Endpoint Security Suite Enterprise

Guía de instalación básica v2.1

Notas, precauciónes y advertencias

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

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

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

2018 - 11

Rev. A01

Contenido

1

Introducción

Esta guía detalla cómo instalar y configurar la aplicación mediante el instalador maestro de Endpoint Security Suite Enterprise. En esta guía se ofrece asistencia para la instalación básica. Consulte la *Guía de instalación avanzada* si necesita información sobre cómo instalar los instaladores secundarios, la configuración de Servidor de administración de seguridad/Servidor virtual de administración de seguridad o información más allá de la asistencia básica para el instalador maestro de Endpoint Security Suite Enterprise.

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

Antes de empezar

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

   - *Security Management ServerServidor de administración de seguridad* (Guía de instalación y migración de Security Management Server)
   - *Security Management Server VirtualServidor virtual de administración de seguridad* (Guía de inicio rápido y guía de instalación de Security Management Server Virtual)
   - Compruebe que las políticas están establecidas de la forma deseada. Explore la ayuda AdminHelp, disponible a través del signo **?** que se encuentra en la esquina superior derecha de la pantalla. AdminHelp es una ayuda a nivel de página diseñada para ayudarlo a definir y modificar las políticas y conocer qué opciones tiene disponibles en el Dell Server.

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

3 Lea detenidamente el capítulo Requisitos de este documento.

4 Implemente los clientes en los usuarios.

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

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

Cómo ponerse en contacto con Dell ProSupport

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

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

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

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

2

Requisitos

Todos los clientes

- Durante la implementación se deberán seguir las prácticas recomendadas para TI. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados, para las pruebas iniciales e implementaciones escalonadas para los usuarios.
- La cuenta de usuario que realiza la instalación/actualización/desinstalación debe ser un usuario administrador local o de dominio, que se puede designar temporalmente mediante una herramienta de implementación como Microsoft SCCM o Quest 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.
- Los administradores deben asegurarse de que todos los puertos necesarios estén disponibles.
- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.
- **NOTA: La línea de productos Dell Data Security no admite versiones de Windows Insider Preview.**

Todos los clientes: Requisitos previos

- El instalador maestro instala los siguientes requisitos previos si todavía no se encuentra instalado en la computadora.

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

Visual C++ 2015 requiere la actualización de Windows KB2999226 si está instalado en Windows 7.

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

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.

Todos los clientes: Hardware

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

Hardware
– Procesador Intel Pentium o AMD
– 500 MB de espacio disponible en el disco
– 2 GB RAM

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

Todos los clientes: localización

- Los clientes Encryption, Advanced Threat Prevention y BitLocker Manager son compatibles con la Interfaz de usuario multilingüe (MUI) y están localizados en los idiomas siguientes. El cifrado de disco completo solo se admite en sistemas operativos en inglés. Los datos de Advanced Threat Prevention aparecen en la consola de administración 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)

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 valida con los proveedores de antivirus líderes del sector. Se aplican exclusiones no modificables para estos proveedores de antivirus con el fin de evitar incompatibilidades entre la detección del antivirus y el cifrado. El cliente Encryption también se ha probado con el kit de herramientas Microsoft Enhanced Mitigation Experience Toolkit.

  Si su empresa utiliza un proveedor antivirus que no se encuentra incluido, consulte http://www.dell.com/support/article/us/en/19/SLN288353/ o póngase en contacto con Dell ProSupport para obtener asistencia.
- No se admite la reinstalación del sistema operativo en el lugar. Para volver a instalar el sistema operativo, realice una copia de seguridad del equipo de destino, borre el equipo, instale el sistema operativo y, a continuación, recupere los datos cifrados siguiendo los procedimientos de recuperación establecidos.

Requisitos previos del cliente Encryption

Sistemas operativos del cliente Encryption

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 con plantilla de compatibilidad de aplicaciones
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)
- VMware Workstation 12.5 y superior

Sistemas operativos Windows (de 32 y 64 bits)

NOTA:
Cuando se utiliza el modo UEFI, la política de hibernación protegida no es compatible.

Sistemas operativos de cliente Encryption con activación aplazada

- La activación aplazada permite que la cuenta de usuario de Active Directory que se utiliza durante la activación sea independiente de la cuenta utilizada para iniciar sesión en el extremo. En lugar de que el proveedor de red capture la información de autenticación, el usuario especifica manualmente la cuenta basada en Active Directory cuando se le solicite. Una vez que se ingresan las credenciales, la información de autenticación se envía de forma segura al Dell Server, el cual la valida comparándola con los dominios configurados de Active Directory. Para obtener más información, consulte http://www.dell.com/support/article/us/en/19/sln306341.
- La tabla siguiente indica los sistemas operativos compatibles con activación aplazada.

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 con plantilla de compatibilidad de aplicaciones
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)

Sistemas operativos Medios externos de cifrado

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

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

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 con plantilla de compatibilidad de aplicaciones
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)

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

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

Cifrado de disco completo

El cifrado de disco completo **solo** puede instalarse a través de una interfaz de línea de comandos (CLI). Si desea instalar el cifrado de disco completo, descargue la guía de instalación avanzada de Endpoint Security Suite Enterprise para obtener instrucciones.

- El cifrado de disco completo requiere activación en un servidor Dell que ejecute la versión 9.8.2 o posterior.
- Full Disk Encryption no es compatible actualmente dentro de equipos host virtualizados.
- Los cifrados de Full Disk de las configuraciones de varias unidades no son compatibles.
- Los proveedores de credenciales de terceros no funcionarán con las funciones de FDE instaladas, mientras que todos los proveedores de credenciales de terceros se deshabilitarán cuando se habilite la PBA.
- La computadora cliente debe tener conectividad de red o un código de acceso para activarse.
- La computadora debe contar con una conexión de red con cable para que un usuario con tarjeta inteligente pueda iniciar sesión mediante la Autenticación previa al inicio (PBA) por primera vez.
- Las actualizaciones de funciones del sistema operativo no admiten el cifrado de disco completo.
- Se requiere una conexión por cable para que PBA pueda comunicarse con el servidor Dell.
- No puede haber un SED presente en la computadora de destino.
- El cifrado de disco completo no es compatible con BitLocker o BitLocker Manager. No instale el cifrado de disco completo en una computadora donde esté instalado BitLocker o BitLocker Manager.
- Cualquier unidad NVMe que se utilice para PBA: el funcionamiento SATA de BIOS se debe establecer en RAID encendido, ya que PBA Management de Dell no es compatible con AHCI en unidades NVMe.
- Cualquier unidad NVMe que se utilice para PBA: el modo de inicio de BIOS debe ser UEFI y deben estar desactivada las ROM de opción heredadas.
- Cualquier unidad no NVMe que se utilice para PBA: el funcionamiento SATA de BIOS se debe establecer en AHCI, ya que PBA Management de Dell no es compatible con RAID con unidades que no sean NVMe.
  - No se admite RAID Encendido porque el acceso a los datos de lectura y escritura relacionados con RAID (en un sector que no está disponible en una unidad bloqueada que no sea NVMe) no está accesible en el inicio y no puede esperar para leer estos datos hasta después de que el usuario haya iniciado sesión.
  - El sistema operativo se bloqueará cuando se cambie de RAID Encendido > AHCI si los controladores de la controladora AHCI no están previamente instalados. Para obtener instrucciones sobre cómo cambiar de RAID > AHCI (o viceversa), consulte http://www.dell.com/support/article/us/en/19/SLN306460.

