los clientes: Hardware

- La siguiente tabla indica el hardware del equipo compatible.

Hardware

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

Todos los clientes: Compatibilidad de idiomas

- Los clientes EncryptionAdvanced Threat Prevention y BitLocker Manager son compatibles con la Interfaz de usuario multilingüe (MUI) y admiten los idiomas siguientes. Los datos de Advanced Threat Prevention aparecen en la Remote Management Console solamente en inglés.

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)

- Los clientes SED y Advanced Authentication son compatibles con la Interfaz de usuario multilingüe (MUI) y admiten los idiomas siguientes. El modo UEFI y la Autenticación previa al inicio (PBA) no están disponibles en ruso, chino tradicional y chino simplificado.

Compatibilidad de idiomas

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

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 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/SLN298707 o póngase en contacto 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 de ESSE instala Microsoft Visual C++ 2012 actualización 4 si todavía no está instalada en el servidor. **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)

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 SP0-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 • VMWare Workstation 5.5 y superior

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

Sistemas operativos para External Media Shield (EMS)

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

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

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

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

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

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

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

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 Enterprise Edition y Endpoint Security Suite Enterprise.
- Server Encryption ofrece lo siguiente:
  - Cifrado de software
  - Cifrado de almacenamiento extraíble
  - 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 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 el equipo 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 ha probado y es compatible con clientes McAfee, VirusScan o Symantec, antivirus Kaspersky y antimalware 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. 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:

- El servidor o servidores de Dell Data Protection que ejecutan bases de datos para Dell Data ProtectionServer
- Server Encryption no es compatible con Endpoint Security Suite, Personal Edition ni Security Tools.
- Server Encryption no es compatible con el cliente BitLocker Manager o SED Management.
- La migración a o desde Server Encryption no es compatible. Las actualizaciones de External Media Edition 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 OS 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.
- La actualización en el lugar del sistema operativo no es compatible con la instalación de Server Encryption. Para actualizar el sistema operativo, desinstale y descifre Server Encryption, actualícelo a una nueva versión y vuelva a instalar Server 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. Para obtener más información acerca de la recuperación de los datos cifrados, consulte la *Recovery Guide (Guía de recuperación)*.

Requisitos previos del cliente Server Encryption

- Debe instalar este componente antes de instalar el cliente Server Encryption.

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

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 SP0-SP1: Home, Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

Sistemas operativos de servidor compatibles

- Windows Server 2008 SP2: Standard Edition, Datacenter Edition con y sin Hyper-V, Enterprise Edition con y sin Hyper-V, Foundation Server Edition
- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition con y sin Hyper-V, Enterprise Edition con y sin Hyper-V, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition

Sistemas operativos compatibles con el modo de UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

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 de External Media Shield (EMS)

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

NOTA:

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

NOTA:

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

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

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

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

- Windows 10: Education, Enterprise, Pro

Sistemas operativos de servidor compatibles

- Windows Server 2008 SP1 o posterior
- Windows Server 2012 R2

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

- OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 y 10.11.5

Cliente Advanced Threat Prevention

- El cliente Advanced Threat Prevention no se puede instalar sin que el cliente Dell Client Security Framework (EMAgent) se haya detectado en el equipo. Si se intenta, fallará la instalación.
- Para completar la instalación de Advanced Threat Prevention cuando Dell Enterprise Server/VE que administra al cliente se está ejecutando en el modo conectado (predeterminado), el ordenador debe tener conexión a la red. Sin embargo, ***no*** se requiere conexión de red para la instalación de Advanced Threat Prevention cuando el servidor Dell administrador funciona en modo desconectado.
- Para aprovisionar un inquilino para Advanced Threat Prevention, el servidor Dell debe tener conexión a Internet.

  NOTA: No se requiere conexión a Internet cuando el servidor Dell está funcionando en modo desconectado.
- Las funciones opcionales Servidor de seguridad del cliente y Protección web ***no*** deben instalarse en ordenadores cliente gestionados por Dell Enterprise Server/VE ejecutándose en el modo desconectado.
- Las aplicaciones de antivirus, antimalware y antispyware de otros proveedores puede entrar en conflicto con el cliente Advanced Threat Prevention. Si es posible, desinstale estas aplicaciones. El software en conflicto no incluye Windows Defender. Se permiten las aplicaciones de servidor de seguridad.

  Si no es posible desinstalar otras aplicaciones de antivirus, antimalware, y antispyware, debe añadir exclusiones para Advanced Threat Protection en el servidor Dell y para el resto de aplicaciones. Para obtener instrucciones sobre cómo agregar exclusiones para Advanced Threat Protection en el servidor Dell, consulte http://www.dell.com/support/article/us/en/04/SLN300970. Para obtener una lista de exclusiones para añadirlas para el resto de aplicaciones de antivirus, consulte http://www.dell.com/support/article/us/en/19/SLN301134.

Sistemas operativos de Advanced Threat Prevention

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Puertos de Advanced Threat Prevention

- Los agentes de Advanced Threat Prevention se administran en y notifican a la plataforma SaaS de la consola de administración. El puerto 443 (https) se utiliza para la comunicación y debe estar abierto en el servidor de seguridad para que los agentes puedan comunicarse con la consola. La consola se aloja en servicios web de Amazon y no tiene ninguna IP fija. Si el puerto 443 está bloqueado por cualquier motivo, no se podrán descargar las actualizaciones, así que puede que los equipos no tengan la protección más reciente. Asegúrese de que los equipos cliente puedan acceder a las direcciones URL siguientes.

Utilizar	Protocolo de aplicación	Protocolo de transporte	Número de puerto	Destino	Dirección
Toda la comunicación	HTTPS	TCP	443	Permitir todo el tráfico https en *.cylance.com	Saliente

Verificación de la integridad de la imagen del BIOS

Si la política *Habilitar la garantía de BIOS* se selecciona en la Remote Management Console, el inquilino Cylance valida un hash del BIOS en sistemas de usuarios finales para asegurarse de que el BIOS no ha sido modificado desde la versión de fábrica de Dell, que es un posible vector de ataque. Si se detecta una amenaza, se pasa una notificación al DDP Server y el administrador de TI recibe un mensaje de alerta en la Remote Management Console. Para obtener una descripción general del proceso, consulte Proceso de verificación de la integridad de la imagen del BIOS.

NOTA: Con esta función, no se puede usar una imagen de fábrica personalizada, ya que BIOS se ha modificado.

Modelos de equipos de Dell compatibles con la verificación de la integridad de la imagen del BIOS

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Estación de trabajo Precision 3510
- Estación de trabajo Precision 5510
- Estación de trabajo Precision 3620
- Estación de trabajo Precision 7510
- Estación de trabajo Precision 7710
- Estación de trabajo Precision T3420
- Venue 10 pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

Cliente SED

- El equipo debe tener conectividad de red con cable para que se instale correctamente SED Management.
- No es compatible con IPv6.
- Recuerde que deberá apagar y reiniciar el equipo después de aplicar las políticas y cuando estén listas para comenzar a aplicarlas.
- Los equipos que cuentan con unidades de cifrado automático no se pueden utilizar con tarjetas HCA. Existen incompatibilidades que impiden el aprovisionamiento del HCA. Dell no vende equipos que tengan unidades de cifrado automático compatibles con el módulo HCA. Esta configuración incompatible será una configuración realizada poscompra.

- Si el equipo marcado para cifrado incluye unidad de cifrado automático, asegúrese de que Active Directory tenga deshabilitada la opción *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*. La Autenticación previa al inicio del sistema no es compatible con esta opción de Active Directory.
- 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.

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

- SED Management no es compatible con Server Encryption o con Advanced Threat Prevention en un SO de servidor.

Controladores OPAL

- Las SED admitidas que cumplen con OPAL necesitan controladores actualizados Intel Rapid Storage Technology, que se pueden encontrar en http://www.dell.com/support.

Requisitos previos del cliente SED

- El instalador maestro de ESSE instala Microsoft Visual C++2010 SP1 **y** Microsoft Visual C++ 2012 actualización 4 si todavía no están instalados en el equipo. **Cuando utilice el instalador secundario**, debe instalar estos componentes antes de instalar SED Management.

Requisitos previos
• Paquete redistribuible Visual C++ 2010 SP1 o posterior (x86 y x64) • Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 y x64)

Hardware del cliente SED

SED que cumplen con OPAL

- Para obtener una lista más reciente de SED compatibles con Opal admitidos con SED Management, consulte este artículo de KB: http://www.dell.com/support/article/us/en/19/SLN296720.

Modelos de equipos Dell compatibles con UEFI

- La siguiente tabla muestra qué modelos de equipos Dell admiten UEFI.

Modelos de equipos Dell - Compatibilidad con UEFI

- Latitude 5280
- Latitude 5480
- Latitude 5580
- Latitude 7370
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M5520
- Optiplex 3040 micro, minitorre, factor de forma pequeña
- Optiplex 3046
- OptiPlex 3050 All-In-One
- Venue Pro 11 (Modelos 5175/5179)
- Venue Pro 11 (Modelo 7139)

Modelos de equipos Dell - Compatibilidad con UEFI

- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7280
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Modelo 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M6800
- Precision M7510
- Precision M7520
- Precision M7710
- Precision M7720
- Precision T3420
- Precision T3620
- Precision T7810
- OptiPlex 3050 torre, factor de forma pequeña, Micro
- Optiplex 5040 minitorre, factor de forma pequeña
- OptiPlex 5050 torre, factor de forma pequeña, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, minitorre, factor de forma pequeña
- OptiPlex 7050 torre, factor de forma pequeña, Micro
- Optiplex 3240 Todo en uno
- OptiPlex 5250 All-In-One
- Optiplex 7440 Todo en uno
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro

NOTA:
Las funciones de autenticación son compatibles con el modo UEFI en estos equipos que ejecutan Windows 8, Windows 8.1 y Windows 10 con SED compatibles con OPAL cualificadas. Otros equipos que ejecutan Windows 7, Windows 8, Windows 8.1 y Windows 10 admiten el modo de inicio heredado.

Teclados internacionales

- En la tabla siguiente se muestran los teclados internacionales compatibles con la Autenticación previa al inicio en equipos UEFI y no UEFI.

Compatibilidad con teclado Internacional: UEFI

- Alemán de Suiza (DE-CH)
- Francés de Suiza (DE-FR)

Compatibilidad con teclado Internacional: Non-UEFI

- Árabe (AR) (con caracteres latinos)
- Alemán de Suiza (DE-CH)
- Francés de Suiza (DE-FR)

Sistemas operativos del cliente SED

- La siguiente tabla detalla los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional (compatibles con el modo de inicio heredado pero no UEFI)

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

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Cliente Advanced Authentication

- Cuando se utiliza Advanced Authentication, los usuarios protegerán el acceso a este equipo por medio de credenciales de autenticación avanzada que son administradas y registradas mediante Security Tools. Security Tools será el administrador principal de sus credenciales de autenticación para el inicio de sesión de Windows, lo que incluye la contraseña de Windows, las huellas digitales y las tarjetas inteligentes. Las credenciales de contraseña de imagen, PIN y huellas digitales registradas con el sistema operativo de Microsoft no se reconocerán en el inicio de sesión de Windows.

  Para seguir utilizando el sistema operativo de Microsoft para administrar credenciales de usuario, no instale Security Tools o desinstálelas.
- La función de Contraseña de un solo uso (OTP) de Security Tools requiere que haya un TPM presente, habilitado y con propietario. OTP no es compatible con TPM 2.0. Para borrar y establecer la propiedad del TPM, consulte https://technet.microsoft.com.
- Una SED no requiere un TPM para proporcionar autenticación avanzada o cifrado.

Hardware de cliente de Advanced Authentication

- La siguiente tabla detalla el hardware de autenticación compatible.

Lectores de tarjetas inteligentes y huellas digitales

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

Tarjetas sin contacto

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

Tarjetas inteligentes

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

  NOTA:
  El cliente ActivIdentity no se carga previamente y debe instalarse por separado.

- Tarjetas CSP
- Tarjetas de acceso común (CAC)
- Tarjetas SIPR Net/Clase B

- La siguiente tabla muestra qué modelos de equipos Dell admiten tarjetas SIPR Net.

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

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

Sistemas operativos del cliente Advanced Authentication

Sistemas operativos Windows

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)

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

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

Sistemas operativos de dispositivos móviles

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

Sistemas operativos Android

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

Sistemas operativos iOS

- iOS 7.x
- iOS 8.x

Sistemas operativos Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Cliente 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.
- El teclado, el mouse y los componentes de vídeo deben estar directamente conectados al equipo. No use un conmutador KVM para administrar los periféricos, ya que el conmutador KVM puede interferir con 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.
- El cliente BitLocker Manager utilizará los algoritmos validados FIPS AES aprobados si el modo FIPS está habilitado para el ajuste 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. No forzamos 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 Server Encryption o Advanced Threat Prevention en un SO de servidor.

Requisitos previos del cliente BitLocker Manager

- El instalador maestro de ESSE instala Microsoft Visual C++2010 SP1 **y** Microsoft Visual C++ 2012 actualización 4 si todavía no están instalados en el equipo. **Cuando utiliza el instalador secundario**, debe instalar estos componentes antes de instalar BitLocker Manager.

Requisitos previos

- Paquete redistribuible Visual C++ 2010 SP1 o posterior (x86 y x64)
- Paquete redistribuible Visual C++ 2012 actualización 4 o posterior (x86 y x64)

Sistemas operativos del cliente BitLocker Manager

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows

- Windows 7 SP0-SP1: Enterprise, Ultimate (32 y 64 bits)
- Windows 8: Enterprise (64 bits)
- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

Opciones de autenticación

- Las siguientes opciones de autenticación precisan un hardware específico:Huellas dactilares, Tarjetas inteligentes, Tarjetas sin contacto, Tarjetas SIPR Net/Clase B y autenticación en equipos UEFI. Las siguientes opciones requieren configuración: tarjetas inteligentes con autenticación de Windows, tarjetas inteligentes con autenticación previa al inicio y contraseña de un solo uso. Las tablas siguientes muestran opciones de autenticación disponibles, por sistema operativo, cuando se cumplan los requisitos de hardware y de configuración.

Cliente Encryption

Sin UEFI

	PBA					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7 SP0-SP1						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]

Sin UEFI

	PBA					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 8.1 actualización 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

UEFI

	PBA - en equipos Dell admitidos					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7 SP0-SP1										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 actualización 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

Cliente SED

Sin UEFI

	PBA					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7 SP0-SP1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8.1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 10	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]

Sin UEFI

	PBA					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

3. Disponible con SED OPAL admitido.

UEFI

	PBA - en equipos Dell admitidos					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7										
Windows 8	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 8.1	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 10	X[4]					X	X[2]	X[2]	X[1]	X[2]

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

4. Disponible con un SED OPAL compatible en equipos UEFI admitidos.

BitLocker Manager

Sin UEFI

	PBA [5]					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

Sin UEFI

	PBA [5]					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

5. El PIN de inicio previo de BitLocker se administra mediante la funcionalidad de Microsoft.

UEFI

	PBA[5]: en equipos Dell admitidos					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

1. Disponible cuando se instala con el instalador maestro o con el paquete de Advanced Authentication si se utilizan instaladores secundarios.

2. Disponible cuando se descargan los controladores de autenticación desde support.dell.com.

5. El PIN de inicio previo de BitLocker se administra mediante la funcionalidad de Microsoft.

3

Configuración de registro

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

Parámetros del registro del cliente Encryption

- Si se utiliza un certificado autofirmado en el servidor Dell para Enterprise Edition para Windows, la validación de confianza de certificado deberá permanecer deshabilitada en el equipo cliente (la validación de confianza está *deshabilitada* de forma predeterminada con Enterprise Edition para Windows). Antes de *habilitar* la validación de confianza en el equipo cliente, deben cumplirse los siguientes requisitos.
  - Un certificado firmado por una autoridad raíz, como por ejemplo EnTrust o Verisign, deberá ser importado a EE Server/VE 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 EE para Windows, cambie el valor de la siguiente entrada de registro a 0 en el equipo cliente.

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

    "IgnoreCertErrors"=dword:00000000

    0 = Falla si se encuentra un error de certificado

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

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

  "MSSmartcardSupport"=dword:1
- 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

- De forma predeterminada, durante la instalación, aparece el icono de la bandeja del sistema. Utilice la siguiente configuración de registro para ocultar el icono de la bandeja del sistema de todos los usuarios administrados en un equipo tras la instalación original. Cree o modifique la configuración de registro tal como se muestra a continuación:

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

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

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

  "SnoozeBeforeSweep"=DWORD:1

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

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

  (CANTIDAD PERMITIDA DE RETRASOS DE LA ACTUALIZACIÓN DE LA POLÍTICA × DURACIÓN DE CADA RETRASO DE ACTUALIZACIÓN DE LA POLÍTICA) + (5 MINUTOS x [CANTIDAD PERMITIDA DE RETRASOS DE LA ACTUALIZACIÓN DE LA POLÍTICA - 1])
- Utilice la siguiente configuración de registro para que el cliente Encryption sondee el EE Server/VE Server en busca de una actualización de política aplicada. Cree o modifique la configuración de registro tal como se muestra a continuación:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  El valor de registro desaparecerá automáticamente cuando finalice.
- Utilice la siguiente configuración de registro para permitir que el cliente Encryption envíe un inventario optimizado al EE Server/VE Server, envíe un inventario completo al EE Server/VE Server, o envíe un inventario completo para todos los usuarios activados al EE Server/VE Server.

  - Enviar el inventario optimizado a EE Server/VE Server:

    Cree o modifique la configuración de registro tal como se muestra a continuación:

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

"OnlySendInvChanges"=REG_DWORD:1

Si no hay ninguna entrada, el inventario optimizado se enviará al EE Server/VE Server.

