Dell Data Protection | Endpoint Security Suite

Guía de instalación básica v1.7

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 básica de Endpoint Security Suite

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción

En esta guía se explica cómo instalar y configurar la aplicación mediante el instalador maestro de ESS . En esta guía se ofrece asistencia para la instalación básica. Consulte la *Advanced Installation Guide* (Guía de instalación avanzada) si necesita información sobre la instalación de los instaladores secundarios, la configuración de EE Server/VE Server o información más completa que la asistencia básica con el instalador maestro ESS .

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 Lea detenidamente el capítulo Requisitos de este documento.

3 Implemente los clientes en los usuarios finales.

Utilización de esta guía

Use esta guía en el orden siguiente.

- Consulte Requisitos para conocer los requisitos previos de los clientes.
- Seleccione una de las opciones siguientes:
  - Instalación interactiva mediante el instalador maestro de ESS

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

Cómo ponerse en contacto con Dell ProSupport

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

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

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

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

2

Requisitos

Todos los clientes

- 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 ESS 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 ESS. 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 ESS. 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 EncryptionThreat Protection, y BitLocker Manager son compatibles con la Interfaz de usuario multilingüe (MUI) y admiten los idiomas siguientes.

Compatibilidad de idiomas

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

- 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.
- 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 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.
- 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 ESS instala Microsoft Visual C++ 2012 actualización 4 si todavía no está instalada en el servidor.

Requisito previo

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

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 Threat Protection

- Los clientes Threat Protection no se pueden instalar sin que el cliente Encryption se haya detectado en el equipo. Si se intenta, fallará la instalación.
- Para instalar Threat Protection correctamente, el equipo debe tener conexión de red.
- Desinstale las aplicaciones antivirus, antimalware, antispyware y de servidor de seguridad de otros proveedores antes de instalar los clientes Threat Protection para evitar errores de instalación. El software en conflicto no incluye Windows Defender ni Endpoint Security Suite.
- La función de protección web solo es compatible con Internet Explorer.

Sistemas operativos del cliente Threat Protection

- 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

Puertos del cliente Threat Protection

- Para asegurar que los clientes Threat Protection reciben las actualizaciones más recientes de Threat Protection, los puertos 443 y 80 deben estar disponibles para que el cliente se comunique con los distintos servidores de destino. Si los puertos están bloqueados por cualquier motivo, no se podrán descargar las actualizaciones de firma del antivirus (archivos DAT), 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	Notas
Actualizaciones del antivirus	HTTP	TCP	443/reserva 80	vs.mcafeeasap.com	Saliente	
Motor antivirus/ Actualizaciones de firma	SSL	TCP	443	vs.mcafeeasap.com	Saliente	
Motor contra el correo electrónico no deseado	HTTP	TCP	443	vs.mcafeeasap.com	Saliente	
Reglas contra el correo electrónico no deseado y actualizaciones de transmisiones	HTTP	TCP	80	vs.mcafeeasap.com	Saliente	Tipos de paquete: X-SU3X-SU3-Component-Name

Utilizar	Protocolo de aplicación	Protocolo de transporte	Número de puerto	Destino	Dirección	Notas
						X-SU3-Component-Type X-SU3-Status
Servicios de reputación	SSL	TCP	443	tunnel.web.trustedsource.org	Saliente	
Comentarios de los servicios de reputación	SSL	TCP	443	gtifeedback.trustedsource.org	Saliente	
Administrador de la cuarentena	HTTP HTTPS	TCP	80 443	Su EE Server/VE Server	Bidireccional	
Actualización de la base de datos de reputación de la URL	HTTP	TCP	80	list.smartfilter.com	Saliente	
Búsqueda de reputación de la URL	SSL	TCP	443	tunnel.web.trustedsource.org	Saliente	

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.

Requisitos previos del cliente SED

- El instalador maestro de ESS instala Microsoft Visual C++2010 SP1 **y** Microsoft Visual C++ 2012 actualización 4 si todavía no están instalados en el equipo.

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

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.

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

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.
- 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.

Requisitos previos del cliente BitLocker Manager

- El instalador maestro de ESS instala Microsoft Visual C++2010 SP1 **y** Microsoft Visual C++ 2012 actualización 4 si todavía no están instalados en el equipo.