    Dell recomienda que la versión del controlador Intel Rapid Storage Technology se 15.2.0.0 o posterior, con unidades NVMe.
- 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 de cifrado de disco completo no es compatible con las configuraciones de inicio dual, dado que es posible cifrar archivos de sistema del otro sistema operativo, lo cual podría interferir en su funcionamiento.
- No se admite la reinstalación del sistema operativo en el lugar. Para volver a instalar el sistema operativo, realice una copia de seguridad del equipo de destino, borre el equipo, instale el sistema operativo y, a continuación, recupere los datos cifrados siguiendo los procedimientos de recuperación establecidos.
- **NOTA: Es necesario el uso de una contraseña en la Autenticación previa al inicio (PBA). Dell recomienda realizar una configuración mínima de la contraseña para que cumpla con las políticas de seguridad internas.**

NOTA: El cifrado de disco completo debe estar configurado con algoritmos de cifrado definidos en AES 256 y con el modo de cifrado configurado en CBC.

Requisitos previos del cliente de cifrado de disco completo

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

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.

Hardware del cliente de cifrado de disco completo

- La siguiente tabla indica el hardware compatible.

Hardware integrado opcional
– TPM 1.2 o 2.0

Sistemas operativos del cliente de cifrado de disco completo

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate (modo de arranque heredado requerido)
– Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4) (modo de arranque de la UEFI requerido)

Cliente Advanced Threat Prevention

- Para completar la instalación de Advanced Threat Prevention cuando el Dell Server que administra al cliente se está ejecutando en el modo Conectado (predeterminado), la computadora debe tener conexión a la red. Sin embargo, ***no*** se requiere conectividad a la red para la instalación de Advanced Threat Prevention cuando el Dell Server que administra se está ejecutando en modo Desconectado.
- Para aprovisionar un inquilino para Advanced Threat Prevention, el Dell Server debe tener conectividad con Internet.
- Las funciones opcionales de Firewall de cliente y Protección web ***no*** deben instalarse en computadoras cliente administradas por el Dell Server ejecutándose en el modo Desconectado.
- Es posible que las aplicaciones de antivirus, antimalware y antispyware de otros proveedores entren 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 agregar exclusiones para Advanced Threat Prevention en el Dell Server y también para otras aplicaciones. Para obtener instrucciones sobre cómo agregar exclusiones para Advanced Threat Prevention en el Dell Server, consulte http://www.dell.com/support/article/us/en/04/SLN300970. Para obtener una lista de exclusiones a fin de agregarlas al resto de las aplicaciones de antivirus, consulte http://www.dell.com/support/article/us/en/04/sln301562.

Sistemas operativos de Advanced Threat Prevention

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows Embedded Standard 7

Sistemas operativos Windows (de 32 y 64 bits)

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)
- Windows Server 2008 R2
- 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

Para obtener información sobre las direcciones URL que se utilizan, consulte: http://www.dell.com/support/article/us/en/19/SLN303898

Verificación de la integridad de la imagen del BIOS

Si la política *Habilitar la garantía de BIOS* se selecciona en la consola de administración, el inquilino Cylance valida un hash del BIOS en computadoras terminales para asegurarse de que el BIOS no se haya 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 Dell Server y el administrador de TI recibe un mensaje de alerta en la consola de administración. 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

Clientes servidor de seguridad del cliente y protección web

- Para instalar el servidor de seguridad del cliente y protección web correctamente, la computadora debe tener conectividad a la red.
- Desinstale las aplicaciones antivirus, antimalware, antispyware y de servidor de seguridad de otros proveedores antes de instalar los clientes servidor de seguridad del cliente y protección web para evitar errores de instalación. El software en conflicto no incluye Windows Defender ni Endpoint Security Suite Enterprise.
- La función de protección web solo es compatible con Internet Explorer.

Sistemas operativos del servidor de seguridad del cliente y del cliente de protección web

- La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (de 32 y 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows 8: Enterprise, Pro
– Windows 8.1: Enterprise, Pro
– Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/Redstone 4)

Puertos de los clientes servidor de seguridad del cliente y protección web

- Para garantizar que los clientes servidor de seguridad del cliente y protección web reciban las actualizaciones más recientes de Client Firewall y Web 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
Servicios de reputación	SSL	TCP	443	tunnel.web.trustedsource.org	Saliente	
Comentarios de los servicios de reputación	SSL	TCP	443	gtifeedback.trustedsource.org	Saliente	
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.
- La computadora debe contar con una conexión de red con cable para que un usuario con tarjeta inteligente pueda iniciar sesión mediante la Autenticación previa al inicio (PBA) por primera vez.
- Los proveedores de credenciales de terceros no funcionarán con SED Management instalado, mientras que todos los proveedores de credenciales de terceros se deshabilitarán cuando se habilite la PBA.
- No es compatible con IPv6.
- SED Manager no es compatible con configuraciones de varias unidades.
- SED Manager no es compatible actualmente dentro de equipos host virtualizados.
- Recuerde que deberá apagar y reiniciar el equipo después de aplicar las políticas y cuando estén listas para comenzar a aplicarlas.
- Los equipos que cuentan con unidades de cifrado automático no se pueden utilizar con tarjetas HCA. Existen incompatibilidades que impiden el aprovisionamiento del HCA. Dell no vende equipos que tengan unidades de cifrado automático compatibles con el módulo HCA. Esta configuración incompatible será una configuración realizada poscompra.
- Si el equipo marcado para cifrado incluye unidad de cifrado automático, asegúrese de que Active Directory tenga deshabilitada la opción *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*. La Autenticación previa al 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 se bloqueará cuando se cambie de *RAID=On* a *AHCI*.