- Enviar el inventario completo a EE Server/VE Server:

  Cree o modifique la configuración de registro tal como se muestra a continuación:

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

  "OnlySendInvChanges"=REG_DWORD:0

  Si no hay ninguna entrada, el inventario optimizado se enviará al EE Server/VE 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 el equipo se reinicia antes de que tenga lugar la carga del inventario, el cliente 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 a lo largo de un período de tiempo establecido para facilitar la carga de EE Server/VE 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.

  IMPORTANTE:
  Configure la activación ranurada solo con ayuda de Dell ProSupport. Una configuración con ranuras de tiempo incorrectas podría hacer que muchos clientes intenten activarse a EE Server/VE Server a la vez, creando posibles problemas de rendimiento graves.

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

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

    Habilita o deshabilita la activación ranurada

    Deshabilitado=0 (valor predeterminado)

    Habilitado=1

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

    El período de tiempo en segundos en que se produce el intervalo de ranura de activación. Utilice esta configuración para invalidar el período de tiempo 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.

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

    El intervalo dentro de la repetición, ACTIVATION_SLOT_CALREPEAT, cuando se producen todas las ranuras de tiempo de activación. Solo se permite un intervalo. Este valor debería ser 0,<CalRepeat>. Un desplazamiento de 0 podría producir resultados inesperados. El valor predeterminado es 0,86400. Para establecer una repetición de siete horas, utilice el valor 0,25200. CALREPEAT se activa cuando un usuario inicia sesión.

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

El número de ranuras de activación que se pueden perder antes de que el equipo intente activarse en el siguiente inicio de sesión del usuario cuyas activaciones se han ranurado. Si la activación falla durante este intento inmediato, el cliente reanudará los intentos de activación ranurada. Si la activación falla debido a un error de red, la activación se intentará en la próxima reconexión de red, aunque el valor de MISSTHRESHOLD no se haya superado. Si un usuario cierra sesión antes de alcanzar el tiempo de ranura de activación, se asignará una nueva ranura para el próximo inicio de sesión.

- [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 el equipo cliente, establezca el siguiente valor de registro en el equipo 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

- Para habilitar la reactivación automática silenciosa en el caso poco frecuente de que un usuario se desactive, el siguiente valor de registro se debe establecer en el equipo 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 el cliente Encryption está procesando una actualización de la política que incluye una política de SDE activa, se cifra de forma predeterminada el directorio del perfil del usuario actual con la clave SDUser (una clave de usuario), en lugar de hacerlo con la clave SDE (una clave de dispositivo). La clave SDUser también se utiliza para cifrar los archivos o carpetas que se hayan copiado (no trasladado) a un directorio de usuarios que no esté cifrado con SDE.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=dword:00000000

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

  Para obtener más información sobre SDUser, consulte www.dell.com/support/article/us/en/19/SLN304916

- 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

- La función de activación no de dominio se puede habilitar poniéndose en contacto con Dell ProSupport y solicitando instrucciones.

Ajustes del registro del cliente Advanced Threat Prevention

- Para que el complemento Advanced Threat Prevention supervise HKLM\SOFTWARE\Dell\Dell Data Protection para determinar si se han producido cambios en el valor de LogVerbosity, y actualizar el nivel de registro de cliente en consecuencia, defina el siguiente valor.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=dword:<see below>

  Dump: 0

  Fatal: 1

  Error 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  El valor de registro se comprueba cuando se inicia el servicio ATP o cuando el valor cambia. Si el valor de registro no existe, no se producirá ningún cambio a nivel de registro.

  Utilice este ajuste del registro solo para realizar pruebas u operaciones de depuración, ya que este ajuste controla el nivel de detalle de registro de otros componentes, incluido el cliente Encryption y Client Security Framework.

- El Modo de compatibilidad permite que se ejecuten aplicaciones en el equipo cliente mientras que están habilitadas las políticas de Protección de memoria o de Protección de memoria y Control de secuencias de comandos. La activación del modo de compatibilidad requiere la adición de un valor de registro en el equipo cliente.

  Para activar el modo de compatibilidad, siga estos pasos:

  a. En la Remote Management Console, deshabilite la política Protección de memoria habilitada. Si la política de Control de secuencias de comandos está habilitada, deshabilítela.
  b. Agregue el valor de registro CompatibilityMode.
     1. Al utilizar el Editor de registro en el equipo cliente, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
     2. Haga clic con el botón derecho del mouse en **Escritorio**, haga clic en **Permisos**, y asuma la propiedad y otórguese Control completo.
     3. Haga clic con el botón derecho del mouse en **Escritorio** y, a continuación, seleccione **Nuevo** > **Valor binario**.
     4. Para el nombre, escriba `CompatibilityMode`.
     5. Abra la configuración de registro y cambie el valor a `01`.
     6. Haga clic en **Aceptar** y, a continuación, cierre el Editor de registro.

Para agregar el valor de registro con un comando, puede utilizar una de las siguientes opciones de línea de comandos para que se ejecute en el equipo cliente:

- (Para un equipo) Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t
REG_BINARY /d 01
```

- (Para varios equipos) Invoke-Command cmdlet:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -
Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}
```

c En la Remote Management Console, vuelva a habilitar la política Protección de memoria habilitada. Si la política de Control de secuencias de comandos se había habilitado anteriormente, vuelva a habilitarla.

Ajustes del registro del cliente SED

- Para establecer el intervalo de reintentos cuando el EE Server/VE Server no está disponible para comunicarse con el cliente SED, agregue el siguiente valor de registro.

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

  "CommErrorSleepSecs"=dword:300

  Este valor es el número de segundos que el cliente SED espera para intentar ponerse en contacto con el EE Server/VE Server si este no está disponible para comunicarse con el cliente SED. El valor predeterminado es 300 segundos (5 minutos).
- Si se utiliza un certificado autofirmado en el EE Server/VE Server para SED Management, la validación de confianza de SSL/TLS deberá permanecer deshabilitada en el equipo cliente (la validación de confianza de SSL/TLS está *deshabilitada* de forma predeterminada con SED Management). 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, como por ejemplo EnTrust o Verisign, deberá ser importado a EE Server/VE 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 SED Management, cambie el valor de la siguiente entrada de registro a 0 en el equipo cliente.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Habilitado

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

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

  "MSSmartcardSupport"=dword:1
- Para utilizar tarjetas inteligentes con la autenticación previa al inicio, el valor de registro siguiente debe estar establecido en el equipo cliente. Establezca también la política Método de autenticación en Tarjeta inteligente en la Remote Management Console, y confirme el cambio.

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

  "MSSmartcardSupport"=dword:1

- 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 establecer el intervalo con el que el cliente SED intentará ponerse en contacto con EE Server/VE Server cuando el servidor no esté disponible para comunicarse con el cliente SED, establezca el siguiente valor en el equipo cliente:

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

  "CommErrorSleepSecs"=DWORD Value:300

  Este valor es el número de segundos que el cliente SED espera para intentar ponerse en contacto con el EE Server/VE Server si este no está disponible para comunicarse con el cliente SED. 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 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
- 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

Ajustes del registro del cliente Advanced Authentication

- Si **no** desea que el cliente Advanced Authentication (Security Tools) cambie los servicios asociados a las tarjetas inteligentes y los dispositivos biométricos a un tipo de inicio "automático", puede deshabilitar la función de inicio del servicio. La deshabilitación de esta función también suprime los avisos asociados con el mal funcionamiento de los servicios necesarios.

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

  - SCardSvr: administra el acceso a las tarjetas inteligentes leídas por el equipo. Si el servicio se detiene, el equipo no podrá leer tarjetas inteligentes. Si el servicio se deshabilita, no podrán iniciarse los servicios que dependan explícitamente de él.
  - SCPolicySvc: permite que el sistema se configure para bloquear el escritorio del usuario cuando se retire la tarjeta inteligente.
  - WbioSrvc: el servicio biométrico de Windows otorga a las aplicaciones de cliente la capacidad de capturar, comparar, manipular y almacenar datos biométricos sin obtener acceso directo a ningún hardware o muestras biométricos. El servicio está alojado en un proceso SVCHOST privilegiado.

    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 autenticación de Windows, el valor de registro siguiente debe estar establecido en el equipo cliente.

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

  "MSSmartcardSupport"=dword:1

- Para utilizar tarjetas inteligentes con autenticación previa al reinicio SED, el valor de registro siguiente debe estar establecido en el equipo cliente equipado con un SED.

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

  "MSSmartcardSupport"=dword:1

  Establezca la política Método de autenticación en Tarjeta inteligente en la Remote Management Console, y confirme el cambio.

Ajustes el registro del cliente BitLocker Manager

- Si se utiliza un certificado autofirmado en el EE Server/VE Server para BitLocker Manager, la validación de confianza de SSL/TLS deberá permanecer deshabilitada en el equipo 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, como por ejemplo EnTrust o Verisign, deberá ser importado a EE Server/VE 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 el equipo cliente.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Habilitado

    1 = Deshabilitado

Instalación mediante el instalador maestro de ESSE

- 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 de ESSE.
- Los archivos de registro del instalador maestro de ESS se encuentran en **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- Indique a los usuarios que consulten el siguiente documento y los archivos de ayuda para obtener ayuda sobre la aplicación:
  - Consulte la Ayuda de cifrado de Dell para saber cómo usar la función del cliente Encryption. Acceda a la ayuda de **<Dir. instalación>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte la Ayuda de EMS para obtener ayuda sobre las funciones de External Media Shield. Acceda a la ayuda desde **<Dir. instalación>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte la *Ayuda de Endpoint Security Suite Enterprise* para obtener información sobre el uso de estas funciones de Advanced Authentication y Advanced Threat Prevention. Puede acceder a esta ayuda desde **<Dir. instalación>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.
- Los usuarios deben actualizar sus políticas haciendo clic con el botón derecho del mouse en el icono de Dell Data Protection de la bandeja del sistema y seleccionando **Comprobar si existen actualizaciones de políticas** una vez finalizada la instalación.
- El instalador maestro de ESSE instala todo el conjunto de productos. Existen dos métodos para realizar la instalación con el instalador maestro de ESSE. Elija una de las siguientes opciones.
  - Instalación interactiva mediante el instalador maestro de ESSE

  O bien

  - Instalación mediante línea de comandos con el instalador maestro de ESSE

Instalación interactiva mediante el instalador maestro de ESSE

- El instalador maestro de ESSE se puede encontrar:
  - **Desde su cuenta FTP de Dell:** localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip.
- Utilice estas instrucciones para instalar Dell Endpoint Security Suite Enterprise de forma interactiva mediante el instalador maestro de ESSE. Este método se puede usar para instalar el conjunto de productos en un equipo al mismo tiempo.

1. Localice el archivo **DDPSuite.exe** en el medio de instalación de Dell. Cópielo al equipo local.
2. Haga doble clic en **DDPSuite.exe** 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 el campo **Nombre de Enterprise Server**, introduzca el nombre de host completo de EE Server/VE Server que administrará al usuario de destino, como server.organization.com.

   En el campo **URL de Device Server**, introduzca la dirección URL de Device Server (Security Server) con la que se comunicará el cliente.

   El formato es https://server.organization.com:**8443**/xapi**/** (incluida la barra inclinada final).

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 pueden surgir problemas si se instala en otras ubicaciones.

7 Seleccione los componentes que deben instalarse.

Security Framework instala Security Framework y Security Tools subyacentes, el cliente Advanced Authentication que administra varios métodos de autenticación, incluido PBA y credenciales como huellas digitales y contraseñas.

Advanced Authentication instala los archivos y servicios necesarios para Advanced Authentication.

Encryption instala el cliente Encryption, el componente que aplica la política de seguridad, independientemente de que un equipo esté conectado a la red, esté desconectado de esta, perdido o robado.

Threat Protection instala los clientes Threat Protection, que son protección contra malware y antivirus para buscar virus, spyware y programas no deseados, servidor de seguridad de cliente para supervisar la comunicación entre el equipo y los recursos de la red y de Internet, y filtrado web para mostrar evaluaciones de seguridad o bloquear el acceso a sitios web durante la navegación en línea.

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.

Advanced Threat Protection instala el cliente Advanced Threat Prevention, que es la próxima generación en protección antivirus que utiliza ciencia algorítmica y aprendizaje automático para identificar, clasificar y prevenir que se ejecuten amenazas cibernéticas, conocidas o desconocidas, o que estas amenazas causen daños a los extremos.

Protección web y Servidor de seguridad instala las características opcionales de la Protección web y el Servidor de seguridad. El Servidor de seguridad del cliente comprueba todo el tráfico entrante y saliente contra su lista de reglas. La Protección web supervisa la exploración de web y las descargas para identificar amenazas y hacer cumplir las acciones definidas en la política cuando se detecta una amenaza, según las clasificaciones de los sitios web.

> **NOTA: Threat Protection y Advanced Threat Prevention no pueden residir en el mismo equipo. El instalador automáticamente impide la selección de ambos componentes. Si desea instalar Threat Protection, descargue la Endpoint Security Suite Advanced Installation Guide (Guía de instalación avanzada de Endpoint Security Suite) para obtener instrucciones.**

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

8 Haga clic en **Instalar** para comenzar la instalación. La instalación tardará varios minutos.

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

La instalación ha finalizado.

Instalación mediante la línea de comandos con el instalador maestro de ESSE

- Los modificadores deben especificarse primero en una instalación de línea de comandos. Otros parámetros se introducen en el argumento que luego pasa al modificador /v.

Modificadores

- La siguiente tabla describe los modificadores que pueden utilizarse con el instalador maestro de ESSE.

Modificador	Descripción
-y -gm2	Extracción previa del instalador maestro de ESSE. Los modificadores -y y -gm2 deben utilizarse juntos. No los separe.
/s	Instalación silenciosa

Modificador	Descripción
/z	Envía las variables al archivo .msi dentro de DDPSuite.exe

Parámetros

- La siguiente tabla describe los parámetros que pueden utilizarse con el instalador maestro de ESSE. El instalador maestro de ESSE no puede excluir los componentes individuales, pero puede recibir comandos para especificar qué componentes deben estar instalados.

Parámetro	Descripción
SUPPRESSREBOOT	Suprime el reinicio automático al terminar la instalación. Se puede utilizar en modo SILENCIOSO.
SERVER	Especifica la dirección URL de EE Server/VE 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. ATP = Advanced Threat Prevention ***sólo*** en un sistema operativo de servidor; Advanced Threat Prevention ***y*** Encryption en un sistema operativo de estación de trabajo DE-ATP = Advanced Threat Prevention y Encryption en un sistema operativo de servidor. Utilice ***solo*** para la instalación en un sistema operativo de servidor. Se trata de la instalación predeterminada en un sistema operativo de servidor si el parámetro FEATURES no se especifica. DE = Drive Encryption (cliente Encryption) Utilice solo para la instalación en el SO de servidor. BLM = BitLocker Manager SED = administración de unidades de autocifrado (controladores EMAgent/Manager, PBA/GPE)(Disponible solo cuando se instala en un SO de estación de trabajo) ATP-WEBFIREWALL = Servidor de seguridad del ciente y Protección web en un sistema operativo de estación de trabajo DE-ATP-WEBFIREWALL = Servidor de seguridad del ciente y Protección web en un sistema operativo de servidor **NOTA: Para actualizaciones a partir de Enterprise Edition o versiones de Endpoint Security Suite Enterprise anteriores a la 1.4, se *debe* especificar ATP-WEBFIREWALL o DE-ATP-WEBFIREWALL para instalar el Servidor de seguridad del cliente y la Protección web. No especifique ATP-WEBFIREWALL o DE-ATP-WEBFIREWALL al instalar un cliente administrado por Dell Enterprise Server/VE ejecutándose en Modo desconectado.**
BLM_ONLY=1	Debe utilizarse cuando se especifica FEATURES=BLM en la línea de comandos para excluir el complemento SED Management.