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)

Sistemas operativos Windows

- Windows Server 2016

Instalación mediante el instalador maestro de ESS

- 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 ESS.
- 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* para obtener información sobre el uso de estas funciones de Advanced Authentication y Threat Protection. Puede acceder a esta ayuda desde **<Dir. instalación>:\Program Files\Dell\Dell Data Protection\Endpoint Security Suite\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 ESS instala todo el conjunto de productos. Existen dos métodos para realizar la instalación con el instalador maestro de ESS. Elija una de las siguientes opciones.
  - Instalación interactiva mediante el instalador maestro de ESS

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

Instalación interactiva mediante el instalador maestro de ESS

- El instalador maestro de ESS 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 de forma interactiva mediante el instalador maestro de ESS . 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 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.

> **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 Advanced Threat Prevention, descargue la Endpoint Security Suite Enterprise Advanced Installation Guide (Guía de instalación avanzada de Endpoint Security Suite Enterprise) 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 ESS

- 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 ESS .

Modificador	Descripción
-y -gm2	Extracción previa del instalador maestro de ESS. Los modificadores -y y -gm2 deben utilizarse juntos. No los separe.
/s	Instalación silenciosa
/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 ESS . El instalador maestro de ESS no puede excluir 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. DE-ATP = Threat Protection y Encryption. DE = Drive Encryption (cliente Encryption) BLM = BitLocker Manager SED = administración de unidades de autocifrado (controladores EMAgent/Manager, PBA/GPE)
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.
- Este ejemplo instala todos los componentes mediante el instalador maestro de ESS 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\""
```

- Este ejemplo instala Threat Protection y Encryption ***solo*** con el instalador maestro de ESS 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-TP\""
```