- La configuración de unidades de autocifrado para SED Management de Dell difiere entre las unidades NVMe y las que no son NVMe (SATA), como se indica a continuación.
  - Cualquier unidad NVMe que se utiliza como una SED: el funcionamiento SATA de BIOS se debe establecer en RAID Encendido, ya que SED Management de Dell no es compatible con AHCI en unidades NVMe.
  - Cualquier unidad NVMe que se utiliza como una SED: el modo de inicio de BIOS debe ser UEFI y deben estar desactivada las ROM de opción heredadas.
  - Cualquier unidad que no sea NVMe que se utiliza como una SED: el funcionamiento SATA de BIOS se debe establecer en AHCI, ya que SED Management de Dell no es compatible con RAID con unidades que no sean NVMe.
    - No se admite RAID Encendido porque el acceso a los datos de lectura y escritura relacionados con RAID (en un sector que no está disponible en una unidad bloqueada que no sea NVMe) no está accesible en el inicio y no puede esperar para leer estos datos hasta después de que el usuario haya iniciado sesión.
    - El sistema operativo se bloqueará cuando se cambie de RAID Encendido > AHCI si los controladores de la controladora AHCI no están previamente instalados. Para obtener instrucciones sobre cómo cambiar de RAID > AHCI (o viceversa), consulte http://www.dell.com/support/article/us/en/19/SLN306460.

  Las SED compatibles que cumplen con OPAL necesitan controladores actualizados Intel Rapid Storage Technology, que se pueden encontrar en http://www.dell.com/support. Dell recomienda que la versión del controlador Intel Rapid Storage Technology se 15.2.0.0 o posterior, con unidades NVMe.

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

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

- **NOTA: Es necesario el uso de una contraseña en la Autenticación previa al inicio (PBA). Dell recomienda realizar una configuración mínima de la contraseña para que cumpla con las políticas de seguridad internas.**

Hardware del cliente SED

Teclados internacionales del cliente SED

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

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

Localización del cliente SED

El cliente SED es compatible con una Interfaz de usuario multilingüe (MUI) y se puede localizar en los siguientes idiomas. El modo UEFI y la autenticación previa al inicio tienen soporte en los siguientes idiomas **excepto** en ruso, chino tradicional o chino simplificado.

Compatibilidad de idiomas	
• Inglés (EN)	• Coreano (KO)
• Francés (FR)	• Chino simplificado (ZH-CN)
• Italiano (IT)	• Chino tradicional /Taiwán (ZH-TW)
• Alemán (DE)	• Portugués brasileño (PT-BR)

Compatibilidad de idiomas

- Español (ES)
- Japonés (JA)
- Portugués europeo (PT-PT)
- Ruso (RU)

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, Ultimate (compatibles con el modo de arranque heredado, pero no UEFI)

  NOTA:
  Unidades NVMe con autocifrado no son compatibles con Windows 7.

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

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.
- Es necesario un Dell Server para utilizar BitLocker Manager.
- Asegúrese de que hay un certificado de firma disponible en la base de datos. Para obtener más información, consulte http://www.dell.com/support/article/us/en/19/sln307028.
- El teclado, el mouse y los componentes de video deben estar conectados directamente al equipo. No use un conmutador KVM para administrar los periféricos, ya que el conmutador KVM puede interferir 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.
- BitLocker Manager no es compatible con Server Encryption ni con Advanced Threat Prevention en un sistema operativo de servidor.

Hardware del cliente BitLocker Manager

- La siguiente tabla indica el hardware compatible.

Hardware integrado opcional

- TPM 1.2 o 2.0

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: Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (April 2018 Update/ Redstone 4)
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

No se deben instalar las actualizaciones de Windows KB3133977 y KB3125574 si instala BitLocker Manager en Windows 7.

Instalación mediante el instalador maestro

- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Para instalar mediante puertos no predeterminados, utilice los instaladores secundarios en lugar del instalador maestro.
- Los archivos de registro del instalador maestro Endpoint Security Suite Enterprise se euentran 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 *Dell Encrypt Help* (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 *Medios externos de cifrado Help* (Ayuda de Encryption External Media) para saber cómo usar las funciones de Medios externos de cifrado. 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 y Advanced Threat Prevention. Acceda a la ayuda en **<Install dir>:\Program Files\Dell\Dell Data Protection\Client Security Framework\Help**.
- Los usuarios deben actualizar sus políticas haciendo clic con el botón secundario en el icono de Dell Encryption del área de notificación y seleccionando **Comprobar si existen actualizaciones de políticas** una vez finalizada la instalación.
- El instalador maestro instala todo el conjunto de productos. Existen dos métodos para realizar la instalación con el instalador maestro. Elija una de las siguientes opciones.
  - Instalación interactiva mediante el instalador maestro

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

Instalación interactiva mediante el instalador maestro

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

1. Localice el archivo **DDSSuite.exe** en el medio de instalación de Dell. Cópielo al equipo local.
2. Haga doble clic en **DDSSuite.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 *Nombre de Dell Management Server local*, introduzca el nombre completo del host del Dell Server para administrar el usuario de destino, por ejemplo, servidor.organización.com.

   En *URL de Dell Device Server*, introduzca la dirección URL del Dell Server con la que se comunicará el cliente.

   El formato es https://server.organization.com:**8443**/xapi**/** (incluida la barra diagonal 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 la infraestructura de seguridad subyacente.

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 Prevention 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: Si intenta instalar la función opcional Advanced Threat Prevention en la actualización Windows 10 October 2018 Update (Redstone 5) o posterior, se mostrará una advertencia de incompatibilidad.

NOTA: Si intenta instalar las funciones opcionales de protección web y firewall en la actualización Windows 10 October 2018 Update (Redstone 5) o posterior, se mostrará una advertencia de incompatibilidad.

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

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

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

La instalación ha finalizado.

Instalación mediante la línea de comandos con el instalador maestro

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

Modificadores

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

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

NOTA: Advanced Threat Prevention no es compatible con la actualización Windows 10 October 2018 Update (Redstone 5) o posterior.

Modificador	Descripción
-y -gm2	Extracción previa del instalador maestro de Endpoint Security Suite Enterprise. Los modificadores -y y -gm2 deben utilizarse juntos. No los separe.
/S	Instalación silenciosa
/z	Envía las variables al archivo .msi dentro de DDSSuite.exe

Parámetros

- En la siguiente tabla se describen los parámetros que se pueden utilizar con el instalador maestro de Endpoint Security Suite Enterprise. El instalador maestro de Endpoint Security Suite Enterprise no puede excluir los componentes individuales, pero puede recibir comandos para especificar qué componentes se deben instalar.