Ejemplo de línea de comandos

- Los parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- (En un sistema operativo de estación de trabajo) Este ejemplo instala todos los componentes mediante el instalador maestro de ESSE en puertos estándar, silenciosamente, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para que utilice el EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- (En un SO de estación de trabajo) Este ejemplo instala Advanced Threat Prevention y Encryption ***solo*** con el instalador maestro, en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (En un SO de estación de trabajo) Este ejemplo instala Advanced Threat Prevention, Encryption y SED Management con el instalador maestro de ESSE en puertos estándar, silenciosamente, con un reinicio menos, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
  SUPPRESSREBOOT=1\""
  ```

- (En un SO de estación de trabajo) Este ejemplo instala Advanced Threat Prevention, Encryption, Protección web y Servidor de seguridad de cliente con el instalador maestro de ESSE en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
  ```

- (En un SO de servidor) Este ejemplo instala Advanced Threat Protection y Encryption ***solo*** con el instalador maestro de ESSE en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```

- (En un SO de servidor) Este ejemplo instala Advanced Threat Prevention, Encryption, Protección web y Servidor de seguridad de cliente con el instalador maestro de ESSE en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
  ```

- (En un SO de servidor) Este ejemplo instala Advanced Threat Protection ***solo*** con el instalador maestro de ESSE en puertos estándar, silenciosamente, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
  ```

- (En un SO de servidor) Este ejemplo instala Encryption ***solo*** con el instalador maestro de ESSE en puertos estándar, silenciosamente, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y lo configura para utilizar el EE Server/VE Server especificado.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
  ```

Desinstalación mediante el instalador maestro de ESSE

- Cada componente debe desinstalarse por separado, seguido de la desinstalación del instalador maestro de ESSE. Los clientes se deben desinstalar en un **orden específico para evitar errores en la desinstalación**.
- Siga las instrucciones que se indican en Extracción de instaladores secundarios del instalador maestro de ESSE para obtener instaladores secundarios.
- Asegúrese de que para la desinstalación se ha utilizado como instalación la misma versión del instalador maestro de ESSE (y, por lo tanto, clientes).
- Este capítulo le remite a otros capítulos que contienen instrucciones *detalladas* sobre cómo desinstalar los instaladores secundarios. Este capítulo explica **únicamente** el último paso, la desinstalación del instalador maestro de ESSE.
- Desinstale los clientes en el siguiente orden.

  a Desinstalación del cliente Encryption.

  b Desinstalación de Advanced Threat Prevention.

  c Desinstalación de clientes SED y Advanced Authentication (se desinstala Dell Client Security Framework, que no puede desinstalarse hasta que se ha desinstalado Advanced Threat Prevention).

  d Desinstalación del cliente BitLocker Manager

  No es necesario desinstalar el paquete de controladores.
- Continúe con Desinstalación del instalador maestro de ESSE.

Desinstalación del instalador maestro de ESSE

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

Desinstalación con la línea de comandos

- El siguiente ejemplo desinstala silenciosamente el instalador maestro de ESSE.

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

  Reinicie el equipo cuando finalice.

Instalación mediante los instaladores secundarios

- Para instalar cada cliente por separado, en primer lugar es necesario extraer los archivos ejecutables secundarios del instalador maestro de ESSE, como se muestra en Extracción de los instaladores secundarios del instalador maestro de ESSE.
- 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. 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 en setup.exe. El contenido siempre debe introducirse entre comillas de texto sin formato.
/s	Modo silencioso
/x	Modo de desinstalación
/a	Instalación administrativa (se copiarán 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

Opción	Significado
/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
/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 la Ayuda de cifrado de Dell para saber cómo usar la función del cliente Encryption. Acceda a la ayuda de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte la Ayuda de EMS para obtener ayuda sobre las funciones de External Media Shield. Acceda a la ayuda desde **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte la para obtener información sobre el uso de estas funciones de Advanced Authentication y Advanced Threat Prevention. Puede acceder a esta ayuda desde **<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.

Instalación de controladores

- Los controladores y el firmware para ControlVault, los lectores de huellas digitales y las tarjetas inteligentes no se incluyen en los archivos ejecutables de instaladores secundarios o en el instalador maestro de ESSE. 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.

Instalación del cliente Encryption

- Revise los Requisitos del cliente Encryption si su organización utiliza un certificado firmado por una entidad emisora de certificados raíz, como por ejemplo, EnTrust o Verisign. Un cambio de configuración de registro será necesario en el equipo cliente para habilitar la validación de certificado.
- Los usuarios deben actualizar sus políticas haciendo clic con el botón derecho del mouse en el icono de Dell Data Protection de la bandeja del sistema y seleccionando **Comprobar si existen actualizaciones de políticas** una vez finalizada la instalación.
- El instalador del cliente Encryption se puede encontrar:
  - **Desde su cuenta FTP de Dell:** localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro de ESSE. Después de la extracción, localice el archivo en **C:\extracted\Encryption**.

Instalación con la línea de comandos

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

Parámetros
SERVERHOSTNAME=<ServerName> (FQDN del servidor Dell para la reactivación)
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 iconos de superposición, 1 deshabilita los iconos de superposición)
HIDESYSTRAYICON=1 (0 habilita el icono de la bandeja del sistema, 1 deshabilita el icono de la bandeja del sistema)

Para obtener una lista de conmutadores .msi básicos y mostrar las opciones que se pueden utilizar en líneas de comandos, consulte instalación mediante los 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=30,300 (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=300 (DEBE coincidir con el límite superior de SLOTINTERVAL o superarlo. Número de segundos que el cliente Encryption espera para generar un intento de activación basado en SLOTINTERVAL.)

Ejemplo de línea de comandos

- 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"
```

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 el cliente Encryption y Encrypt for Sharing, se oculta el icono de la bandeja del sistema DDP, se oculta los iconos superpuestos, sin diálogo, sin barra de progreso, se elimina el 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/ 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"
```

NOTA:
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 /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"
```

Instalación de Server Encryption

Existen dos métodos disponibles para instalar Server Encryption. Seleccione uno de los siguientes métodos:

- Instalar Server Encryption de forma interactiva

  NOTA:
  Server Encryption puede instalarse de forma interactiva solo en equipos que ejecutan los sistemas operativos del 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.

- Instalación de Server Encryption mediante la 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 Server Encryption. La contraseña y la autenticación de DPAPI se deshabilitan para que solo el Usuario de servidor virtual pueda acceder a las claves de cifrado en el equipo.

Antes de empezar

- La cuenta de usuario que realiza la instalación debe ser un usuario local o de dominio con permisos de nivel de administrador.
- Para suprimir el requisito de que un administrador de dominio, active Server Encryption; para ejecutar Server Encryption en servidores multidominio o sin dominio, configura la propiedad ssos.domainadmin.verify como Falso en el archivo application.properties. El archivo se guarda en las siguientes rutas de acceso de archivos, en función del DDP Server que se esté utilizando:

  Dell Enterprise Server: <*carpeta instalación*>/Security Server/conf/application.properties

  Virtual Edition - /opt/dell/server/security-server/conf/application.properties
- 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 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 el equipo a menos que se configure una Conexión de escritorio remoto antes de aplicar la política.
- Para activar Server Encryption correctamente, el equipo debe tener conexión de red.
- Cuando Trusted Platform Module (TPM) está disponible, se utiliza para sellar la clave GPK en el hardware de Dell. Si un TPM no está disponible, Server Encryption usa la API Data Protection de Microsoft (DPAPI) para proteger la clave de finalidad general.

  NOTA:
  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 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2 para obtener instrucciones.

Extraiga el instalador secundario

- Server Encryption solo requiere uno de los instaladores del Instalador maestro. Para instalar Server Encryption, primero debe extraer el instalador secundario del cliente Encryption (**DDPE_xxbit_setup.exe**) del instalador maestro. Consulte Extracción de instaladores secundarios del instalador maestro.

Instalación de Server Encryption de forma interactiva

- Use estas instrucciones para instalar Server Encryption 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 Server Encryption en un servidor, haga doble clic en el archivo **DDPE_XXbit_setup.exe** para iniciar el instalador.

> **NOTA:**
> Si Server Encryption está instalado en un equipo que está ejecutando un sistema operativo de servidor, como por ejemplo Windows Server 2012 R2, el instalador instala el cifrado en modo Servidor de manera predeterminada.

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 Haga clic en **Siguiente** para instalar Server Encryption en la ubicación predeterminada.

> **NOTA:**
> Dell recomienda realizar la instalación en la ubicación predeterminada. No se recomienda la instalación en una ubicación diferente a la ubicación predeterminada, ya sea en un directorio diferente, en la unidad D o en una unidad USB.

6 Haga clic en **Siguiente** para omitir el cuadro de diálogo **Tipo de administración**.

7 En el campo Nombre de Dell Enterprise Server, escriba el nombre de host completo del Dell Enterprise Server o Virtual Edition que administrará el usuario de destino, como *server.organization.com*.

8 Escriba el nombre de dominio en el campo **Dominio administrado** (por ejemplo, organización), y haga clic en **Siguiente**.

9 Haga clic en **Siguiente** para omitir el cuadro de diálogo **Información de Dell Policy Proxy** autocompletado.

10 Haga clic en **Siguiente** para omitir el cuadro de diálogo **Información de Dell Device Server** autocompletado.

11 Haga clic en **Instalar** para comenzar la instalación.
La instalación puede tardar varios minutos.

12 En el cuadro de diálogo **Configuración completada**, haga clic en Finalizar.
La instalación ha finalizado.

> **NOTA:**
> El archivo de registro para la instalación se encuentra en el directorio %temp% de la cuenta, ubicado en **C:\Users\<nombre_usuario>\AppData\Local\Temp**. Para ubicar el archivo de registro del instalador, busque un nombre de archivo que empiece por MSI y termine con una extensión .log. El archivo debe tener un sello con fecha/hora que coincida con la hora en la que ejecutó el instalador.

> **NOTA:**
> Como parte de la instalación, se crea una **cuenta de usuario de servidor virtual** para el uso exclusivo de Server Encryption. La contraseña y la autenticación de DPAPI se deshabilitan para que solo el Usuario de servidor virtual pueda acceder a las claves de cifrado en el equipo.

13 Reinicie el equipo.

> **IMPORTANTE: Seleccione Posponer reinicio solo si necesita tiempo para guardar su trabajo y cerrar cualquier aplicación abierta.**

Instalación de Server Encryption mediante la línea de comandos

Cliente Server Encryption: ubique 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=<Nombre de servidor de administración> SERVERMODE=1 POLICYPROXYHOSTNAME=<Nombre de RGK> MANAGEDDOMAIN=<Mi dominio> DEVICESERVERURL=<Nombre de servidor de activación> GKPORT=<Nuevo puerto GK> MACHINEID=<Nombre de máquina> RECOVERYID=<Id. de recuperación> 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.
- No se recomienda la instalación en una ubicación diferente a la ubicación predeterminada, ya sea en un directorio diferente de C: o en una unidad USB. Dell recomienda realizar la instalación en la ubicación predeterminada.
- Incorpore un valor que contenga uno o más caracteres especiales, como un espacio, en comillas de escape.
- La URL de Dell Activation Server (DEVICESERVERURL) distingue entre mayúsculas y minúsculas.

Ejemplo de instalación con la línea de comandos

- En el siguiente ejemplo se instala el cliente con los parámetros predeterminados (cliente Server Encryption, instalación silenciosa, 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"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 el cliente Server Encryption con un archivo de registro y los parámetros predeterminados (cliente Server Encryption, instalación silenciosa, Encrypt for Sharing, sin diálogo, sin barra de progreso, sin reinicio, instalados en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\Encryption) y especifica un nombre de archivo de registro personalizado que termina con un número (DDP_ssos-090.log) que se debe aumentar si la línea de comandos se ejecuta más de una vez en el mismo servidor.

  ```
  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"
  ```

  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 creará registros de instalación en una carpeta C:\Logs.

Reinicie el equipo.

Después de la instalación, reinicie el equipo. El equipo debe reiniciarse lo antes posible.

IMPORTANTE:

Seleccione **Posponer reinicio** solo si necesita tiempo para guardar su trabajo y cerrar cualquier aplicación abierta.

Activación de Server Encryption

- El servidor debe estar conectado a la red de la empresa.
- Asegúrese de que el nombre del equipo del servidor es el nombre del extremo que desea que se muestre en la Remote Management Console.
- Un usuario interactivo, en vivo, 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). El cliente de Server Encryption 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 al equipo 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 Remote Management Console como SERVIDOR-USUARIO@*<nombre del servidor completo>*. 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 de visualización no cambiará en la Remote Management Console. Sin embargo, si el cliente de Server Encryption se activa de nuevo después de que se cambie el nombre del servidor, el nuevo nombre del servidor aparecería en la Remote Management Console.

Se muestra un cuadro de diálogo de activación después de cada reinicio, para solicitar al usuario que active Server Encryption. Si la activación no se ha completado, siga estos pasos:

1 Inicie sesión en el servidor ya sea en el servidor o a través Remote Desktop Connection.

2 Haga clic con el botón derecho del mouse en el icono de cifrado  en la bandeja del sistema y haga clic en **Acerca de**.

3 Compruebe que el cifrado se está ejecutando en modo Servidor.

4 Seleccione **Activar Encryption** en el menú.

5 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 DDP 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.

6 Haga clic en **Cerrar**.

Después de la activación, comienza el cifrado.

7 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 *Credenciales de Windows seguras* se establece en Verdadero, Server Encryption cifra los archivos de **\Windows\system32\config**, que incluye las credenciales de Windows. Los archivos en **\Windows\system32\config** se cifran incluso si la política *Cifrado de SDE habilitado* se establece en **No seleccionada**. De manera predeterminada, la política *Secure Windows Credentials* se establece como **Seleccionada**.

NOTA:
Después de reiniciar el equipo, la autenticación para el material de claves común *siempre* requiere la clave de la máquina del servidor protegido. El DDP Server devuelve una clave de desbloqueo para acceder a las claves y políticas de cifrado en el almacén. (Las claves y políticas son para el servidor, no para el usuario). Sin la clave de máquina del servidor, la clave de cifrado de archivo común no puede desbloquearse y el equipo no puede recibir actualizaciones de la política.

Confirmar la activación

Desde la consola local, abra el cuadro de diálogo **Acerca de**, para confirmar que está instalado, autenticado y en modo Servidor. Si la Id. de Shield está en **rojo**, el cifrado aún no se ha activado.

Usuario de Virtual Server

- En la Remote Management Console, puede encontrarse 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 es utilizada por Server Encryption y es transparente a la operación del servidor protegido. El usuario de del servidor virtual se asocia con el paquete de claves de cifrado y con 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, el equipo se autentica automáticamente con el usuario del servidor virtual y descarga la clave de la máquina de Dell Data Protection Server.

Instalación del cliente Advanced Threat Prevention

- Threat Protection y Advanced Threat Prevention **no pueden residir en el mismo equipo**. No instale estos dos componentes en el mismo equipo, ya que se producirán problemas de compatibilidad. Si desea instalar Threat Protection, descargue la Endpoint Security Suite Advanced Installation Guide (Guía de instalación avanzada de Endpoint Security Suite) para obtener instrucciones.
- Los instaladores deben ejecutarse en un orden específico. Si no instala los componentes en el orden correcto, la instalación será errónea. Ejecute los instaladores en el siguiente orden:

1 **(En un SO de estación de trabajo solamente)** \Security Tools: Advanced Threat Prevention necesita el componente Dell Client Security Framework.

(En un SO de servidor solamente) Componente de Dell Client Security Framework, tal como se muestra en Instalación de línea de comandos.

2 **(En un SO de estación de trabajo solamente)**\Security Tools\Authentication: en un SO de estación de trabajo solamente, Security Tools y Authentication deben instalarse conjuntamente; Authentication no está disponible en un SO de servidor y no es necesario que se instale.

3 Cliente Advanced Threat Prevention, como se muestra en Instalación desde la línea de comandos.

- El instalador del cliente Advanced Threat Prevention se puede encontrar:
  - **Desde su cuenta FTP de Dell**: localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip y extraiga los instaladores secundarios del instalador maestro de ESSE. Después de la extracción, localice el archivo en **C:\extracted\Advanced Threat Protection**.
- Los instaladores de cliente SED y Advanced Authentication se pueden encontrar en estas ubicaciones:
  - **Desde su cuenta FTP de Dell**: localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip y extraiga los instaladores secundarios del instalador maestro de ESSE. Tras la extracción, localice el archivo en **C:\extracted\Security Tools** y **C:\extracted\Security Tools\Authentication**.

NOTA: Los clientes Advanced Authentication y SED pueden instalarse solamente en un SO de estación de trabajo, no en un SO de servidor.

Instalación con la línea de comandos

- Hay comandos .msi básicos disponibles para la instalación.
- La tabla a continuación indica los parámetros disponibles para la instalación.

Parámetros
CM_EDITION=1 <administración remota>
INSTALLDIR=<cambiar el destino de la instalación>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <sin entrada en la lista de programas del Panel de control>
REBOOT=ReallySuppress <suprime el reinicio>
FEATURE=BASIC <***necesario*** en el SO de un servidor; también se puede utilizar (opcionalmente) en el SO de una estación de trabajo; evita la instalación de SED Management y BitLocker Manager>

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.

Ejemplos de líneas de comandos

- En el siguiente ejemplo se instala el componente Dell Client Security Framework básico, sin el cliente SED Management ni BitLocker Manager (instalación silenciosa, sin reinicio, sin entradas en la lista de programas del panel de control instalado en la ubicación predeterminada de C:\Program Files\Dell\Dell Data Protection).

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

- El siguiente ejemplo instala Advanced Threat Prevention (instalación silenciosa, sin reinicio, archivo de registro de instalación y carpeta de instalación en las ubicaciones indicadas)

```
MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
\AdvancedThreatProtectionPlugins.msi.log"
```

y

```
AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
```

NOTA: Estos componentes deben instalarse únicamente desde la línea de comandos. Al hacer doble clic para instalar el componente, se instala una versión del producto no gestionada que no es de Dell, que no se admite. Si realiza esta acción de forma accidental, vaya a Agregar/Quitar programas y desinstale dicha versión.

Instalación de la Protección web y el Servidor de seguridad

- Advanced Threat Prevention y Threat Protection **no pueden residir en el mismo equipo**. No instale estos dos componentes en el mismo equipo, ya que se producirán problemas de compatibilidad. Sin embargo, Advanced Threat Prevention puede instalarse con los componentes de la Protección web y el Servidor de seguridad.
- Los instaladores deben ejecutarse en un orden específico. Si no instala los componentes en el orden correcto, la instalación será errónea. Ejecute los instaladores en el siguiente orden:

1 Se requiere el cliente Encryption con los componentes de Protección web y Servidor de seguridad. Vaya a Ejemplo de línea de comandos para obtener un ejemplo de instalación.

2 Protección web y Servicor de seguridad, tal y como se muestra en Instalación con la línea de comandos.

Instalación con la línea de comandos

- La siguiente tabla detalla los parámetros disponibles para el archivo **EnsMgmtSdkInstaller.exe.**

Parámetros	Descripción
LoadCert	Carga el certificado en el directorio especificado.

- La siguiente tabla detalla los parámetros disponibles para el archivo **setupEP.exe**.

Parámetros	Descripción
ADDLOCAL="fw,wc"	Identifica los módulos que se instalarán: fw = Servidor de seguridad del cliente wc = Protección web
override "hips"	No instala Host Intrusion Prevention
INSTALLDIR	Ubicación de instalación no predeterminada
nocontentupdate	Indica al instalador que no actualice automáticamente archivos de contenido como parte del proceso de instalación. Dell recomienda programar una actualización tan pronto como la instalación se haya completado.
nopreservesettings	No guarda la configuración.