- Este ejemplo instala Threat Protection, Encryption y SED Management con el instalador maestro de ESS, 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=DE-TP, SED,
SUPPRESSREBOOT=1\""
```

-

Desinstalación mediante el instalador maestro de ESS

- Cada componente debe desinstalarse por separado, seguido de la desinstalación del instalador maestro de ESS. 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 ESS para obtener instaladores secundarios.
- Asegúrese de que para la desinstalación se ha utilizado como instalación la misma versión del instalador maestro de ESS (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 ESS.
- Desinstale los clientes en el siguiente orden.

  a Desinstalación de clientes Threat Protection.

  b Desinstalación del cliente Encryption.

  c Desinstalación de los clientes SED y Advanced Authentication.

  d Desinstalación del cliente BitLocker Manager.
- Continúe con Desinstalación del instalador maestro de ESS.

Desinstalación del instalador maestro de ESS

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

Desinstalación con la línea de comandos

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

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

  Reinicie el equipo cuando finalice.

5

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 ESS, como se muestra en Extracción de los instaladores secundarios del instalador maestro de ESS 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 clientes Threat Protection

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESS, el instalador del cliente Threat Protection 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 Threat Prevention
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Luego:
- El siguiente ejemplo desinstala el cliente Threat Protection .

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

Desinstalación de los clientes 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

- 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.

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro de ESS, 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.
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 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 ESSE , el instalador del cliente SED se encuentra en C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- Una vez extraído el instalador maestro de ESS , 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 ESS , 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.

Extracción de instaladores secundarios del instalador maestro de ESS

- El instalador maestro de ESS no es un *desinstalador* maestro. Cada cliente debe desinstalarse por separado, seguido por la desinstalación del instalador maestro de ESS. Utilice este proceso para extraer los clientes del instalador maestro de ESS 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.

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.
- 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”).

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.

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.

Solución de problemas

Todos los clientes: Solución de problemas

- Los archivos de registro del instalador del maestro de **ESS** 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

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.

Interacciones entre EMS y PCS

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

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

Cifrar datos de escritura en medios de CD/DVD:

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

Uso de WSScan

- WSScan le permite asegurarse de que todos los datos se descifran al desinstalar el cliente Encryption, así como ver el estado de cifrado e identificar los archivos no cifrados que se deben cifrar.

- Se requieren privilegios de administrador para ejecutar esta utilidad.

Ejecutar WSScan

1 Desde el medio de instalación de Dell, copie WSScan.exe en el equipo de Windows que desea explorar.

2 Inicie la línea de comandos en la ubicación anterior e introduzca **wsscan.exe** en el símbolo del sistema. Se inicia WSScan.

3 Haga clic en **Avanzado**.

4 Seleccione el tipo de unidad que desea explorar desde el menú desplegable: *Todas las unidades, Unidades fijas, Unidades extraíbles o CD-ROM/ DVD-ROM*.

5 Seleccione el tipo de informe de Encryption en el menú desplegable: *archivos cifrados*, *archivos sin cifrar*, *todos los archivos* o *archivos sin cifrar en infracción*:

   - *Archivos cifrados*: para garantizar que todos los datos se descifran cuando se desinstala el cliente Encryption. Siga el actual proceso para el descifrado de datos, como la emisión de la actualización de una política de descifrado. Después de descifrar los datos, pero antes de proceder al reinicio para la desinstalación, ejecute WSScan a fin de asegurarse de que todos los datos hayan sido descifrados.
   - *Archivos no cifrados*: para identificar archivos que no están cifrados, con una indicación de si los archivos se deben cifrar (Y/N).
   - *Todos los archivos*: para generar una lista de todos los archivos cifrados y no cifrados, con una indicación de si los archivos se deben cifrar (Y/N).
   - *Archivos sin cifrar en infracción*: para identificar los archivos que no están cifrados y se deben cifrar.

6 Haga clic en **Buscar**.

O bien

1 Haga clic en **Avanzado** para cambiar la vista a **Simple** para explorar una carpeta específica.

2 Vaya a Configuración de exploración e introduzca la ruta de acceso de la carpeta en el campo **Ruta de búsqueda**. Si se utiliza este campo, se ignora la selección realizada en el cuadro desplegable.

3 Si no desea escribir la salida de WSScan en un archivo, desactive la casilla de verificación **Salida a archivo**.

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

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

6 Seleccione el formato de salida:

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

7 Haga clic en **Buscar**.

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

Salida de WSScan

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

Ejemplo de salida:

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

Salida	Significado
Sello con la fecha/hora	La fecha y la hora en la que se exploró el archivo.
Tipo de cifrado	El tipo de cifrado utilizado para cifrar el archivo.

Salida	Significado
	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

Comprobación del estado de Encryption Removal Agent

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

- **En espera de desactivación de SDE**: el cliente Encryption aún está instalado, configurado, o ambos. El descifrado no se inicia hasta que el cliente Encryption se haya desinstalado.
- **Barrido inicial**: el servicio está realizando un barrido inicial, calculando el número de archivos cifrados y los bytes. El barrido inicial se produce una sola vez.
- **Barrido de descifrado**: el servicio está descifrando archivos y posiblemente solicitando el descifrado de archivos bloqueados.
- **Descifrar al reiniciar (parcial)**: el barrido de descifrado ha terminado y en el próximo reinicio se descifrarán algunos archivos (no todos) bloqueados.
- **Descifrar al reiniciar**: el barrido de descifrado ha terminado y todos los archivos bloqueados se descifrarán en el próximo reinicio.
- **No se han podido descifrar todos los archivos**: el barrido de descifrado ha terminado pero no se han podido descifrar todos los archivos. Este último estado significa que ocurrió una de las siguientes situaciones:
  - No se pudo programar el descifrado de los archivos bloqueados porque eran demasiado grandes, o porque se produjo un error al hacer la solicitud de desbloqueo.
  - Se produjo un error entrada/salida durante el cifrado de los archivos.

- No se pudieron descifrar los archivos debido a una política.
- Los archivos están marcados como deben ser cifrados.
- Se produjo un error durante el barrido de descifrado.
- Cualquiera que sea el caso, se crea un archivo de registro (si llevar un registro está configurado) cuando la configuración sea LogVerbosity=2 (o superior). Para solucionar problemas, configure LogVerbosity en 2 y reinicie Encryption Removal Agent Service a fin de forzar otro barrido de descifrado.

- **Completado**: el barrido de descifrado se ha completado. El Servicio, el ejecutable, el controlador y el ejecutable del controlador están programados para ser eliminados en el siguiente reinicio.

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.

Glosario

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

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.

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.

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.

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.

Threat Protection: el producto Threat Protection se basa en políticas administradas de forma centralizada que protegen los equipos de empresa frente a las amenazas a la seguridad. Threat Protection se compone de: protección contra malware y comprobaciones para detectar posibles virus, spyware, programas no deseados y otras amenazas explorando elementos automáticamente cuando se accede a ellos o cuando se basa en programas definidos en una política. - 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. - Protección web: bloquea los sitios web y descargas no seguros durante la navegación en línea y las búsquedas, según las clasificaciones de seguridad y los informes para los sitios web.