Parámetro	Descripción
SUPPRESSREBOOT	Suprime el reinicio automático al terminar la instalación. Se puede utilizar en modo SILENCIOSO.
SERVER	Especifica la dirección URL del Dell Server.
InstallPath	Indica la ruta de la instalación. Se puede utilizar en modo SILENCIOSO.
FEATURES	Especifica los componentes que se pueden instalar en modo SILENCIOSO. ATP = Advanced Threat Prevention *solamente* DE-ATP = Advanced Threat Prevention y Encryption. Es la opción de instalación predeterminada si no se especifica el parámetro FUNCIONES DE = cliente del cifrado de disco solamente BLM = BitLocker Manager SED = SED Management (controladores EMAgent/Manager, PBA/GPE)(Disponible solo cuando se instala en un sistema operativo de estación de trabajo) ATP-WEBFIREWALL = Advanced Threat Prevention con el firewall de cliente y protección web DE-ATP-WEBFIREWALL = Encryption y Advanced Threat Prevention con el firewall de cliente y protección web **NOTA: Para actualizaciones de Encryption Enterprise o de 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 Protección web. No especifique ATP-WEBFIREWALL o DE-ATP-WEBFIREWALL cuando instale un cliente administrado por el Dell Server 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) En este ejemplo se instalan todos los componentes mediante el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de manera silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de estación de trabajo) En este ejemplo se instalan Advanced Threat Prevention y Encryption ***solo*** con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de estación de trabajo) En este ejemplo se instalan Advanced Threat Prevention, Encryption y SED Management con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, con un reinicio menos, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de estación de trabajo) En este ejemplo se instalan Advanced Threat Prevention, Encryption, Web Protection y Client Firewall con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de servidor) En este ejemplo se instalan Advanced Threat Prevention y Encryption ***solo*** con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de servidor) En este ejemplo se instalan Advanced Threat Prevention, Encryption, Web Protection y Client Firewall con el instalador maestro de Endpoint Security Suite Enterprise de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\

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

- (En un sistema operativo de servidor) En este ejemplo se instala Advanced Threat Prevention ***solo*** con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

- (En un sistema operativo de servidor) En este ejemplo se instala Encryption ***solo*** con el instalador maestro de Endpoint Security Suite Enterprise en puertos estándar, de forma silenciosa, en la ubicación predeterminada C:\Program Files\Dell\Dell Data Protection\, y se configura para utilizar el Dell Server especificado.

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

4

Desinstalación del instalador maestro

- Dell recomienda utilizar el Desinstalador de Data Security para eliminar la suite de Data Security.
- Cada componente se debe desinstalar por separado, seguido de la desinstalación del instalador maestro de Endpoint Security Suite Enterprise . Los clientes se deben desinstalar en un **orden específico para evitar errores en la desinstalación**.
- Siga las instrucciones en Extracción de instaladores secundarios del instalador maestro para obtener instaladores secundarios.
- Asegúrese de que se utilice la misma versión de instalador maestro de Endpoint Security Suite Enterprise (y, por lo tanto, los clientes) tanto para la desinstalación como la instalación.
- Este capítulo le remite a otros capítulos que contienen instrucciones *detalladas* sobre cómo desinstalar los instaladores secundarios. En este capítulo **solo** se explica el último paso, la desinstalación del instalador maestro .
- Desinstale los clientes en el siguiente orden.

  a Desinstalación del cliente Encryption.

  b Desinstalación de Advanced Threat Prevention.

  c Desinstalación del cliente SED (se desinstala Dell Encryption Management Agent, que no se puede desinstalar hasta que se haya desinstalado Advanced Threat Prevention).

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

Desinstalar el instalador maestro de Endpoint Security Suite Enterprise

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

Desinstalación con la línea de comandos

- En el siguiente ejemplo se desinstala en forma silenciosa el instalador maestro de Endpoint Security Suite Enterprise.

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

  Reinicie el equipo cuando finalice.

5

Desinstalación mediante los instaladores secundarios

- Dell recomienda utilizar el Desinstalador de Data Security para eliminar la suite de Data Security.
- Para desinstalar cada cliente por separado, en primer lugar es necesario extraer los archivos ejecutables secundarios del instalador maestro de Endpoint Security Suite Enterprise, como se muestra en Extracción de los instaladores secundarios del instalador maestro En forma alternativa, 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 ingresarse entre comillas de texto sin formato.
/s	Modo silencioso
/x	Modo de desinstalación
/a	Instalación administrativa (se copian todos los archivos en el .msi)

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

Opción	Significado
/q	Sin diálogo de progreso; se reinicia automáticamente tras completar el proceso
/qb	Diálogo de progreso con botón **Cancelar** , indica que es necesario reiniciar

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 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.
- Dell Encryption y Encryption External Media actualizan el Dell Server para cambiar el estado de este a *Desprotegido* al principio de un proceso de desinstalación de Cliente Encryption. Sin embargo, en caso de que el cliente no se pueda comunicar con el Dell Server, el estado no se podrá actualizar, independientemente del motivo. En este caso, deberá *Quitar el terminal* manualmente en la consola de administración. Si su empresa utiliza este flujo de trabajo por razones de cumplimiento de normal, Dell recomienda comprobar que se haya configurado el estado *Desprotegido* de la manera esperada, en la consola de administración o en Compliance Reporter.

Proceso

- Key Server (y Servidor de administración de seguridad) debe estar configurado antes de la desinstalación si utiliza la opción **Descargar claves del Encryption Removal Agent del servidor**. Consulte Configurar Key Server para la desinstalación de cliente Encryption activado en Security Management Server para obtener instrucciones. No se necesitan acciones si el cliente que vaya a realizar la desinstalación se activa en un Servidor virtual de administración de seguridad, ya que Servidor virtual de administración de seguridad 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 que el instalador maestro se extrae del Endpoint Security Suite Enterprise, el instalador del cliente Encryption se puede encontrar en **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.
- La tabla a continuación indica los parámetros disponibles para la desinstalación.

Parámetro	Selección
CMG_DECRYPT	Propiedad para seleccionar el tipo de instalación de Encryption Removal Agent: 3 - Usar el paquete LSARecovery

Parámetro	Selección
	2 - Usar el material de claves forenses descargado con anterioridad 1 - Descargar claves del Dell Server 0 - No instalar Encryption Removal Agent
CMGSILENTMODE	Propiedad para desinstalación silenciosa: 1 - Silencioso 0 - No silencioso
Propiedades requeridas	
DA_SERVER	FQHN para el Servidor de administración de seguridad que aloja la sesión de negociación.
DA_PORT	Puerto en el Servidor de administración de seguridad 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 Servidor de administración de seguridad.
DA_RUNAS	Nombre de usuario en formato compatible con SAM en cuyo contexto se realiza la solicitud de búsqueda de clave. Este usuario debe estar en la lista de Key Server en Servidor de administración de seguridad.
DA_RUNASPWD	Contraseña para el usuario de runas.
FORENSIC_ADMIN	Cuenta de administrador forense del Dell Server, que se puede utilizar para solicitudes de administración forense relacionadas con desinstalaciones o claves.
FORENSIC_ADMIN_PWD	La contraseña para la cuenta del administrador forense.
Propiedades opcionales	
SVCLOGONUN	Nombre de usuario en formato UPN para inicio de sesión del servicio Encryption Removal Agent como parámetro.
SVCLOGONPWD	Contraseña para el inicio de sesión como usuario.