- La siguiente tabla detalla los parámetros disponibles para el archivo **DellThreatProtection.msi**.

Parámetros	Descripción
Reboot=ReallySuppress	Suprime el reinicio.
ARP	0=Ninguna entrada en Agregar/Quitar programas 1=Entrada en Agregar/Quitar programas

- La siguiente tabla detalla los parámetros disponibles para el archivo **EnsMgmtSdkInstaller.exe.**

Parámetros	Descripción
ProtectProcesses	Especifica el nombre de archivo y la ubicación de los procesos que proteger.
InstallSDK	Instala el SDK en la ubicación especificada.
RemoveRightClick	Quita la opción del menú derecho del mouse para usuarios finales.
RemoveMcTray	Quita la bandeja del sistema.

Ejemplo de línea de comandos

\Dell Threat Protection\SDK

- La siguiente línea de comandos carga los parámetros predeterminados del certificado.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
```

NOTA:
Este instalador se puede omitir si se realiza la actualización.

Luego:

\Dell Threat Protection\EndPointSecurity

- En el siguiente ejemplo se instala la protección web y el Servidor de seguridad del cliente con los parámetros predeterminados (modo silencioso, instalación de Servidor de seguridad del cliente y Protección web, invalidación de la Prevención de intrusiones en el host, sin actualizaciones de contenido, sin guardar la configuración).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /nocontentupdate /nopreservesettings /qn
```

Luego:

\Dell Threat Protection\ThreatProtection\WinXXR

- En el siguiente ejemplo se instala el cliente con los parámetros predeterminados (supresión del reinicio, sin diálogo, sin barra de progreso, sin entrada en la lista de programas del Panel de control).

```
"Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- El siguiente ejemplo instala el SDK de Threat Protection.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Instalación de los clientes SED Management y Advanced Authentication

- Para Advanced Authentication en v8.x se requiere el cliente SED.
- Revise los Requisitos del cliente SED 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 usuarios inician sesión en PBA mediante sus credenciales de Windows.

- Los instaladores de cliente SED y Advanced Authentication se pueden encontrar:
  - **Desde su cuenta FTP de Dell:** localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro de ESSE. Tras la extracción, localice el archivo en **C:\extracted\Security Tools** y **C:\extracted\Security Tools\Authentication**.

Instalación con la línea de comandos

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

Parámetros
CM_EDITION=1 <administración remota>
INSTALLDIR=<cambiar el destino de la instalación>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <sin entrada en la lista de programas del Panel de control>

Para obtener una lista de conmutadores .msi básicos y mostrar las opciones que se pueden utilizar en líneas de comandos, consulte instalación mediante los instaladores secundarios.

Ejemplo de línea de comandos

\Security Tools

- En el ejemplo siguiente se instala remotamente el SED 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:

\Security Tools\Authentication

- En el siguiente ejemplo se instala Advanced Authentication (instalación silenciosa, sin reinicio)

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

Instalación del cliente BitLocker Manager

- 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:
  - **Desde su cuenta FTP de Dell:** localice el paquete de instalación en DDP-Endpoint-Security-Suite-1.x.x.xxx.zip y luego extraiga los instaladores secundarios del instalador maestro de ESSE. Después de la extracción, localice el archivo en **C:\extracted\Security Tools**.

Instalación con la línea de comandos

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

Parámetros
CM_EDITION=1 <administración remota>
INSTALLDIR=<cambiar el destino de la instalación>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <instalar solo BitLocker Manager>
FEATURE=BLM,SED <instalar BitLocker Manager con SED>
ARPSYSTEMCOMPONENT=1 <sin entrada en la lista de programas del Panel de control>

Para obtener una lista de conmutadores .msi básicos y mostrar las opciones que se pueden utilizar en líneas de comandos, consulte instalación mediante los 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"
```

7

Desinstalación mediante los instaladores secundarios

- Para desinstalar cada cliente por separado, en primer lugar es necesario extraer los archivos ejecutables secundarios del instalador maestro de ESSE, como se muestra en Extracción de los instaladores secundarios del instalador maestro de ESSE También puede ejecutar 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 introducirse entre comillas de texto sin formato.
/s	Modo silencioso
/x	Modo de desinstalación
/a	Instalación administrativa (se copiarán 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

Opción	Significado
/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

Desinstalación de la Protección web y el Servidor de seguridad

Si la Protección web y el Servidor de seguridad no están instalados, proceda con la Desinstalación del cliente Encryption.

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESS, el instalador del cliente Protección web y Servidor de seguridad se puede localizar en **C:\extracted\Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi.**
- Vaya a Agregar/Quitar programas en el Panel de control y desinstale los siguientes componentes en este orden.
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Luego:
- El siguiente ejemplo desinstala la Protección web y el Servidor de seguridad .

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

Desinstalación de los clientes Encryption y Server Encryption

- 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.
- Windows Shields han actualizado el EE Server/VE Server para cambiar el estado a *No protegido* al principio de un proceso de desinstalación de Shield. Sin embargo, en caso de que el cliente no se pueda comunicar con EE Server/VE Server, el estado no se podrá actualizar, independientemente del motivo. En este caso, deberá *quitar el extremo* manualmente en Remote Management Console. Si su empresa utiliza este flujo de trabajo por razones de cumplimiento, Dell le recomienda comprobar que se haya configurado el estado *No protegido* de la manera esperada, en la Remote Management Console o en Compliance Reporter.

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 EE Server) deben estar configurados antes de la desinstalación si utilizan la opción **Descargar claves del Encryption Removal Agent del servidor**. Consulte Configurar Key Server para la desinstalación de cliente Encryption activado en EE Server para obtener instrucciones. No es necesaria ninguna acción si el cliente que vaya a realizar la desinstalación se activa en un VE Server, ya que VE Server 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 Servicios.

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESSE, el instalador del cliente Encryption se encuentra 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: 3 - Usar el paquete LSARecovery 2 - Usar el material de claves forenses descargado con anterioridad 1 - Descargar claves del servidor Dell 0 - No instalar Encryption Removal Agent
CMGSILENTMODE	Propiedad para desinstalación silenciosa: 1 - Silencioso 0 - No silencioso
Propiedades requeridas	
DA_SERVER	FQHN para el EE Server que aloja la sesión de negociación.
DA_PORT	Puerto en el EE 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 EE Server.
DA_RUNAS	Nombre de usuario en formato compatible con SAM en cuyo contexto se realizará la solicitud de búsqueda de clave. Este usuario debe figurar en la lista de Key Server en el EE Server.

Parámetro	Selección
DA_RUNASPWD	Contraseña para el usuario de runas.
FORENSIC_ADMIN	La cuenta de Administrador forense del servidor Dell, que puede utilizarse 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.

- El siguiente ejemplo desinstala el cliente Encryption de forma silenciosa y descarga las claves de cifrado desde el EE 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.

- El siguiente ejemplo desinstala de forma silenciosa el cliente Encryption y descarga 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.

IMPORTANTE:

Dell recomienda las siguientes acciones al utilizar una contraseña de Administrador forense en la línea de comandos:

1. Cree una cuenta de Administrador forense en la Remote Management Console 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.

NOTA:

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"
```

Desinstalación de Advanced Threat Prevention

Desinstalación con la línea de comandos

- El siguiente ejemplo desinstala el cliente Advanced Threat Prevention. ***Este comando debe ejecutarse desde un símbolo del sistema de administrador.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  Apague y reinicie el equipo y, a continuación, desinstale el componente de Dell Client Security Framework.

- **IMPORTANTE: Si ha instalado los clientes SED y Advanced Authentication o ha activado la Autenticación previa al inicio, siga las instrucciones de desinstalación en Desinstalación de los clientes SED y Advanced Authentication.**

  El ejemplo siguiente desinstala solo el componente de Dell Client Security Framework y no los clientes SED y Advanced Authentication.

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

Desinstalación de los clientes SED y Advanced Authentication

- Se requiere la conexión de red con EE Server/VE Server para la desactivación de PBA.

Proceso

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

Desactivación de la PBA

1. Como administrador de Dell, inicie sesión en la Remote Management Console.
2. En el panel izquierdo, haga clic en **Proteger y administrar** > **Extremos**.
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 icono de **Detalles** del equipo que desee.
7. Haga clic en **Políticas de seguridad** en el menú superior.
8. Seleccione **Unidades de cifrado automático** en el menú desplegable **Categoría de política**.
9. Expanda el área **Administración SED** y cambie las políticas **Habilitar Administración SED** y **Activar PBA** de *True* a ***False***.
10. Haga clic en **Guardar**.
11. En el panel izquierdo, haga clic en **Acciones** > **Confirmar políticas**.
12. Haga clic en **Aplicar cambios**.

    Espere a que se propague la política desde EE Server/VE Server al equipo de destino para la desactivación.

Desinstale los clientes SED y Authentication después de desactivar PBA.

Desinstalación de los clientes SED y Advanced Authentication

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESS, el instalador del cliente SED se encuentra en **C:\extracted\Security Tools \EMAgent_XXbit_setup.exe**.
- Una vez extraído el instalador maestro de ESSE, el instalador del cliente SED se encuentra en **C:\extracted\Security Tools \Authentication\<x64/x86>\setup.exe**.
- El siguiente ejemplo desinstala de forma silenciosa el cliente SED.

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

  Apague y reinicie el equipo cuando finalice.

  Luego:

- El siguiente ejemplo desinstala de forma silenciosa el cliente Advanced Authentication.

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

  Apague y reinicie el equipo cuando finalice.

Desinstalación del cliente BitLocker Manager

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESSE, el instalador del cliente BitLocker se encuentra en **C:\extracted\Security Tools \EMAgent_XXbit_setup.exe**.
- El siguiente ejemplo desinstala de forma silenciosa el cliente de BitLocker Manager.

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

  Reinicie el equipo cuando finalice.

8

Situaciones frecuentes

- Para instalar cada cliente por separado, en primer lugar es necesario extraer los archivos ejecutables secundarios del instalador maestro de ESSE, como se muestra en Extracción de los instaladores secundarios del instalador maestro de ESSE.
- El cliente SED es necesario para Advanced Authentication en v8.x, motivo por el que forma parte de la línea de comandos en los siguientes ejemplos.
- El componente de instalador secundario de Advanced Threat Prevention debe instalarse únicamente desde la línea de comandos. Al hacer doble clic para instalar el componente, se instala una versión del producto no gestionada que no es de Dell, que no se admite. Si realiza esta acción de forma accidental, vaya a Agregar/Quitar programas y desinstale dicha versión.
- 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

Opción	Significado
/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 la Ayuda de cifrado de Dell para saber cómo usar la función del cliente Encryption. Acceda a la ayuda de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte la Ayuda de EMS para obtener ayuda sobre las funciones de External Media Shield. Acceda a la ayuda desde **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte la *Ayuda de Endpoint Security Suite Enterprise* para obtener información sobre el uso de estas funciones de Advanced Authentication y Advanced Threat Prevention. Puede acceder a esta ayuda desde **<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.

Cliente Encryption, Advanced Threat Prevention y Advanced Authentication

- En el ejemplo siguiente se instala remotamente el SED 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**). Este componente instala Dell Client Security Framework, que es necesario para Advanced Threat Prevention.

  ```
  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 Advanced Threat Prevention (instalación silenciosa, sin reinicio, archivo de registro de instalación y carpeta de instalación en las ubicaciones indicadas)

  ```
  MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
  APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
  \AdvancedThreatProtectionPlugins.msi.log"
  ```

  y

  ```
  AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
  "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
  ```

- En el siguiente ejemplo se instala el cliente Encryption 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"
  ```

- Los siguientes ejemplos instalan las características ***opcionales***, la Protección web y el Servidor de seguridad.
- **\Dell Threat Protection\SDK**

  La siguiente línea de comandos carga los parámetros predeterminados del certificado.

  ```
  EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs
  \McAfeeSDKInstallerBeforeEndPoint.log"
  ```

NOTA:
Este instalador se puede omitir si se realiza la actualización.

Luego:

\Dell Threat Protection\EndPointSecurity

- En el siguiente ejemplo se instala las características opcionales de Protección web y Servidor de seguridad con los parámetros predeterminados (modo silencioso, instalación de Threat Protection, Servidor de seguridad del cliente y Protección web, invalidación de la Prevención de intrusiones en el host, sin actualizaciones de contenido, sin guardar la configuración).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
nocontentupdate /nopreservesettings /qn
```

Luego:

\Dell Threat Protection\ThreatProtection\WinXXR

- En el siguiente ejemplo se instala el cliente con los parámetros predeterminados (supresión del reinicio, sin diálogo, sin barra de progreso, sin entrada en la lista de programas del Panel de control).

```
"DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- El siguiente ejemplo instala el SDK de Threat Protection.

```
EnsMgmtSdkInstaller.exe -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat
Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell
\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Cliente SED (incluye Advanced Authentication) y External Media Edition Shield

- En el ejemplo siguiente se instala remotamente el SED 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 ejemplo siguiente se instala solo EMS (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"
```

BitLocker Manager y External Media Edition Shield

- 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 EMS (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"
```

BitLocker Manager y Advanced Threat Prevention

- 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**). Este componente instala la infraestructura Dell Client Security Framework necesaria para Advanced Threat Prevention.

```
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:

- El siguiente ejemplo instala Advanced Threat Prevention (instalación silenciosa, sin reinicio, archivo de registro de instalación y carpeta de instalación en las ubicaciones indicadas)

```
MSIEXEC.EXE /I "AdvancedThreatProtection_xXX.msi" /qn REBOOT="ReallySuppress"
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP.log"
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection"
```

Aprovisionar un inquilino para Advanced Threat Prevention

Si su empresa utiliza Advanced Threat Prevention, debe aprovisionar un inquilino en el servidor Dell antes de que la aplicación de las políticas de Advanced Threat Prevention sea activa.

Requisitos previos

- Lo debe llevar a cabo el administrador con el rol de administrador del sistema.
- Debe tener conexión a Internet para el aprovisionamiento en el servidor Dell.
- Debe tener conexión a Internet en el cliente para mostrar la integración del servicio en línea de Advanced Threat Prevention en la Remote Management Console.
- El aprovisionamiento se basa en una señal generada a partir de un certificado durante el proceso de aprovisionamiento.
- Las licencias de Advanced Threat Prevention deben estar presentes en el servidor Dell.

Aprovisionar un inquilino

1 Inicie sesión en Remote Management Console y vaya a **Administración de servicios**.

2 Haga clic en **Configurar servicio Advanced Threat Protection**. Importe sus licencias ATP si se produce un error en este punto.

3 La configuración guiada se inicia una vez que se han importado las licencias. Haga clic en **Siguiente** para empezar.

4 Lea y acepte el EULA (la casilla de verificación está **desactivada** de forma predeterminada) y haga clic en **Siguiente**.

5 Proporcione las credenciales de identificación a DDP Server para aprovisionar el inquilino. Haga clic en **Siguiente**. *No se permite aprovisionar un inquilino existente con marca Cylance.*

6 Descargue el certificado. Esto es necesario para poder llevar a cabo una recuperación si se produce algún problema con DDP Server. No se realiza automáticamente ninguna copia de seguridad de este certificado con el "actualizador" de la versión 9.2. Realice una copia de seguridad del certificado en una ubicación segura de otro equipo. Seleccione la casilla para confirmar que ha realizado una copia de seguridad del certificado y haga clic en **Siguiente**.

7 La configuración ha terminado. Haga clic en **Aceptar**.

Configuración de actualización automática del agente Advanced Threat Prevention

En la Remote Management Console de Dell, puede inscribirse para recibir actualizaciones automáticas del agente Advanced Threat Prevention. La inscripción para recibir las actualizaciones automáticas del agente permite a los clientes descargar y aplicar automáticamente las actualizaciones desde el servidor Advanced Threat Prevention. Las actualizaciones se efectúan mensualmente.

NOTA: Las actualizaciones automáticas del agente son compatibles con el servidor Dell v9.4.1 o posterior.

Cómo recibir actualizaciones automáticas del agente

Para inscribirse y recibir actualizaciones automáticas del agente:

1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración** > **Administración de servicios**.

2 En la pestaña **Amenazas avanzadas**, bajo Actualización automática del agente, haga clic en el botón **Activar** y, a continuación, en el botón **Guardar preferencias**.

Es posible que se tarde unos minutos en rellenar la información y mostrar las actualizaciones automáticas.

Cómo dejar de recibir actualizaciones automáticas del agente

Para dejar de recibir actualizaciones automáticas del agente:

1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración** > **Administración de servicios**.

2 En la pestaña **Amenazas avanzadas**, bajo Actualización automática del agente, haga clic en el botón **Desactivar** y, a continuación, en el botón **Guardar preferencias**.

Configuración previa a la instalación para la Contraseña de un solo uso, SED UEFI y BitLocker

Inicialización del TPM

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

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

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

Configuración previa a la instalación para equipos UEFI

Habilitar conectividad de red durante la autenticación previa al inicio de UEFI

Para que la autenticación previa al inicio sea correcta en un equipo 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 requerirá 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".
- 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. El parámetro predeterminado indica que la herramienta de la línea de comandos seguirá el mismo proceso que el asistente de configuración de BitLocker.

```
BdeHdCfg -target default
```

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

Configuración de GPO en la controladora de dominio para habilitar derechos

- Si sus clientes están autorizados por Dell Digital Delivery (DDD), siga estas instrucciones para establecer GPO en la controladora de dominio, a fin de habilitar los derechos (es posible que no sea el mismo servidor que ejecuta EE Server/VE Server).
- La estación de trabajo debe ser miembro del OU donde se aplica el GPO.

> **NOTA:**
> Asegúrese de que el puerto de salida 443 esté disponible para establecer comunicación con EE Server/VE Server. Si el puerto 443 está bloqueado (por cualquier motivo), la función de autorización no funcionará.

1. En el controlador de dominio para administrar los clientes, haga clic en **Inicio** > **Herramientas administrativas** > **Administración de políticas de grupo**.
2. Haga clic con el botón derecho del mouse en el OU donde se debe aplicar la política y seleccione **Crear un GPO en este dominio**, y **Vincularlo aquí...**
3. Introduzca 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 mouse en el GPO creado y seleccione **Editar**.
5. Se carga el Editor de administración de políticas de grupo. Acceda a **Configuración del equipo** > **Preferencias** > **Configuración de Windows** > **Registro**.
6. Haga clic con el botón derecho del mouse 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 de EE Server/VE 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.

Extracción de instaladores secundarios del instalador maestro de ESSE

- Para instalar cada cliente de manera individual, extraiga los archivos secundarios ejecutables del instalador.
- El instalador maestro de ESSE no es un *desinstalador* maestro. Cada cliente debe desinstalarse por separado, seguido por la desinstalación del instalador maestro de ESSE. Utilice este proceso para extraer los clientes del instalador maestro de ESSE de modo que se puedan utilizar para la desinstalación.

1 Desde el medio de instalación de Dell, copie el archivo **DDPSuite.exe** al equipo local.

2 Abra un símbolo del sistema en la misma ubicación que el archivo **DDPSuite.exe** e introduzca:

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

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

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

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

Configurar Key Server para la desinstalación de cliente Encryption activado en EE Server

- Esta sección explica cómo configurar los componentes a fin de utilizarlos con la autenticación/autorización Kerberos al utilizar un EE Server. VE Server 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. Dicho acceso se otorga a través de la Remote Management Console mediante dominios individuales.
- 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 VE Server no utiliza Key Server, la desinstalación normal se ve afectada. Cuando un cliente Encryption que está activado en un VE Server se desinstala, se utiliza la recuperación de clave forense estándar a través de Security Server en lugar del método Kerberos de Key Server. Consulte Desinstalación de línea de comandos para obtener más información.

Panel Servicios: Agregar el usuario de cuenta de dominio

1 En EE Server, navegue hasta el 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 el campo *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 operaciones posteriores).

5 Vaya hasta <Directorio de instalación de Key Server> log.txt a fin de comprobar que el servicio arrancó correctamente.

Archivo de configuración de Key Server: Agregar usuario para EE Server Communication

1 Vaya hasta el <Directorio de instalación de Key Server>.

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 EE 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 EE Server es aceptable porque se requiere la validación de esa cuenta de usuario a fin de obtener autorización de Active Directory.

Por ejemplo, en un entorno multi-dominios, si solo se coloca el nombre de la cuenta del SAM, “jdoe”, probablemente fallará porque EE Server no podrá autenticar “jdoe” ya que no puede encontrar “jdoe”. En un entorno multi-dominios, 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="<valor cifrado de la contraseña>" /> y cambie “epw” a “password”. Luego proceda a cambiar el texto "<valor cifrado de la contraseña>" a la contraseña del usuario (paso 3). La contraseña se cifrará nuevamente cuando se reinicie EE 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 EE 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 Remote Management Console. El formato “superadmin” puede ser cualquier método que pueda autenticarse con EE 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 EE Server es aceptable porque se requiere la validación de esa cuenta de usuario a fin de obtener autorización de Active Directory. Por ejemplo, en un entorno multi-dominios, si solo se coloca el nombre de la cuenta del SAM, “jdoe”, probablemente fallará porque EE Server no podrá autenticar “jdoe” ya que no puede encontrar “jdoe”. En un entorno multi-dominios, 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 quiénes tienen permiso para 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 la antigüedad que puede llegar a tener 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 Server. Si la contraseña "superadmin" fue cambiada, se debe cambiar aquí.]

</appSettings>

</configuration>

Panel Servicios: Reiniciar el servicio Key Server

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

Remote Management Console: Agregar administrador forense

1 De ser necesario, inicie una sesión en la Remote Management Console.
2 Haga clic en **Poblaciones** > **Dominios**.
3 Seleccione el dominio adecuado.
4 Haga clic en la pestaña **Key Server**.
5 En el campo Cuenta, agregue el usuario que realizará las actividades de administrador. El formato es DOMINIO\NombreUsuario. 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 fue agregado 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.

Usar la utilidad de descarga administrativa (CMGAd)

- Esta herramienta permite la descarga de una agrupación de material de claves para usar en un equipo que no esté conectado a un EE Server/VE Server.
- Esta utilidad utiliza uno de los siguientes métodos para descargar una agrupación de claves, dependiendo del 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

Uso de la Utilidad de descarga administrativa en modo Forense

1 Haga doble clic en **cmgad.exe** para lanzar 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/.

Admin de Dell: nombre del administrador con credenciales de administrador forense (habilitado en la Remote Management Console), como, por ejemplo, jdoe

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

> **SUGERENCIA:**
> Normalmente, es suficiente con especificar el MCID *o* DCID. No obstante, si conoce ambos, es útil especificar los dos. Cada parámetro contiene diferente información sobre el cliente y el equipo cliente.

Haga clic en **Siguiente**.

3 En el campo 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 ha guardado o haga clic en ... para seleccionar una ubicación diferente.

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.

Uso de la Utilidad de descarga administrativa en modo Administración

El VE Server no utiliza el Key Server, así que el modo Administración no podrá usarse para obtener una agrupación de claves de un VE Server. Utilice el modo Forense para obtener la agrupación de claves si el cliente está activado en un VE Server.

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\nombreusuario. 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

> **SUGERENCIA:**
> Normalmente, es suficiente con especificar el MCID *o* DCID. No obstante, si conoce ambos, es útil especificar los dos. Cada parámetro contiene diferente información sobre el cliente y el equipo cliente.

Haga clic en **Siguiente**.

3 En el campo 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 guardarán o haga clic en ... para seleccionar una ubicación diferente.

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.

Configurar Server Encryption

Habilitar Server Encryption

NOTA:
Server Encryption convierte el cifrado de usuario en cifrado común.

1 Inicie sesión como Administrador de Dell en la Dell Remote Management Console.

2 Seleccione **Grupo de extremos** (o **Extremo**), busque el extremo o grupo del extremo que desea habilitar, seleccione **Políticas de seguridad** y, a continuación, seleccione la categoría de la política **Server Encryption**.

3 Establezca las siguientes políticas:

- Server Encryption: **seleccione** para habilitar Server Encryption 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 desde el menú del icono Encryption, ubicado en la bandeja del sistema.

Establecer políticas EMS de Server Encryption

El ***equipo de cifrado de origen*** es el equipo que cifra originariamente un dispositivo extraíble. Cuando el equipo de origen es un ***servidor protegido***, un servidor con Server Encryption 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 EMS 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, controlando el 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 Remote Management Console bajo el grupo de tecnología *Server Encryption*.

Server Encryption y medios externos

Cuando la política *Medios externos de cifrado de EMS* del servidor protegido está establecida en **Seleccionado**, se cifran los medios externos. Server 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 del equipo al que esté conectado.

NOTA:
Server Encryption 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 con el equipo.

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 de origen.

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 podrán 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 el equipo de cifrado de origen de un dispositivo extraíble es un servidor protegido, el propietario/usuario siempre debe iniciar sesión en el dispositivo extraíble cuando lo utilice en equipos que no sean de origen, independientemente de la configuración de la política de EMS definida en los demás equipos.

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

Suspender una instancia de servidor cifrado

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

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.

IMPORTANTE:

Úselo con cuidado. La suspensión de una instancia de servidor cifrado podría generar inestabilidad dependiendo de la configuración de la política y de si el servidor protegido se suspende mientras que está desconectado de la red.

Requisitos previos

- Los derechos de administrador de soporte técnico, asignados en la Remote Management Console, son necesarios para suspender un extremo.
- El administrador debe iniciar sesión en la Remote Management Console.

  En el panel izquierdo de la Remote Management Console, haga clic en **Poblaciones** > **Extremos**.

  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** , a continuación, **Sí**.

  NOTA:

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

Solución de problemas

Todos los clientes: Solución de problemas

- Los archivos de registro del instalador del maestro de **ESSE** se encuentran disponibles 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\<UserName>\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\<UserName>\AppData\Local\Temp. For example, C:\Users\<UserName>\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=30653 para descargar la versión completa de Microsoft .Net Framework 4.5.
- Consulte *Compatibilidad de Dell Data Protection | Security Tools* si el equipo en el que se va a llevar a cabo la instalación tiene (o ha tenido) el producto Dell Access instalado. DDP|A no es compatible con esta suite de productos.

Solución de problemas de los clientes Encryption y Server Encryption

Realizar la actualización de aniversario de Windows 10