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

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

  Comando MSI:

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

  Reinicie el equipo cuando finalice.

- En el siguiente ejemplo se desinstala de forma silenciosa el cliente Encryption y se 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 cuando se utiliza una contraseña de administrador forense en la línea de comandos:

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

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 la computadora y, a continuación, desinstale el componente de Encryption Management Agent.

- **IMPORTANTE: Si instaló el cliente SED y activó la Autenticación previa al inicio, siga las instrucciones de desinstalación en Desinstalación del cliente SED.**

  En siguiente el ejemplo se desinstala solo el componente Encryption Management Agent de Dell y no el cliente SED.

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

Desinstalación del cliente SED

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

Proceso

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

Desactivación de la PBA

1. Como un administrador de Dell, inicie sesión en la Management Console.

2 En el panel izquierdo, haga clic en **Poblaciones** > **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 hostname de la computadora que desea.
7 Haga clic en **Políticas de seguridad** en el menú superior.
8 Seleccione **Unidades de cifrado automático** en la página **Categoría de política**.
9 Cambie la **Unidad de cifrado automático (SED)** y la política de `On` a ***`Off`***.
10 Haga clic en **Guardar**.
11 En el panel izquierdo, haga clic en **Confirmar políticas**.
12 Haga clic en **Confirmar políticas**.

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

Desinstale los clientes SED y Authentication después de desactivar PBA.

Desinstalación del cliente SED

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro, el instalador del cliente Encryption se puede encontrar en C:\extracted\Encryption Management Agent\EMAgent_XXbit_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 haya terminado.

Desinstalación del cliente BitLocker Manager

Desinstalación con la línea de comandos

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

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

  Reinicie el equipo cuando finalice.

6

Desinstalador de Data Security

Desinstalar Endpoint Security Suite Enterprise

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

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

Para obtener más información o para usar una interfaz de línea de comandos (CLI), consulte el artículo de la base de conocimientos (KB) SLN307791.

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

Para ejecutar la utilidad, abra la carpeta que la contiene, haga clic con el botón secundario en **DataSecurityUninstaller.exe** y **ejecútela como administrador**.

Haga clic en **Siguiente**.

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

NOTA: Las dependencias necesarias se seleccionan o borran automáticamente.

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

Seleccione **Agente de eliminación de cifrado: descargar claves desde servidor**.

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

Seleccione **Eliminar** para iniciar la desinstalación.

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

La desinstalación y eliminación se han completado.

7

Aprovisionamiento de un inquilino

Debe aprovisionar un inquilino en Dell Server antes de que se active la aplicación de las políticas de Advanced Threat Prevention.

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 Dell Server.
- Debe tener conexión a Internet en el cliente para mostrar la integración del servicio en línea de Advanced Threat Prevention en la consola de administración.
- 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 Dell Server.

Aprovisionamiento de un inquilino

1 Como administrador de Dell, inicie sesión en la Consola de administración.

2 En el panel izquierdo de la consola de administración, haga clic en **Administración > Administración de servicios**.

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

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

5 Lea y acepte el EULA y haga clic en **Siguiente**.

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

7 Descargue el certificado. Esto es necesario para poder llevar a cabo una recuperación si se produce algún problema con Dell Server. No se realiza automáticamente una copia de seguridad de este certificado. Realice una copia de seguridad del certificado en una ubicación segura de otro equipo. Seleccione la casilla de verificación para confirmar que se realizó una copia de seguridad del certificado y haga clic en **Siguiente**.

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

8

Configuración de actualización automática del agente Advanced Threat Prevention

En la consola de administración, 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 servicio de Advanced Threat Prevention. Las actualizaciones se efectúan mensualmente.

NOTA:
Las actualizaciones automáticas del agente son compatibles con Dell Server 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 consola de administración, haga clic en **Administración** > **Administración de servicios**.
2 En la pestaña *Amenazas avanzadas*, en *Actualización automática del agente*, haga clic en **Activar** y, a continuación, en **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 consola de administración, haga clic en **Administración** > **Administración de servicios**.
2 En la pestaña *Amenazas avanzadas*, en *Actualización automática del agente*, haga clic en **Desactivar** y, a continuación, en **Guardar preferencias**.

9

Extracción de instaladores secundarios

- El instalador maestro no es un *desinstalador* maestro. Cada componente se debe desinstalar por separado, seguido de la desinstalación del instalador maestro. Utilice este proceso para extraer los clientes del instalador maestro con el fin de poder utilizarlos para la desinstalación.