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

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 activar no son las credenciales del administrador de 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: Ha fallado la activación debido a que la cuenta de usuario no tiene derechos de administración de dominio.

Las credenciales utilizadas para la activación no tienen derechos de administrador de dominio o el nombre de usuario del administrador no se encontraba en formato UPN.

Posible solución: en el cuadro de diálogo Activación, introduzca credenciales para un Administrador de dominio y asegúrese de que se encuentran en formato UPN.

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

O bien

`The operation timed out.`

Server Encryption no ha podido comunicarse con el puerto 8449 sobre https hasta el DDP Security Server.

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 DDP 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 puede activarse contra un servidor heredado; la versión de DDP Server debe ser la versión 9.1 o posterior. Si fuera necesario, actualice su DDP Server a la versión 9.1 o posterior.
- Compruebe la URL del DDP 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 Server Encryption requiere un usuario en directo para acceder al servidor. El usuario que haya iniciado sesión puede ser de cualquier tipo: dominio o sin dominio, conectado-escritorio-remoto o usuario interactivo, pero el usuario debe tener acceso a las credenciales de Administrador de dominio.

El cuadro de diálogo Activación se muestra cuando una de las dos siguientes cosas sucede:

- Un nuevo usuario (no administrado) inicia sesión en el equipo.
- Cuando un nuevo usuario hace clic con el botón derecho del mouse en el icono que aparece en la bandeja del sistema y selecciona Activar Dell Encryption.

  El proceso de activación inicial es el siguiente:

1. El usuario inicia sesión.
2. Al detectar un nuevo usuario (no administrado), se muestra el diálogo Activar. El usuario hace clic en **Cancelar**.
3. El usuario abre el cuadro de diálogo Acerca de Server Encryption para confirmar que se está ejecutando en modo Servidor.
4. El usuario hace clic con el botón derecho del mouse en el icono que aparece en la bandeja del sistema y selecciona **Activar Dell Encryption.**
5. El usuario introduce las credenciales de administrador de dominios en el diálogo Activar.

NOTA:
El requisito de credenciales de administrador de dominios es una medida de seguridad que impide que Server Encryption se extienda a otros entornos de servidores que no lo admiten. Para desactivar el requisito para credenciales de administrador de dominios, consulte Antes de empezar.

6 DDP Server comprueba las credenciales en el almacén de la empresa (Active Directory o equivalente) para verificar que las credenciales sean las credenciales de un administrador de dominios.

7 Un UPN se construye utilizando las credenciales.

8 Con el UPN, DDP Server crea una cuenta de usuario nueva para el usuario de servidor virtual y almacena las credenciales en el almacén de DDP 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 reinicia el equipo y comienza 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 reinicie el equipo, Server Encryption inicia sesión automáticamente como el usuario de servidor virtual, solicitando la clave de máquina del DDP Enterprise Server. Esto tiene lugar incluso antes de que cualquier usuario pueda iniciar sesión.

- Abra el cuadro de diálogo Acerca de para confirmar que Server Encryption está autenticado y en modo Servidor.
- Si la Id. de Shield está en rojo, el cifrado aún no se ha activado.
- En la Remote Management Console, 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.

    Consulte AdminHelp, disponible en la Remote Management Console para obtener los detalles sobre la política *Reintentar el intervalo tras un error de red*.

Proceso de activación de dispositivo y autenticación

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 El equipo comprueba su estado de activación de dispositivo con DDP Server:

- Si el equipo no tiene activación de dispositivo previa, DDP Server asigna al equipo un MCID, un DCID y un certificado de confianza, y almacena toda la información en el almacén de DDP Server.

- Si el equipo tiene activación de dispositivo previa, DDP Server verifica el certificado de confianza.

3 Después de que DDP 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.
- No se crea el archivo de registro de Encryption Removal Agent hasta después de que el servicio de Encryption Removal Agent se haya ejecutado, lo que ocurre después de reiniciar el equipo. Se eliminará permanentemente el archivo de registro, una vez que el cliente esté totalmente desinstalado y el equipo totalmente descifrado.
- La ruta de acceso del archivo de registro es C:\ProgramData\Dell\Dell Data Protection\Encryption.
- Cree la siguiente entrada de registro en el equipo destinado para el descifrado.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: sin registros

  1: registra errores que evitan la ejecución del servicio

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

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

  5: registra la información de depuración

Búsqueda de versión TSS

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

Interacciones entre EMS y PCS

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

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

Cifrar datos de escritura en medios de CD/DVD:

- Establecer EMS - Cifrar medios externos = Verdadero.

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

Uso de WSScan

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

Ejecutar WSScan

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

O bien

1 Haga clic en **Avanzado** para cambiar la vista a **Simple** para explorar una carpeta específica.
2 Vaya a Configuración de exploración e introduzca la ruta de acceso de la carpeta en el campo **Ruta de búsqueda**. Si se utiliza este campo, se ignora la selección realizada en el cuadro desplegable.
3 Si no desea escribir la salida de WSScan en un archivo, desactive la casilla de verificación **Salida a archivo**.
4 Cambie la ruta de acceso y el nombre de archivo predeterminados en *Ruta de acceso*, si lo desea.
5 Seleccione **Agregar a archivo existente** si no desea sobrescribir ningún archivo de salida de WSScan existente.
6 Seleccione el formato de salida:

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

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

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.
-f	Informar sobre el especificador de formato (Informar, Fijo, Delimitado)
-r	Ejecutar WSScan sin privilegios de administrador. **Algunos archivos pueden no estar visibles si se utiliza este modo.**
-u	Incluir archivos no cifrados en el archivo de salida. 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. **SysData:** clave de cifrado de SDE. **Usuario:** clave de cifrado de Encryption. **Común:** clave de cifrado común. WSScan no informa archivos cifrados mediante Encrypt for Sharing.
KCID	La Id. de equipo clave Como se muestra en el ejemplo anterior, "**7vdlxrsb**" Si se exploró una unidad de red asignada, el informe de exploración no proporciona una KCID.
UCID	La Id. del usuario. Como se muestra en el ejemplo anterior, "**_SDENCR_**" La UCID la comparten todos los usuarios de ese equipo.
Archivo	La ruta de acceso del archivo cifrado. Como se muestra en el ejemplo anterior, "**c: \temp\Dell: test.log**"
Algoritmo	El algoritmo de cifrado utilizado para cifrar el archivo. Como se muestra en el ejemplo anterior, "**todavía está cifrado según AES256**" RIJNDAEL 128 RIJNDAEL 256 AES 128 AES 256 3DES

Usar WSProbe

La utilidad de sondeo debe usarse con todas las versiones del cliente Encryption, con excepción de las políticas de EMS. Utilice la utilidad de sondeo para:

- Explorar o programar la exploración de un equipo cifrado. La utilidad de sondeo observa su política de prioridad de exploración 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 Verdadero. Si Explorar estación de trabajo al iniciar sesión está establecido como Verdadero, cuando un usuario inicie sesión, el cliente comparará cuántos archivos de carpetas cifradas actualmente (y previamente) están cifrados según las políticas de usuario, y realizará 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	Especificar, opcionalmente, una ruta de acceso concreta en el dispositivo que desea explorar en busca de 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 (seleccione Servicio > haga clic con el botón derecho del mouse > Actualizar) para actualizar el estado.

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

Solucionar problemas del cliente Advanced Threat Prevention

Buscar el código del producto con Windows PowerShell

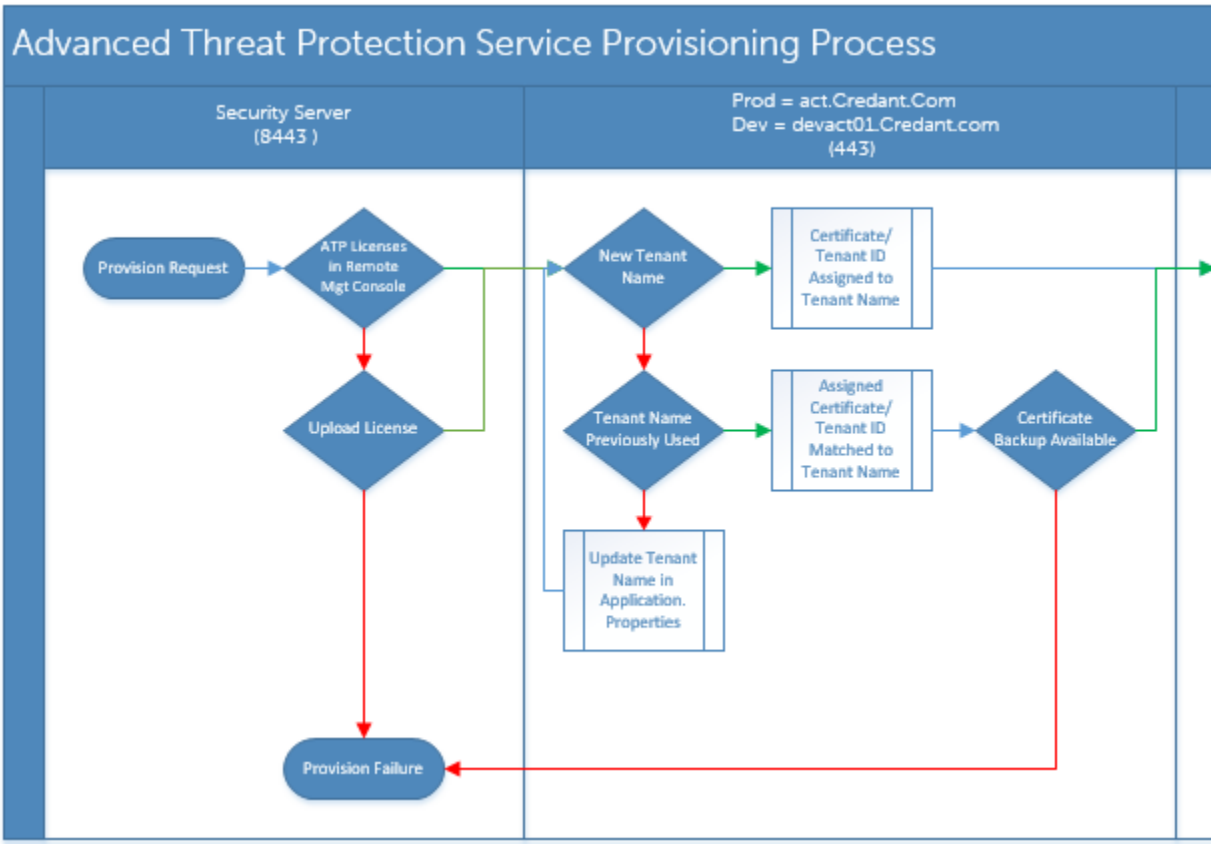
- Mediante este método, es muy sencillo identificar el código del producto si dicho código cambia más adelante.

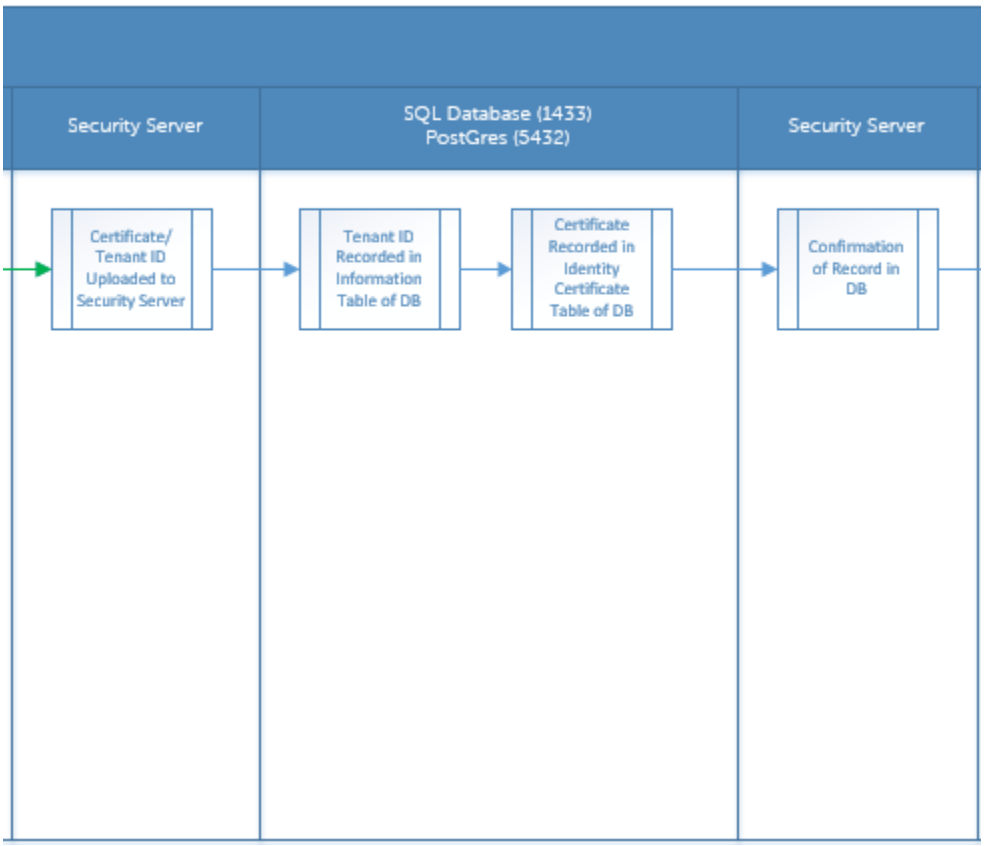
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

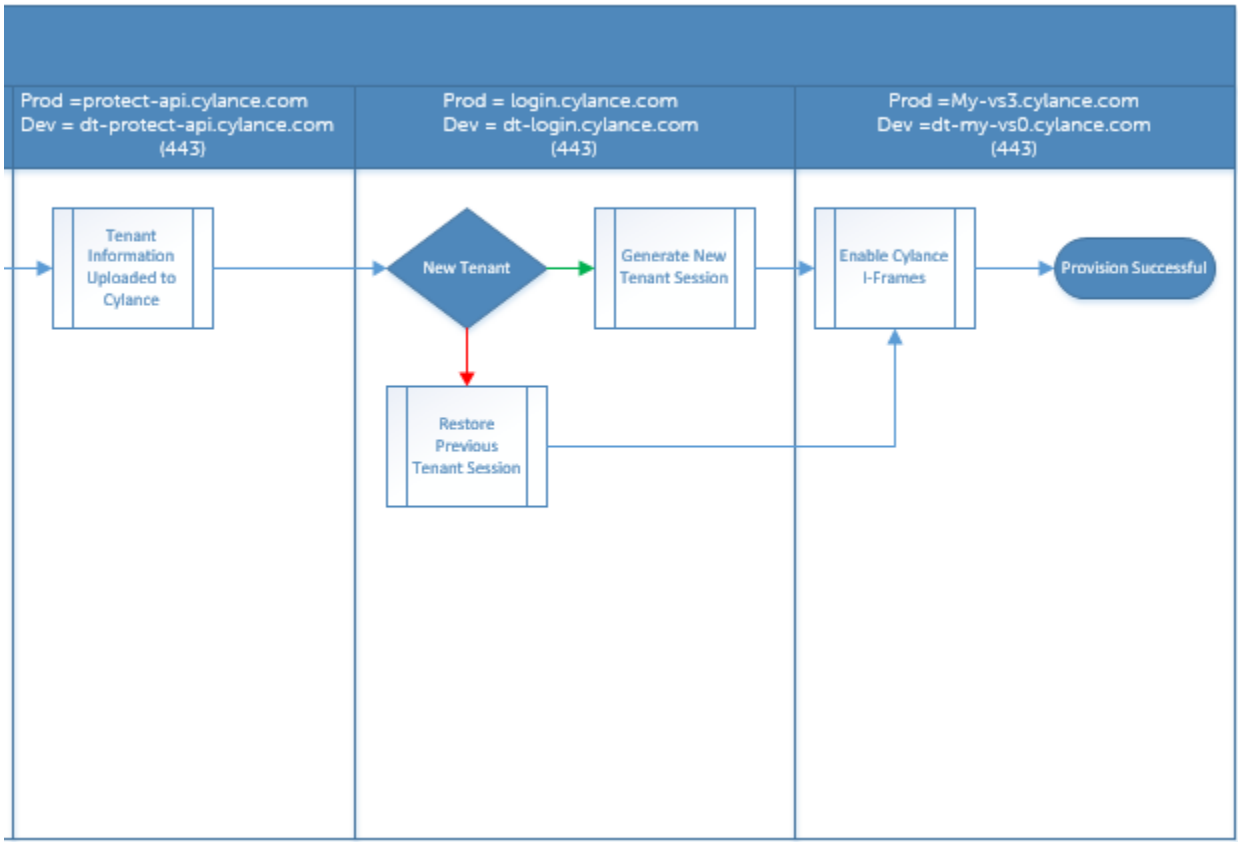
  La salida mostrará la ruta completa y el nombre del archivo .msi (el nombre convertido hexadecimal del archivo).

Comunicación de agentes y aprovisionamiento de Advanced Threat Prevention

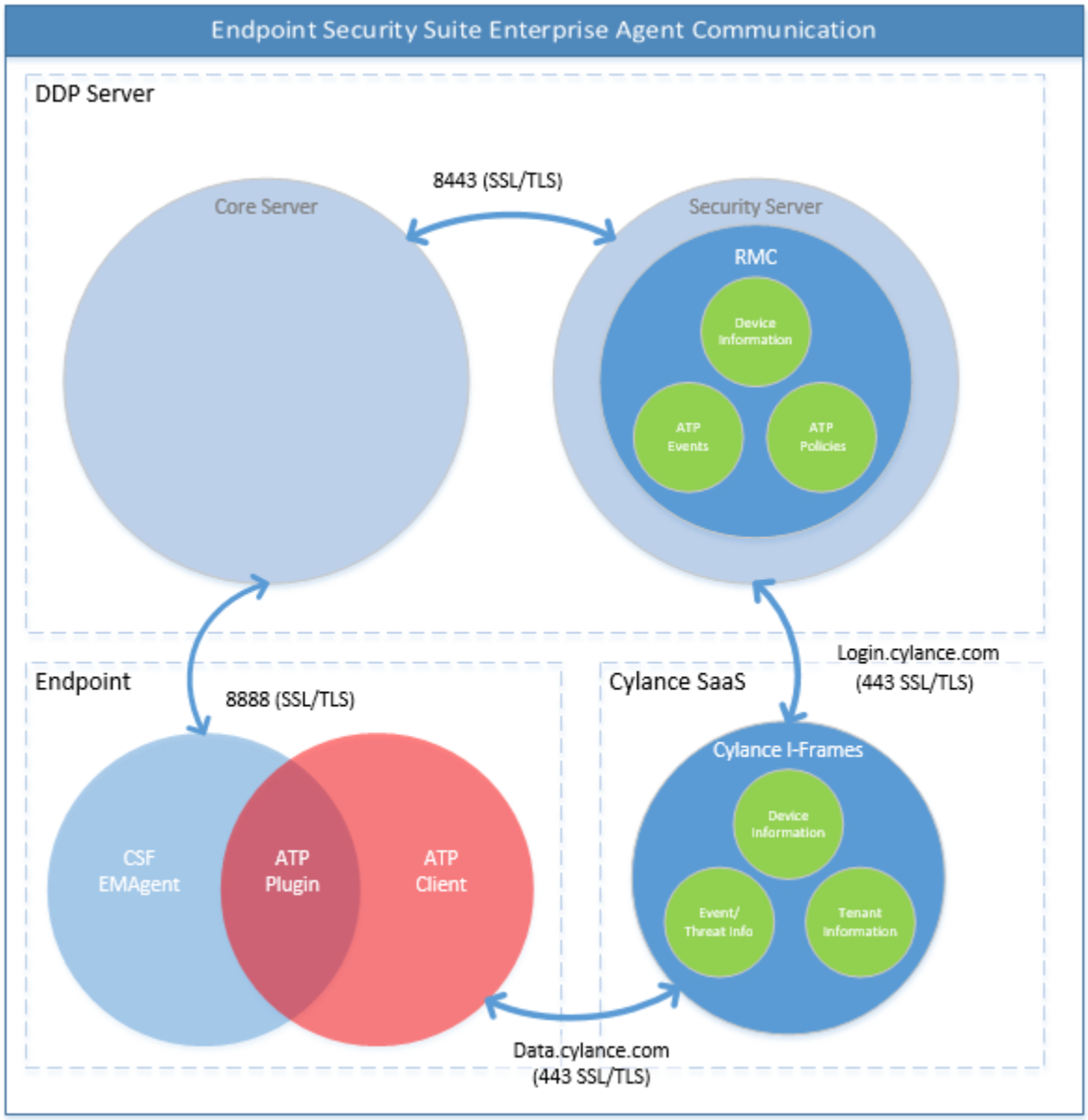
Los siguientes diagramas muestran el proceso de aprovisionamiento del servicio de Advanced Threat Prevention.


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB

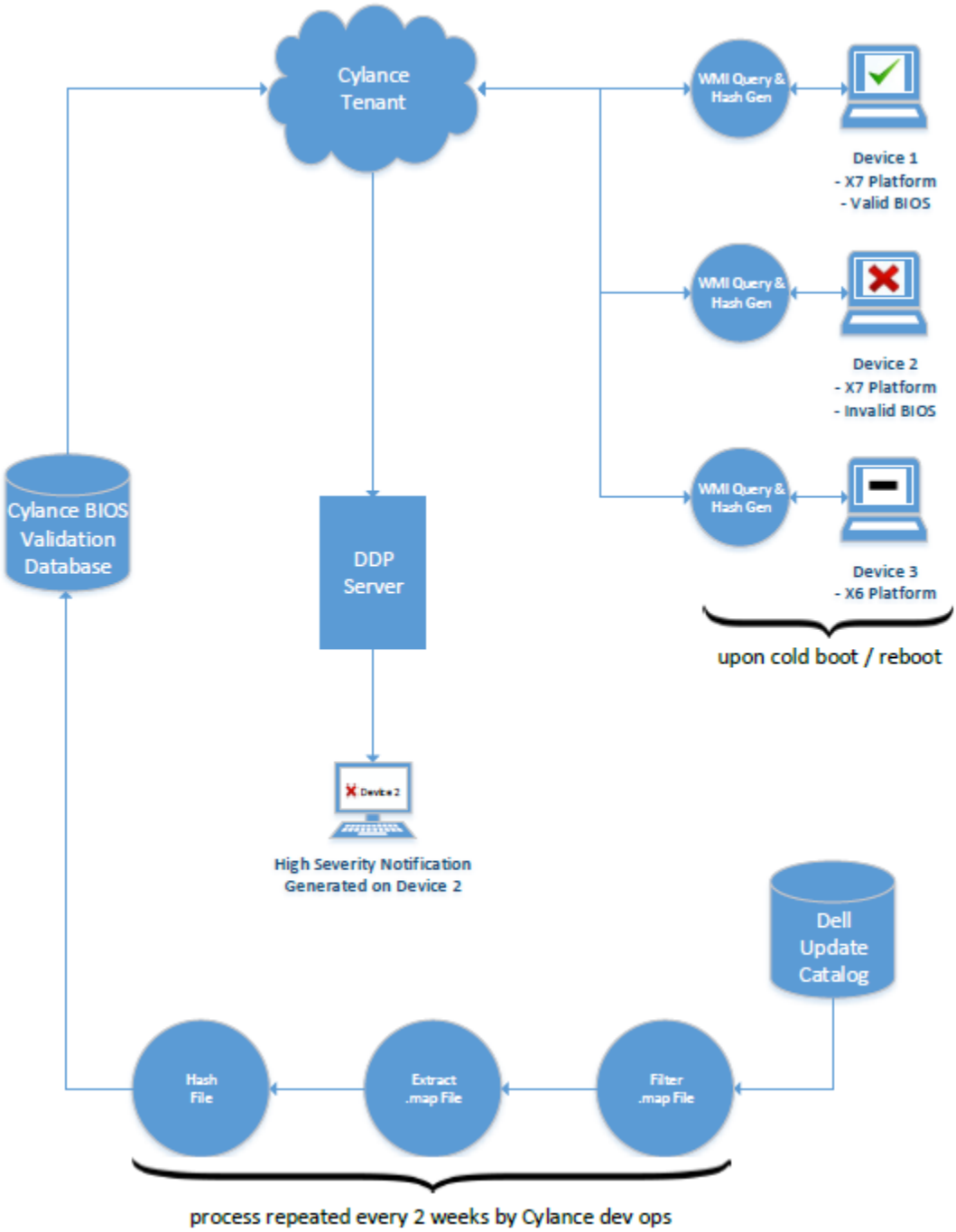


El siguiente diagrama muestra el proceso de comunicación de agentes de Advanced Threat Prevention.



Proceso de verificación de la integridad de la imagen del BIOS

El siguiente diagrama muestra el proceso de verificación de la imagen del BIOS. Para obtener una lista de los modelos de equipos de Dell compatibles con la verificación de la integridad de la imagen del BIOS, consulte Requisitos: Verificación de la integridad de la imagen del BIOS.



Resolución de problemas del cliente SED

Usar la política 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 a EE Server/VE 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 final se activa mediante el *Código de acceso inicial*, no quedará registro en EE Server/VE Server de que ese usuario se activó en este equipo. Por el contrario, no hay manera de generar un Código de respuesta desde EE Server/VE Server para el usuario final 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 mostrará **únicamente** en las circunstancias siguientes:
  - Un usuario nunca ha sido activado en la PBA.
  - El cliente no tiene conexión con la red o con EE Server/VE Server.

Usar el código de acceso inicial

1. Configure un valor para la política del **Código de acceso inicial** en la Remote Management Console.
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 azul**.
6. Cuando se muestre la pantalla Aviso legal, haga clic en **OK**.
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 la Security Console y compruebe que el usuario de PBA haya sido creado correctamente.

   Haga clic en **Registro** en el menú superior y busque el mensaje *Usuario de PBA creado para <dominio\nombre de usuario>*, que 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 al crear 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. (Solo Credant Manager) Responda a las solicitudes de preguntas y respuestas.

    Haga clic en la **flecha azul**.
12. 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 icono 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 con EE Server/VE Server. El archivo de registro contiene información para hacer un diagnóstico de los problemas de conectividad de EE Server/VE Server.
  - Aparece un error de autenticación aun cuando introduce las credenciales correctas. El archivo de registro, en conjunto con los registros de EE Server/VE 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 environment
```

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 el equipo e inicie sesión en la PBA. 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 actualizará y se grabará 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 support.dell.com.

2 Seleccione el modelo del equipo.

3 Seleccione **Controladores y descargas**.

4 Seleccione el **Sistema operativo** del equipo de destino.

5 Expanda la categoría **Seguridad**.

6 Descargue y guarde los controladores Dell ControlVault.

7 Descargue y guarde el firmware Dell ControlVault.

8 Si es necesario, copie el firmware y los controladores en los equipos de destino.

Instalación del controlador Dell ControlVault

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

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

:

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

Haga clic en **Continuar** para empezar.

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

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

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

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

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

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

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

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

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

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

Comprobación de la instalación del controlador

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

Instalación del firmware Dell ControlVault

1. Vaya hasta la carpeta en la que haya descargado el archivo para la instalación del firmware.
2. Haga doble clic sobre el firmware Dell ControlVault para iniciar el archivo ejecutable autoextraíble.
3. Haga clic en **Continuar** para empezar.
4. Haga clic en **Aceptar** para descomprimir los archivos del controlador en la ubicación predeterminada C:\Dell\Drivers\<Nueva carpeta>
5. Haga clic en **Sí** para permitir la creación de una nueva carpeta.
6. Haga clic en **Aceptar** cuando aparezca el mensaje correctamente descomprimido.
7. Tras la extracción, debería aparecer la carpeta que contiene los archivos. Si no aparece, vaya hasta la carpeta en la que haya extraído los archivos. Seleccione la carpeta **firmware**.
8. Haga doble clic en **ushupgrade.exe** para iniciar el instalador de firmware.
9. Haga clic en **Iniciar** para empezar la actualización del firmware.

:

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

Aparecerán varios mensajes de estado.

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

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

Equipos UEFI

Solución de problemas de conexiones de red

- Para que la autenticación previa al inicio sea correcta en un equipo con firmware UEFI, el modo 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. Si el procedimiento del equipo descrito en Configuración previa a la instalación para equipos UEFI es correcto y se configura adecuadamente, el icono de la conexión de red aparecerá en la pantalla de autenticación previa al inicio cuando el equipo esté conectado a la red.

- Compruebe que el cable de red esté conectado al equipo si el icono de conexión de red sigue sin aparecer durante la autenticación previa al inicio. 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 0x80280000	Se trata de una máscara de error para convertir los errores de hardware de TPM en errores de WIN.
TPM_E_AUTHFAIL 0x80280001	Error de autenticación.
TPM_E_BADINDEX 0x80280002	El índice a un PCR, DIR u otro registro es incorrecto.
TPM_E_BAD_PARAMETER 0x80280003	Uno o más parámetros son erróneos.
TPM_E_AUDITFAILURE 0x80280004	Una operación completada correctamente pero ha fallado la auditoría de dicha operación.
TPM_E_CLEAR_DISABLED 0x80280005	Se establece el marcador para deshabilitar borrados, por lo que ahora todas las operaciones de borrado requerirán el acceso físico.
TPM_E_DEACTIVATED 0x80280006	Activar el TPM.
TPM_E_DISABLED 0x80280007	Habilitar el TPM.
TPM_E_DISABLED_CMD 0x80280008	Se ha deshabilitado el comando de destino.
TPM_E_FAIL 0x80280009	Ha fallado la operación.
TPM_E_BAD_ORDINAL	El ordinal no se reconoce o no es consistente.

Constante/Valor	Descripción
0x8028000A	
TPM_E_INSTALL_DISABLED	La capacidad para instalar un propietario está deshabilitada.
0x8028000B	
TPM_E_INVALID_KEYHANDLE	No puede interpretarse el identificador de claves.
0x8028000C	
TPM_E_KEYNOTFOUND	El identificador de claves apunta a una clave no válida.
0x8028000D	
TPM_E_INAPPROPRIATE_ENC	Combinación de cifrado no aceptable.
0x8028000E	
TPM_E_MIGRATEFAIL	Error al autorizar la migración.
0x8028000F	
TPM_E_INVALID_PCR_INFO	No se puede interpretar la información de PCR.
0x80280010	
TPM_E_NOSPACE	No hay espacio para cargar la clave.
0x80280011	
TPM_E_NOSRK	No hay ninguna Clave raíz de almacenamiento (SRK) establecida.
0x80280012	
TPM_E_NOTSEALED_BLOB	Un blob cifrado no es válido o no fue creado por este TPM.
0x80280013	
TPM_E_OWNER_SET	El TPM ya tiene un propietario.
0x80280014	
TPM_E_RESOURCES	El TPM no tiene recursos internos suficientes para realizar la acción solicitada.
0x80280015	
TPM_E_SHORTRANDOM	Una cadena aleatoria es demasiado corta.
0x80280016	
TPM_E_SIZE	El TPM no cuenta con el espacio para realizar la operación.
0x80280017	
TPM_E_WRONGPCRVAL	El valor de PCR especificado no coincide con el valor de PRC actual.
0x80280018	
TPM_E_BAD_PARAM_SIZE	El argumento paramSize para el comando no es correcto

Constante/Valor	Descripción
0x80280019	
TPM_E_SHA_THREAD 0x8028001A	No hay ningún subproceso SHA-1 existente.
TPM_E_SHA_ERROR 0x8028001B	El cálculo no puede continuar por un error en el subproceso SHA-1 existente.
TPM_E_FAILEDSELFTEST 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 0x8028001D	Error al autorizar la segunda clave en una función de 2 claves.
TPM_E_BADTAG 0x8028001E	El valor de etiqueta enviado para un comando no es válido.
TPM_E_IOERROR 0x8028001F	Error de E/S al transmitir información al TPM.
TPM_E_ENCRYPT_ERROR 0x80280020	El proceso de descifrado tuvo un problema.
TPM_E_DECRYPT_ERROR 0x80280021	El proceso de descifrado no se completó.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Se usó un identificador no válido.
TPM_E_NO_ENDORSEMENT 0x80280023	El TPM no tiene ninguna Clave de aprobación (EK) instalada.
TPM_E_INVALID_KEYUSAGE 0x80280024	No se permite el uso de una clave.
TPM_E_WRONG_ENTITYTYPE 0x80280025	No se permite el tipo de entidad enviado.
TPM_E_INVALID_POSTINIT 0x80280026	El comando se recibió con una secuencia incorrecta, con respecto a TPM_Init y un TPM_Startup subsiguiente.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Los datos firmados no pueden incluir información DER adicional.

Constante/Valor	Descripción
TPM_E_BAD_KEY_PROPERTY 0x80280028	Las propiedades de clave en TPM_KEY_PARMs no son compatibles con este TPM.
TPM_E_BAD_MIGRATION 0x80280029	Las propiedades de migración de esta clave no son correctas.
TPM_E_BAD_SCHEME 0x8028002A	La firma o combinación de cifrado para esta clave no es correcta o no se permite en esta situación.
TPM_E_BAD_DATASIZE 0x8028002B	El tamaño del parámetro de datos (o blob) no es correcto o no es consistente con la clave especificada.
TPM_E_BAD_MODE 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 0x8028002D	El bit physicalPresence o el bit physicalPresenceLock tiene el valor incorrecto.
TPM_E_BAD_VERSION 0x8028002E	El TPM no puede realizar esta versión de funcionalidad.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	El TPM no permite las sesiones de transporte ajustadas.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	Error al construir la auditoría de TPM y el comando subyacente también devolvió un código de error.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	Error al construir la auditoría de TPM y el comando subyacente devolvió un código correcto.
TPM_E_NOTRESETABLE 0x80280032	Se intentó restablecer un registro PCR sin el atributo restablecible.
TPM_E_NOTLOCAL 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 0x80280034	El blob para hacer identidades no se escribió correctamente.
TPM_E_INVALID_RESOURCE 0x80280035	Al guardar el contexto, el tipo de recurso identificado no coincide con el recurso real.
TPM_E_NOTFIPS 0x80280036	El TPM intenta ejecutar un comando que solo está disponible en modo FIPS.

Constante/Valor	Descripción
TPM_E_INVALID_FAMILY 0x80280037	El comando intenta usar una Id. de familia no válida.
TPM_E_NO_NV_PERMISSION 0x80280038	El permiso para manipular el permiso no volátil no está disponible.
TPM_E_REQUIRES_SIGN 0x80280039	La operación requiere un comando firmado.
TPM_E_KEY_NOTSUPPORTED 0x8028003A	Operación incorrecta para cargar una clave no volátil.
TPM_E_AUTH_CONFLICT 0x8028003B	El blob NV_LoadKey requiere autorización tanto del propietario como del blob.
TPM_E_AREA_LOCKED 0x8028003C	El área no volátil está bloqueada y no se puede escribir en ella.
TPM_E_BAD_LOCALITY 0x8028003D	La localidad no es la correcta para la operación que se intentó.
TPM_E_READ_ONLY 0x8028003E	El área no volátil solo es de lectura y no se puede escribir en ella.
TPM_E_PER_NOWRITE 0x8028003F	No hay ninguna protección en el área no volátil de escritura.
TPM_E_FAMILYCOUNT 0x80280040	El valor de conteo de familia no coincide.
TPM_E_WRITE_LOCKED 0x80280041	Ya se escribió en el área no volátil.
TPM_E_BAD_ATTRIBUTES 0x80280042	Conflicto de atributos en el área no volátil.
TPM_E_INVALID_STRUCTURE 0x80280043	La etiqueta y versión de estructura no son válidas ni consistentes.
TPM_E_KEY_OWNER_CONTROL 0x80280044	La clave está bajo el control del Propietario de TPM, y solo dicho propietario la puede expulsar.
TPM_E_BAD_COUNTER 0x80280045	El identificador de contador no es correcto.

Constante/Valor	Descripción
TPM_E_NOT_FULLWRITE 0x80280046	La escritura no es una escritura completa del área.
TPM_E_CONTEXT_GAP 0x80280047	La separación entre los conteos de contexto guardado es demasiado grande.
TPM_E_MAXNVWRITES 0x80280048	Se superó el número máximo de escrituras no volátiles permitidas sin un propietario.
TPM_E_NOOPERATOR 0x80280049	No se estableció ningún valor de AuthData.
TPM_E_RESOURCEMISSING 0x8028004A	El recurso al que apunta el contexto no está cargado.
TPM_E_DELEGATE_LOCK 0x8028004B	La administración de delegación está bloqueada.
TPM_E_DELEGATE_FAMILY 0x8028004C	Se intentó administrar una familia diferente a la familia delegada.
TPM_E_DELEGATE_ADMIN 0x8028004D	La administración de la tabla de delegación no está habilitada.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Se ejecutó un comando fuera de una sesión exclusiva de transporte.
TPM_E_OWNER_CONTROL 0x8028004F	Se intentó guardar el contexto de una clave controlada expulsada por el propietario.
TPM_E_DAA_RESOURCES 0x80280050	El comando DAA no tiene recursos disponibles para ejecutar el comando.
TPM_E_DAA_INPUT_DATA0 0x80280051	Error en la comprobación de consistencia en el parámetro de DAA inputData0.
TPM_E_DAA_INPUT_DATA1 0x80280052	Error en la comprobación de consistencia en el parámetro de DAA inputData1.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	Error en la comprobación de consistencia en el parámetro de DAA issuerSettings.
TPM_E_DAA_TPM_SETTINGS 0x80280054	Error en la comprobación de consistencia en el parámetro de DAA tpmSpecific.

Constante/Valor	Descripción
TPM_E_DAA_STAGE 0x80280055	El proceso atómico indicado por el comando DAA enviado no es el esperado.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	La comprobación de validez del emisor ha detectado una incoherencia.
TPM_E_DAA_WRONG_W 0x80280057	Error en la comprobación de consistencia en w.
TPM_E_BAD_HANDLE 0x80280058	El identificador no es correcto.
TPM_E_BAD_DELEGATE 0x80280059	La delegación no es correcta.
TPM_E_BADCONTEXT 0x8028005A	El blob de contexto no es válido.
TPM_E_TOOMANYCONTEXTS 0x8028005B	El TPM administra demasiados contextos.
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	Error al validar la firma de autoridad de migración.
TPM_E_MA_DESTINATION 0x8028005D	El destino de migración no está autenticado.
TPM_E_MA_SOURCE 0x8028005E	El origen de migración no es correcto.
TPM_E_MA_AUTHORITY 0x8028005F	La autoridad de migración no es correcta.
TPM_E_PERMANENTEK 0x80280061	Se intentó revocar el EK, pero el EK no es revocable.
TPM_E_BAD_SIGNATURE 0x80280062	El vale CMK no tiene una firma correcta.
TPM_E_NOCONTEXTSPACE 0x80280063	No hay espacio en la lista de contextos para ningún contexto adicional.
TPM_E_COMMAND_BLOCKED 0x80280400	Se bloqueó el comando.

Constante/Valor	Descripción
TPM_E_INVALID_HANDLE 0x80280401	No se ha encontrado el identificador especificado
TPM_E_DUPLICATE_VHANDLE 0x80280402	El TPM devolvió un identificador duplicado, por lo que se deberá volver a enviar el comando.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	Se bloqueó el comando dentro del transporte.
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	El comando dentro del transporte no es compatible.
TPM_E_RETRY 0x80280800	El TPM está demasiado ocupado para responder al comando de inmediato, pero se podrá reenviar el comando más tarde.
TPM_E_NEEDS_SELFTEST 0x80280801	No se ha ejecutado SelfTestFull.
TPM_E_DOING_SELFTEST 0x80280802	El TPM está actualmente ejecutando una prueba automática completa.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	El TPM se está defendiendo contra ataques de diccionario y está en un periodo de tiempo de espera.
TBS_E_INTERNAL_ERROR 0x80284001	Se ha detectado un error de software interno.
TBS_E_BAD_PARAMETER 0x80284002	Uno o más parámetros de entrada son erróneos.
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Un puntero de salida especificado es erróneo.
TBS_E_INVALID_CONTEXT 0x80284004	El identificador de contexto especificado no hace referencia a ningún contexto válido.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Un búfer de salida especificado es demasiado pequeño.
TBS_E_IOERROR 0x80284006	Error al comunicarse con el TPM.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Uno o más parámetros de contexto son inválidos.

Constante/Valor	Descripción
TBS_E_SERVICE_NOT_RUNNING 0x80284008	El servicio TBS no está en ejecución y no se puede iniciar.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	No se puede crear un nuevo contexto porque ya hay demasiados contextos abiertos.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	No se puede crear un nuevo recurso virtual porque ya hay demasiados recursos virtuales abiertos.
TBS_E_SERVICE_START_PENDING 0x8028400B	El servicio TBS se inició pero todavía no está en ejecución.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	La interfaz de presencia física no es compatible.
TBS_E_COMMAND_CANCELED 0x8028400D	Se ha cancelado el comando.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	El búfer de salida o de entrada es demasiado grande.
TBS_E_TPM_NOT_FOUND 0x8028400F	No se puede encontrar en este equipo un dispositivo de seguridad de TPM compatible.
TBS_E_SERVICE_DISABLED 0x80284010	Se ha deshabilitado la configuración del servicio TBS.
TBS_E_NO_EVENT_LOG 0x80284011	No hay disponible ningún registro de eventos de TCG.
TBS_E_ACCESS_DENIED 0x80284012	El autor de la llamada no dispone de los permisos necesarios para realizar la operación solicitada.
TBS_E_PROVISIONING_NOT_ALLOWED 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 0x80284014	La interfaz de presencia física de este firmware no admite el método solicitado.

Constante/Valor	Descripción
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	No se encontró el valor OwnerAuth de TPM solicitado.
TBS_E_PROVISIONING_INCOMPLETE 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 0x80290100	El búfer de comando no está en el estado correcto.
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	El búfer de comando no contiene suficientes datos para atender la solicitud.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	Ya no caben más datos en el búfer de comando.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Al menos un parámetro de salida era NULL o no era válido.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Uno o más parámetros de entrada no son válidos.
TPMAPI_E_OUT_OF_MEMORY 0x80290105	No hay suficiente memoria para atender la solicitud.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	El búfer especificado es demasiado pequeño.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Se detectó un error interno.
TPMAPI_E_ACCESS_DENIED 0x80290108	El autor de la llamada no dispone de los permisos necesarios para realizar la operación solicitada.
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	La información de autorización especificada no es válida.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	El identificador de contexto especificado no es válido.
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Error al comunicarse con el TBS.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	El TPM devolvió un resultado inesperado.

Constante/Valor	Descripción
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	El mensaje es demasiado largo para la combinación de codificación.
TPMAPI_E_INVALID_ENCODING 0x8029010E	No se reconoce la codificación en el blob.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	El tamaño de clave no es válido.
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	Error en la operación de cifrado.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	La estructura de parámetros de clave no es válida
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	Los datos proporcionados que se solicitaron no parecen ser un blob válido de autorización de migración.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	El índice PCR especificado no es válido
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	Los datos proporcionados no parecen ser un blob válido de delegación
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Al menos uno de los parámetros de contexto especificados no es válido.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	Los datos proporcionados no parecen ser un blob válido de claves
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Los datos PCR especificados no son válidos..
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	El formato de los datos de autenticación de propietario no es válido.
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	El número aleatorio generado no aprobó la comprobación RNG de FIPS.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	El registro de eventos de TCG no contiene datos.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Una entrada del registro de eventos de TCG no es válida.

Constante/Valor	Descripción
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	No se encontró un separador de TCG.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Un valor implícito en una entrada del registro de TCG no coincidía con los datos con hash.
TPMAPI_E_POLICY_DENIES_OPERATION 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 0x80290200	El búfer especificado es demasiado pequeño.
TBSIMP_E_CLEANUP_FAILED 0x80290201	No se puede limpiar el contexto.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	El identificador de contexto especificado no es válido.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Se especificó un parámetro de contexto no válido.
TBSIMP_E_TPM_ERROR 0x80290204	Error al comunicarse con el TPM
TBSIMP_E_HASH_BAD_KEY 0x80290205	No se encontró ninguna entrada con la clave especificada.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	El identificador virtual especificado coincide con un identificador virtual ya en uso.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	El puntero a la ubicación de identificador devuelta era NULL o no era válida
TBSIMP_E_INVALID_PARAMETER 0x80290208	Uno o más parámetros no son válidos.
TBSIMP_E_RPC_INIT_FAILED 0x80290209	No se puede inicializar el subsistema RPC.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	El programador de TBS no está en ejecución.
TBSIMP_E_COMMAND_CANCELED 0x8029020B	Se ha cancelado el comando.