1 Desde el medio de instalación de Dell, copie el archivo **DDSSuite.exe** a la computadora local.

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

```
DDSSuite.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

- En esta sección se explica cómo configurar los componentes a fin de utilizarlos con la autenticación/autorización Kerberos al utilizar un Servidor de administración de seguridad. Servidor virtual de administración de seguridad 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 el Servidor virtual de administración de seguridad no utiliza Key Server, se ve afectada la desinstalación normal. Cuando se desinstala un cliente Encryption que está activado en un Servidor virtual de administración de seguridad, se utiliza la recuperación de clave forense estándar a través de Security Server, en lugar del método Kerberos de Key Server. Consulte Desinstalación de la línea de comandos para obtener más información.

Panel Servicios: Agregar usuario de cuenta de dominio

1 En el Servidor de administración de seguridad, 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 *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 a <Key Server install dir> log.txt a fin de comprobar que el servicio arrancó correctamente.

Archivo de configuración del Key Server: agregar usuario para la comunicación de Servidor de administración de seguridad

1 Vaya a <Key Server install dir>.

2 Abra ***Credant.KeyServer.exe.config*** con un editor de texto.

3 Vaya a <add key="user" value="superadmin" /> y cambie el valor de "superadmin" al nombre del usuario correspondiente (también puede dejarlo como "superadmin").

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

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 de Windows (Inicio > Ejecutar > services.msc > Aceptar).

2 Reinicie el servicio Key Server.

3 Vaya a <Key Server install dir> log.txt a fin de comprobar que el servicio arrancó correctamente.
4 Cierre el panel Servicios.

Management Console: agregar administrador forense

1 Como un administrador de Dell, inicie sesión en la Management Console.
2 Haga clic en **Poblaciones** > **Dominios**.
3 Seleccione el dominio adecuado.
4 Haga clic en la pestaña **Key Server**.
5 En *Cuenta*, agregue el usuario que realizará las actividades de administrador. El formato es DOMINIO\Nombre de usuario. Haga clic en **Agregar cuenta**.
6 En el menú de la izquierda, haga clic en **Usuarios**. En la casilla de búsqueda, escriba el nombre de usuario que se agregó en el paso 5. Haga clic en **Buscar**.
7 Una vez que haya encontrado al usuario correcto, haga clic en la pestaña **Admin**.
8 Seleccione **Administrador forense** y haga clic en **Actualizar**.

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

Uso de la Utilidad de descarga administrativa (CMGAd)

- Esta herramienta permite la descarga de una agrupación de material de claves para usar en una computadora que no esté conectada a un Servidor de administración de seguridad/Servidor virtual de administración de seguridad.
- 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

> **CONSEJO:**
> 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 Servidor virtual de administración de seguridad no utiliza el Key Server, así que el modo Administración no se puede usar para obtener una agrupación de claves de un Servidor virtual de administración de seguridad. Utilice el modo Forense para obtener la agrupación de claves si el cliente está activado en un Servidor virtual de administración de seguridad.

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

CONSEJO:

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.

12

Solución de problemas

Todos los clientes: Solución de problemas

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

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

Todos los clientes: estado de la protección

En el Dell Security Management Server versión 9.8.2, se implementó un nuevo método para derivar un estado protegido del dispositivo. Anteriormente, el área de estado protegido de los extremos en el panel de la consola de administración solo indicaría el estado de cifrado por dispositivo.

El estado protegido ahora se señala si se cumple alguno de los siguientes criterios:

- Está instalada y activada Advanced Threat Prevention.
- La protección web o el firewall de cliente está instalado y está activada la política de la protección web o la del firewall de cliente.
- Está instalado y activado Dell Data Guardian.
- La administración de unidades de autocifrado está instalada y activada, y la autenticación previa al inicio (PBA) está activada.
- BitLocker Manager está instalado, activado y se completó el cifrado.
- Dell Encryption (MAC) está instalado y activado, y se aplicó el cifrado basado en la política.
- Dell Encryption (Windows) está instalado, activado y se estableció el cifrado basado en la política para el extremo y los barridos de dispositivo están completos.

Solución de problemas de los clientes Encryption y Server Encryption

Realizar la actualización de Windows 10 Creators Update

Para realizar la actualización Windows 10 October 2018 Update, siga las instrucciones que se indican 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 la activación no son las credenciales del administrador del dominio.

Mensaje de error: Nombre de usuario desconocido o contraseña incorrecta

El nombre de usuario o contraseña no coinciden.

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

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

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

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

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

O bien

```
The operation timed out.
```

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

Posibles soluciones

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

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

Posibles soluciones

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

Proceso de activación inicial

El siguiente diagrama muestra una activación inicial correcta.

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

El cuadro de diálogo Activación 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 ícono 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 secundario del mouse en el ícono de cliente de Encryption en el área de notificaciones 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 dominio es una medida de seguridad que impide que Server Encryption se extienda a otros entornos de servidores que no lo admitan. Para desactivar el requisito para credenciales de administrador de dominios, consulte Antes de empezar.

6 El Dell Server comprueba las credenciales en el vault de la empresa (Active Directory o equivalente) para comprobar que las credenciales sean las de un administrador de dominio.
7 Un UPN se construye utilizando las credenciales.
8 Con el UPN, el Dell Server crea una cuenta de usuario nueva para el usuario del servidor virtual y almacena las credenciales en el almacén del Dell Server.

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

NOTA:
La contraseña y la autenticación DPAPI están desactivadas para esta cuenta para que *solo* el usuario de servidor virtual pueda acceder a las claves de cifrado en el equipo. Esta cuenta no se corresponde con ninguna otra cuenta de usuario en el equipo o en el dominio.

9 Cuando la activación se realiza correctamente, el usuario debe reiniciar el equipo y comenzar la segunda parte de dicha activación, autenticación y activación del dispositivo.

Solución de problemas de la autenticación y activación del dispositivo

La activación del dispositivo falla cuando:

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

Después de la activación, cuando se reinicia el equipo, Server Encryption inicia sesión automáticamente como el usuario de servidor virtual y solicita la clave de máquina del Dell 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 Cliente Encryption está en rojo, el cifrado aún no se ha activado.
- En la consola de administración, la versión de un servidor con Server Encryption instalado se incluye como *Shield para servidor*.
- Si falla la recuperación de la clave de máquina debido a un error de red, Server Encryption registra notificaciones de red con el sistema operativo.

- Si falla la recuperación de la clave de máquina:
  - El inicio de sesión de usuario de servidor virtual sigue siendo correcto.
  - Configure la política *Reintentar el intervalo tras un error de red* para realizar intentos de recuperación de la clave en un intervalo de tiempo.

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

Autenticación y activación de dispositivo

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

1 Cuando se haya reiniciado después de una activación inicial satisfactoria, un equipo con cifrado del servidor se autentica automáticamente mediante la cuenta de usuario de servidor virtual y se ejecuta el cliente Encryption en modo Servidor.

2 La computadora comprueba su estado de activación de dispositivo con el Dell Server:

- Si el equipo no tiene activación previa de dispositivo, el Dell Server asigna a la computadora un MCID, un DCID y un certificado de confianza, y almacena toda la información en el almacén del Dell Server.
- Si la computadora tiene activación previa de dispositivo, el Dell Server verifica el certificado de confianza.

3 Después de que el Dell Server asigne el certificado de confianza al servidor, el servidor puede acceder a sus claves de cifrado.

4 La activación del dispositivo es correcta.

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

Medios externos de cifrado e interacciones con PCS

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

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