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

Constante/Valor	Descripción
TBSIMP_E_NO_EVENT_LOG 0x8029021B	No hay disponible ningún registro de eventos de TCG.
TPM_E_PPI_ACPI_FAILURE 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 0x80290301	El usuario no puede confirmar la solicitud de operación TPM.
TPM_E_PPI_BIOS_FAILURE 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 0x80290303	El BIOS no es compatible con la interfaz de presencia física.
TPM_E_PPI_BLOCKED_IN_BIOS 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 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 0x80290401	El dispositivo criptográfico de la plataforma no está listo actualmente. Necesita estar totalmente aprovisionado para poder funcionar.
TPM_E_PCP_INVALID_HANDLE 0x80290402	El identificador proporcionado al proveedor de servicios criptográficos de plataforma no es válido.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Un parámetro proporcionado al proveedor de servicios criptográficos de plataforma no es válido.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Una marca proporcionada al proveedor de servicios criptográficos de plataforma no es compatible.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	Este proveedor de servicios criptográficos de plataforma no admite la operación solicitada.
TPM_E_PCP_BUFFER_TOO_SMALL 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 0x80290407	Error interno inesperado en el proveedor de servicios criptográficos de plataforma.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Error en la autorización para usar un objeto de proveedor.

Constante/Valor	Descripción
TPM_E_PCP_AUTHENTICATION_IGNORED 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 0x8029040A	No se encontró la directiva a la que se hizo referencia.
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	No se encontró el perfil al que se hizo referencia.
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	La validación no ha sido correcta.
PLA_E_DCS_NOT_FOUND 0x80300002	No se encontró el Conjunto de recopiladores de datos.
PLA_E_DCS_IN_USE 0x803000AA	El Conjunto de recopiladores de datos o alguna de sus dependencias ya está en uso.
PLA_E_TOO_MANY_FOLDERS 0x80300045	No se puede iniciar el Conjunto de recopiladores de datos porque ya hay demasiadas carpetas.
PLA_E_NO_MIN_DISK 0x80300070	No hay suficiente espacio en disco para iniciar el Conjunto de recopiladores de datos.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	El Conjunto de recopiladores de datos ya existe.
PLA_S_PROPERTY_IGNORED 0x00300100	Se omitirá el valor de la propiedad.
PLA_E_PROPERTY_CONFLICT 0x80300101	Conflicto con el valor de la propiedad.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	La configuración actual de este Conjunto de recopiladores de datos requiere que contenga exactamente un recopilador de datos.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	Se requiere una cuenta de usuario para confirmar las propiedades del Conjunto de recopiladores de datos actual.
PLA_E_DCS_NOT_RUNNING 0x80300104	El Conjunto de recopiladores de datos no está en ejecución.
PLA_E_CONFLICT_INCL_EXCL_API 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.

Constante/Valor	Descripción
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	La ruta ejecutable especificada hace referencia a un recurso compartido de red o a una ruta UNC.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	La ruta ejecutable especificada ya está configurada para el seguimiento de APIs.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	La ruta de acceso ejecutable especificada no existe. Compruebe que sea correcta.
PLA_E_DC_ALREADY_EXISTS 0x80300109	El recopilador de datos ya existe.
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	Se agotó el tiempo de espera para notificar el inicio del Conjunto de recopilador de datos.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	Se agotó el tiempo de espera para que inicie el recopilador de datos.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	Se agotó el tiempo de espera para que la herramienta de generación de informes finalice.
PLA_E_NO_DUPLICATES 0x8030010D	No se permiten elementos duplicados.
PLA_E_EXE_FULL_PATH_REQUIRED 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 0x8030010F	El nombre de sesión proporcionado no es válido.
PLA_E_PLA_CHANNEL_NOT_ENABLED 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 0x80300111	El canal del registro de eventos Microsoft-Windows-TaskScheduler debe estar habilitado para realizar esta operación.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Error al ejecutar el Administrador de reglas.
PLA_E_CABAPI_FAILURE 0x80300113	Error al intentar comprimir o extraer los datos.
FVE_E_LOCKED_VOLUME 0x80310000	El Cifrado de unidad BitLocker está bloqueando esta unidad. Debe desbloquear la unidad desde el Panel de control.

Constante/Valor	Descripción
FVE_E_NOT_ENCRYPTED 0x80310001	La unidad no está cifrada.
FVE_E_NO_TPM_BIOS 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 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 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 0x80310005	El sector de arranque de esta unidad 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_WRONG_BOOTMGR 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 0x80310007	Se requiere al menos un protector de clave segura para realizar esta operación.
FVE_E_NOT_ACTIVATED 0x80310008	Cifrado de unidad BitLocker no está habilitado en esta unidad. Active BitLocker.
FVE_E_ACTION_NOT_ALLOWED 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 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 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 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 0x8031000D	El atributo leído de Active Directory no contiene ningún valor. Puede que la información de recuperación de BitLocker falte o esté dañada.

Constante/Valor	Descripción
FVE_E_AD_ATTR_NOT_SET 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 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 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 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.
FVE_E_SYSTEM_VOLUME 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 0x80310013	La unidad no se puede cifrar porque no se admite el sistema de archivos.
FVE_E_BAD_PARTITION_SIZE 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 0x80310015	Esta unidad no se puede cifrar.
FVE_E_BAD_DATA 0x80310016	Los datos no son válidos.
FVE_E_VOLUME_NOT_BOUND 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 0x80310018	Debe inicializar el TPM para poder utilizar Cifrado de unidad deBitLocker.
FVE_E_NOT_DATA_VOLUME 0x80310019	La operación que se intentó no se puede realizar en una unidad del sistema operativo.
FVE_E_AD_INSUFFICIENT_BUFFER 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 0x8031001B	Error en una operación de lectura al convertir la unidad. No se convirtió la unidad. Vuelva a habilitar BitLocker.

Constante/Valor	Descripción
FVE_E_CONV_WRITE 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 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 0x8031001E	Cifrado de unidad BitLocker no admite configuraciones en clúster.
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	La unidad especificada ya está configurada para desbloquearse automáticamente en el equipo actual.
FVE_E_OS_NOT_PROTECTED 0x80310020	Cifrado de unidad BitLocker no protege a la unidad del sistema operativo.
FVE_E_PROTECTION_DISABLED 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 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 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 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 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 0x80310026	El algoritmo de cifrado de unidad no se puede usar en este tamaño de sector.
FVE_E_FAILED_AUTHENTICATION 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 0x80310028	La unidad especificada no es la unidad del sistema operativo.
FVE_E_AUTOUNLOCK_ENABLED 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.

Constante/Valor	Descripción
FVE_E_WRONG_BOOTSECTOR 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 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 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 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.
FVE_E_CANNOT_ENCRYPT_NO_KEY 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 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 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 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 0x80310033	El protector de clave especificado no se encontró en la unidad. Intente usar otro protector de clave.
FVE_E_INVALID_KEY_FORMAT 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 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 0x80310036	Error en la prueba de comprobación del generador de números aleatorios.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 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

Constante/Valor	Descripción
	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 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 0x80310039	La unidad debe estar totalmente descifrada para poder completar esta operación.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	El protector de clave especificado no se puede usar para esta operación.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	No hay ningún protector de clave en la unidad para poder realizar la prueba de hardware.
FVE_E_KEYFILE_NOT_FOUND 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 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 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 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 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 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.

Constante/Valor	Descripción
FVE_E_TPM_NO_VMK 0x80310042	No se puede obtener la clave de cifrado de BitLocker a partir del Módulo de plataforma segura (TPM).
FVE_E_PIN_INVALID 0x80310043	No se puede obtener la clave de cifrado de BitLocker a partir del MTP y PIN.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	Se modificó una aplicación de arranque después de haberse habilitado Cifrado de unidad BitLocker.
FVE_E_AUTH_INVALID_CONFIG 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 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 en contacto con el administrador del dominio para obtener más información.
FVE_E_FS_NOT_EXTENDED 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 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 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 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 0x8031004B	La unidad no se puede bloquear mientras se está usando.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	El token de acceso asociado con el subproceso actual no es un token suplantado.
FVE_E_DRY_RUN_FAILED 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 0x8031004E	Debe reiniciar el equipo antes de continuar con Cifrado de unidad BitLocker.
FVE_E_DEBUGGER_ENABLED 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	No se realizó ninguna acción ya que el Cifrado de unidad BitLocker está en modo de acceso sin procesar.

Constante/Valor	Descripción
0x80310050	
FVE_E_RAW_BLOCKED 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 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 0x80310053	Cifrado de unidad BitLocker se puede usar solo en aprovisionamientos limitados o para la recuperación cuando el equipo se ejecuta en entornos de preinstalación o recuperación.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	La clave maestra de desbloqueo automático no estaba disponible en la unidad del sistema operativo.
FVE_E_MOR_FAILED 0x80310055	El firmware del sistema no pudo habilitar el borrado de la memoria del sistema al reiniciar el equipo.
FVE_E_HIDDEN_VOLUME 0x80310056	No se puede cifrar la unidad oculta.
FVE_E_TRANSIENT_STATE 0x80310057	Se omitieron las claves de cifrado de BitLocker porque la unidad se encontraba en un estado transitorio.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	No se permiten protectores basados en claves públicas en esta unidad.
FVE_E_VOLUME_HANDLE_OPEN 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 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 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 0x8031005C	La configuración de la directiva de grupo no permite la creación de una contraseña de recuperación.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	La configuración de la directiva de grupo requiere la creación de una contraseña de recuperación.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	La configuración de la directiva de grupo no permite la creación de una clave de recuperación.

Constante/Valor	Descripción
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	La configuración de la directiva de grupo requiere la creación de una clave de recuperación.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 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 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 0x80310062	La configuración de la directiva de grupo no permite el uso de una clave de inicio. Elija otra opción de inicio de BitLocker.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 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 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 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 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 0x80310068	El PIN proporcionado no cumple los requisitos de longitud mínima o máxima.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 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 0x8031006A	La configuración de la directiva de grupo no permite la creación de una contraseña.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	La configuración de la directiva de grupo requiere la creación de una contraseña.
FVE_E_FIPS_PREVENTS_PASSPHRASE 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 0x8031006D	No se puede agregar una contraseña a la unidad del sistema operativo.

Constante/Valor	Descripción
FVE_E_INVALID_BITLOCKER_OID 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 0x8031006F	La unidad es demasiado pequeña para protegerse con Cifrado de unidad BitLocker.
FVE_E_DV_NOT_SUPPORTED_ON_FS 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 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.
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 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 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 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 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 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 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 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 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 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.

Constante/Valor	Descripción
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 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 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 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.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 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 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 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 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 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 0x80310089	La virtualización solicitada es demasiado grande.

Constante/Valor	Descripción
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 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 0x80310091	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 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 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 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 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 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 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 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 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 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.

Constante/Valor	Descripción
FVE_E_INVALID_PIN_CHARS 0x8031009A	El PIN de TPM solicitado contiene caracteres no válidos.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	La información de administración almacenada en la unidad contenía un tipo desconocido. Si usa una versión anterior de Windows, intente obtener acceso a la unidad desde la versión más reciente.
FVE_E_EFI_ONLY 0x8031009C	La característica solo se admite en sistemas EFI.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Se encontró más de un certificado de protector de clave de red en el sistema.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	La eliminación del certificado de protector de clave de red debe realizarse mediante el complemento Certificados.
FVE_E_INVALID_NKP_CERT 0x8031009F	Se encontró un certificado no válido en el almacén de certificados de protector de clave de red.
FVE_E_NO_EXISTING_PIN 0x803100A0	Esta unidad no está protegida con un PIN.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Escriba el PIN actual correcto.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 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 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 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 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 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 0x803100A7	La unidad no admite la longitud de la de clave de autenticación requerida.
FVE_E_NO_EXISTING_PASSPHRASE	Esta unidad no está protegida con una contraseña.

Constante/Valor	Descripción
0x803100A8	
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Escriba la contraseña actual correcta.
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	La contraseña no puede superar los 256 caracteres.
FVE_E_NO_PASSPHRASE_WITH_TPM 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 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 0x803100AD	Este comando solo se puede ejecutar desde el nodo del coordinador del volumen CSV especificado.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Este comando no se puede ejecutar en un volumen si forma parte de un clúster.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 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 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 0x803100B1	La configuración de la directiva de grupo no permite el uso de cifrado basado en hardware.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	La unidad especificada no admite el uso de cifrado basado en hardware.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	BitLocker no se puede actualizar durante el cifrado o descifrado del disco.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	Los volúmenes de detección no se admiten en volúmenes que usan cifrado de hardware.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	No se detectó un teclado de prearranque. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	No se detectó teclado de prearranque o entorno 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	La configuración de la directiva de grupo requiere la creación de un PIN de inicio, pero no hay ningún teclado de prearranque disponible

Constante/Valor	Descripción
0x803100B7	en el 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 0x803100B8	La configuración de la directiva de grupo requiere la creación de una contraseña de recuperación, pero no hay ni teclado prearranque ni entorno de recuperación de Windows disponibles en el dispositivo. Es posible que el usuario no pueda especificar la información necesaria para desbloquear el volumen.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	Actualmente no se está eliminando el espacio disponible.
FVE_E_SECUREBOOT_DISABLED 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 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 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 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 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 0x803100BF	El firmware del equipo no puede admitir el cifrado de hardware.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 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 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 0x803100C2	BitLocker no puede guardar la contraseña de recuperación porque la cuenta Microsoft especificada está suspendida.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	BitLocker no puede guardar la contraseña de recuperación porque la cuenta Microsoft especificada está bloqueada.
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 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.

Constante/Valor	Descripción
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Este equipo no puede admitir el cifrado del dispositivo porque hay volúmenes de datos fijos sin cifrar.
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Este equipo no cumple con los requisitos de hardware necesarios para admitir el cifrado del dispositivo.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Este equipo no puede admitir el cifrado del dispositivo porque WinRE no está configurado correctamente.
FVE_E_DE_PROTECTION_SUSPENDED 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 0x803100C9	Este equipo no está aprovisionado para admitir el cifrado del dispositivo.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	Se ha desencadenado el bloqueo del dispositivo debido a demasiados intentos de contraseña incorrectos.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 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 0x803100CC	El PIN solo puede incluir números del 0 al 9.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	BitLocker no puede usar la protección de reproducción de hardware porque no hay contadores disponibles en su PC.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Error de validación de estado de bloqueo de dispositivo debido a contadores no coincidentes.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	El búfer de entrada es demasiado grande.

18

Glosario

Activar: la activación se produce cuando el equipo se ha registrado en Dell Enterprise Server/VE y ha recibido 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.

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

Advanced Threat Prevention: el producto Advanced Threat Prevention constituye la protección antivirus de próxima generación, que utiliza ciencia algorítmica y aprendizaje automático para identificar, clasificar y evitar que se ejecuten amenazas cibernéticas, conocidas o desconocidas, y que estas amenazas causen daños a los extremos. La función opcional de servidor de seguridad del cliente supervisa la comunicación entre el equipo y los recursos en la red y en Internet, e intercepta comunicaciones potencialmente maliciosas. La función opcional de protección web bloquea los sitios web y descargas no seguros durante la navegación y las búsquedas en línea, según las clasificaciones de seguridad y los informes de sitios web.

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

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

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

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

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

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

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

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

Contraseña de un solo uso (OTP): una Contraseña de un solo uso es una contraseña que se puede utilizar solamente una vez y es válida durante un periodo de tiempo limitado. OTP requiere que haya un TMP presente, habilitado y con propietario. Para habilitar OTP, se asocia un dispositivo móvil con el equipo mediante la Security Console y la aplicación Security Tools Mobile. La aplicación Security Tools Mobile genera la contraseña en el dispositivo móvil que se utiliza para iniciar sesión en el equipo en la pantalla de inicio de sesión de Windows. En función de la política, es posible que la función OTP se utilice para recuperar el acceso al equipo si la contraseña ha caducado o se ha olvidado, si la OTP no ha sido utilizada para iniciar sesión en el equipo. La función OTP se puede utilizar para la autenticación o la recuperación, pero no para ambas cosas. La seguridad OTP supera la de otros métodos de autenticación ya que la contraseña generada se puede utilizar una sola vez y se vence en un periodo corto de tiempo.

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

Control de script: el control de script protege los dispositivos mediante el bloqueo de la ejecución de scripts maliciosos.

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

Usuario del servidor: Dell Server Encryption crea una cuenta de usuario virtual con el propósito de administrar claves de cifrado y actualizaciones de políticas. Esta cuenta de usuario no se corresponde con ninguna otra cuenta de usuario en el equipo 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 UCID exclusivo en Dell Enterprise Server/VE Remote Management Console.

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

interfieren de manera alguna con el registro de inicio maestro. Cuando el equipo arranca, los archivos cifrados están disponibles antes del inicio de sesión de los usuarios (a fin de activar la administración de revisiones, SMS y las herramientas de copias de seguridad y de recuperación). La deshabilitación del cifrado SDE desencadena el descifrado automático de todos los archivos y directorios cifrados de SDE de los usuarios correspondientes, sin tener en cuenta las otras políticas de SDE, como las Reglas de cifrado de SDE.

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

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. Al ejecutar Dell Data Encryption, el cifrado de usuario se convierte en cifrado común. Existe una excepción para dispositivos de medios externos; cuando se insertan en un servidor con Encryption instalado, los archivos se cifran con la clave de Usuario en roaming.