Cifrar datos de escritura en medios de CD/DVD:

- Establecer Windows Media Encryption = activado.
- Establecer EMS, Excluir cifrado de CD/DVD = no seleccionado.
- Establecer subclase de almacenamiento: Control de unidad óptica = Solo UDF.

Uso de WSScan

- WSScan le permite asegurarse de que todos los datos se descifran 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 analizar: *Todas las unidades, Unidades fijas*, *Unidades extraíbles* o *CD-ROM/DVD-ROM*.

5 Seleccione el tipo de informe de Encryption: *Archivos cifrados*, *Archivos sin cifrar*, *Todos los archivos* o *Archivos sin cifrar en infracción*:

- *Archivos cifrados*: para garantizar que todos los datos se descifran cuando se desinstala 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 en el menú.

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

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

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

6 Seleccione el formato de salida:

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

7 Haga clic en **Buscar**.

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

Salida de WSScan

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

Ejemplo de salida:

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

Salida	Significado
Sello con la fecha/hora	La fecha y la hora en la que se exploró el archivo.
Tipo de cifrado	El tipo de cifrado utilizado para cifrar el archivo. **SysData:** clave de SDE. **Usuario:** clave de cifrado de usuario. **Común:** clave de cifrado común. WSScan no informa archivos cifrados mediante Encrypt for Sharing.
KCID	La Id. de equipo clave

Salida	Significado
	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 manera periódica (seleccione Servicio > haga clic con el botón secundario 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 realiza un barrido inicial, calculando la cantidad de archivos cifrados y los bytes. El barrido inicial se produce una sola vez.
- **Barrido de descifrado**: El servicio descifra archivos y posiblemente solicita el descifrado de archivos bloqueados.
- **Descifrar al reiniciar (parcial)**: el barrido de descifrado ha terminado y en el próximo reinicio se descifrarán algunos archivos (no todos) bloqueados.
- **Descifrar al reiniciar**: el barrido de descifrado ha terminado y todos los archivos bloqueados se descifrarán en el próximo reinicio.
- **No se han podido descifrar todos los archivos**: el barrido de descifrado ha terminado pero no se han podido descifrar todos los archivos. Este último estado significa que ocurrió una de las siguientes situaciones:
  - No se pudo programar el descifrado de los archivos bloqueados porque eran demasiado grandes, o porque se produjo un error al hacer la solicitud de desbloqueo.
  - Se produjo un error entrada/salida durante el cifrado de los archivos.
  - No se pudieron descifrar los archivos debido a una política.
  - Los archivos están marcados como deben ser cifrados.
  - Se produjo un error durante el barrido de descifrado.
  - Cualquiera que sea el caso, se crea un archivo de registro (si llevar un registro está configurado) cuando la configuración sea LogVerbosity=2 (o superior). Para solucionar problemas, configure LogVerbosity en 2 y reinicie el servicio de Encryption Removal Agent para forzar otro barrido de descifrado.
- **Completado**: el barrido de descifrado se ha completado. El servicio, el ejecutable, el controlador y el ejecutable del controlador están programados para ser eliminados en el siguiente reinicio.

Solucionar problemas del cliente Advanced Threat Prevention

Buscar el código del producto con Windows PowerShell

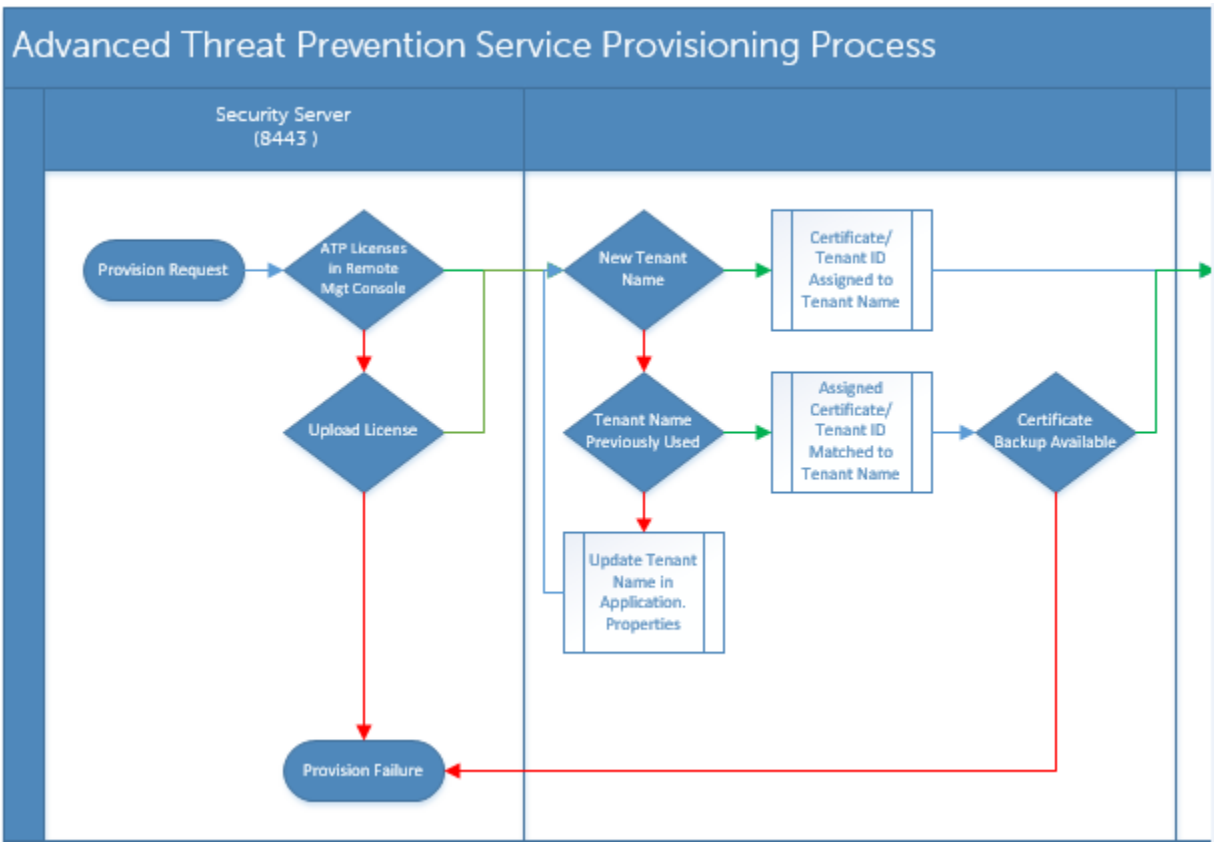
- Mediante este método, es muy sencillo identificar el código del producto si dicho código cambia más adelante.

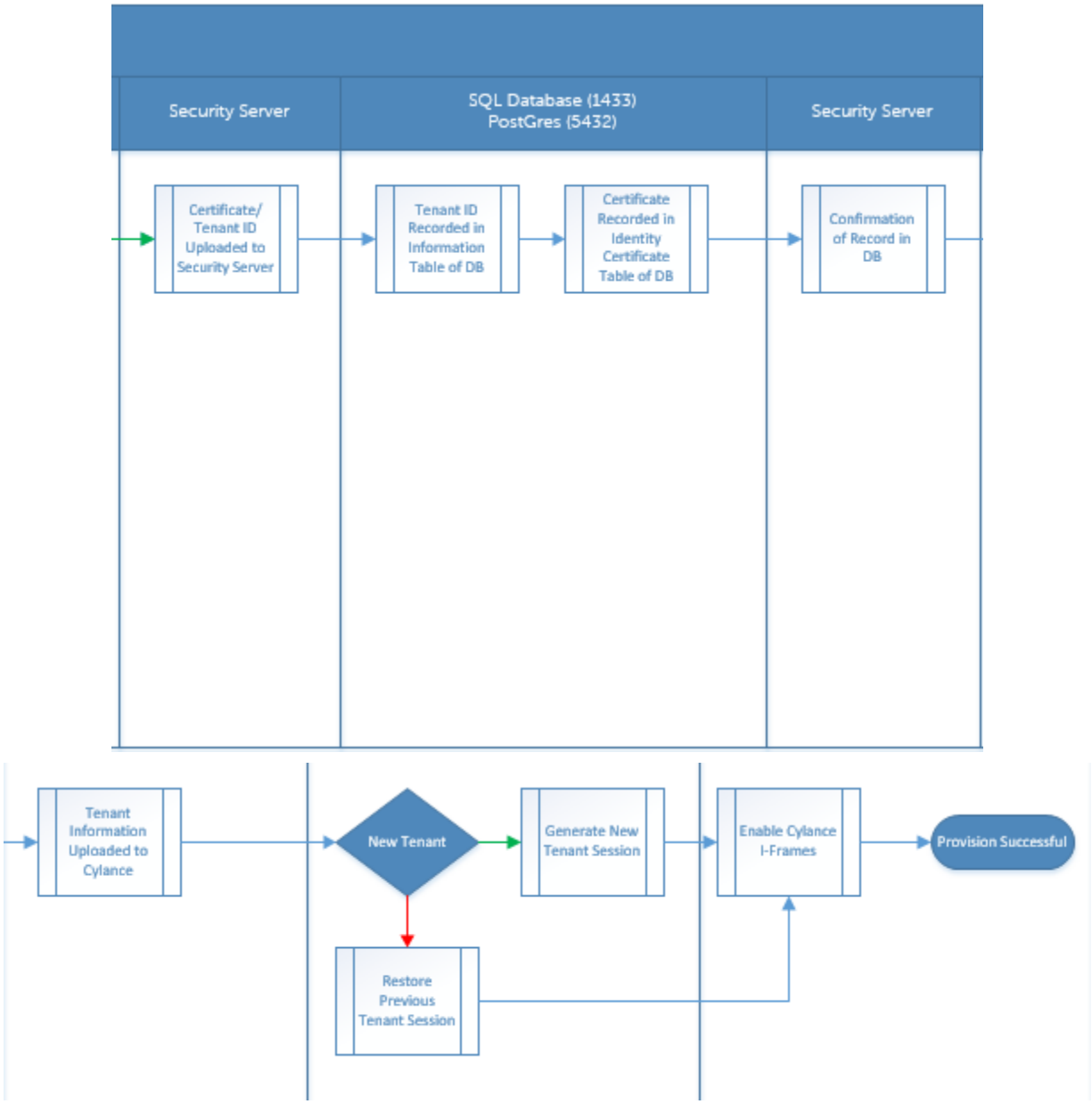
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

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

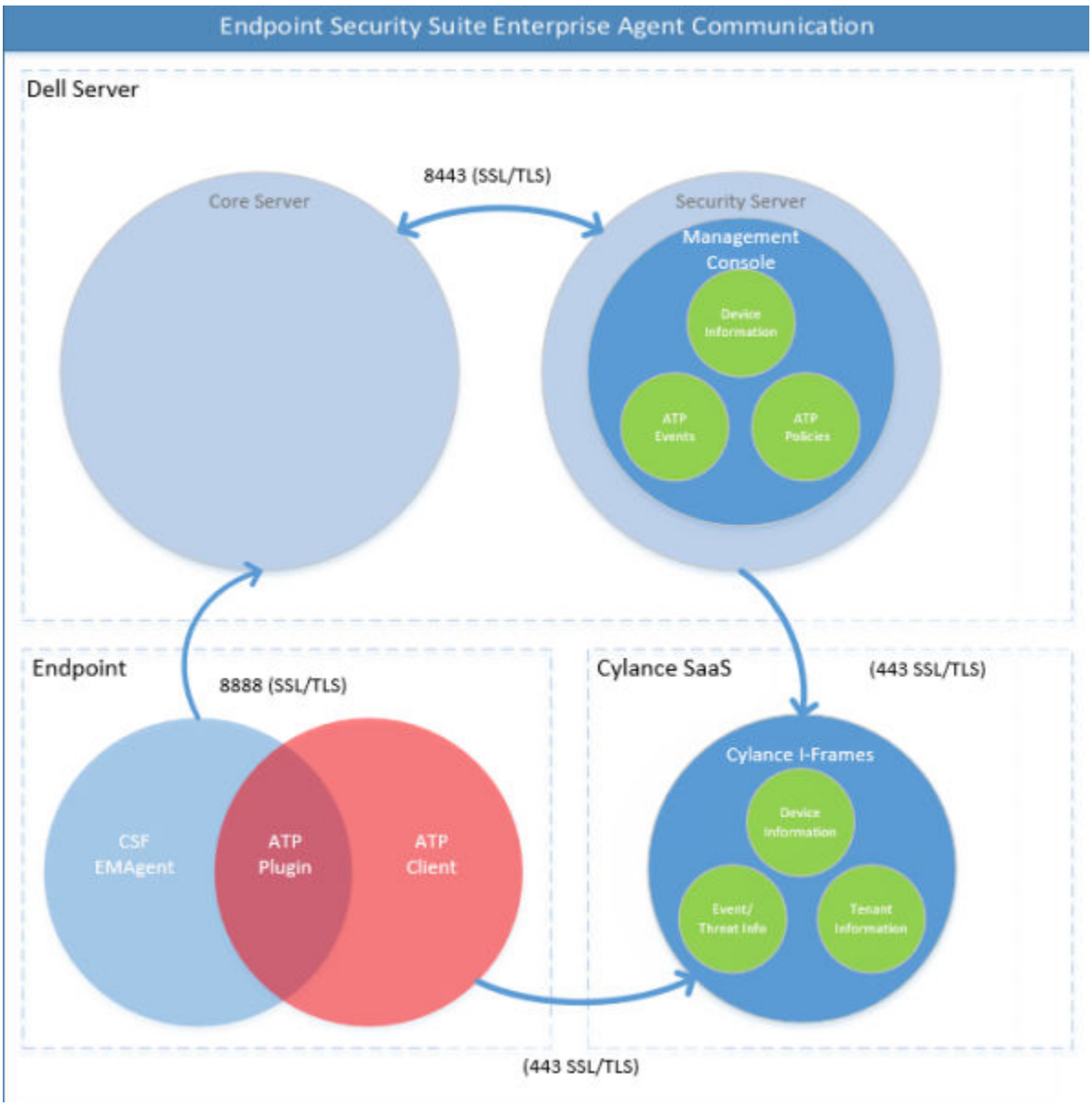
Comunicación de agentes y aprovisionamiento de Advanced Threat Prevention

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



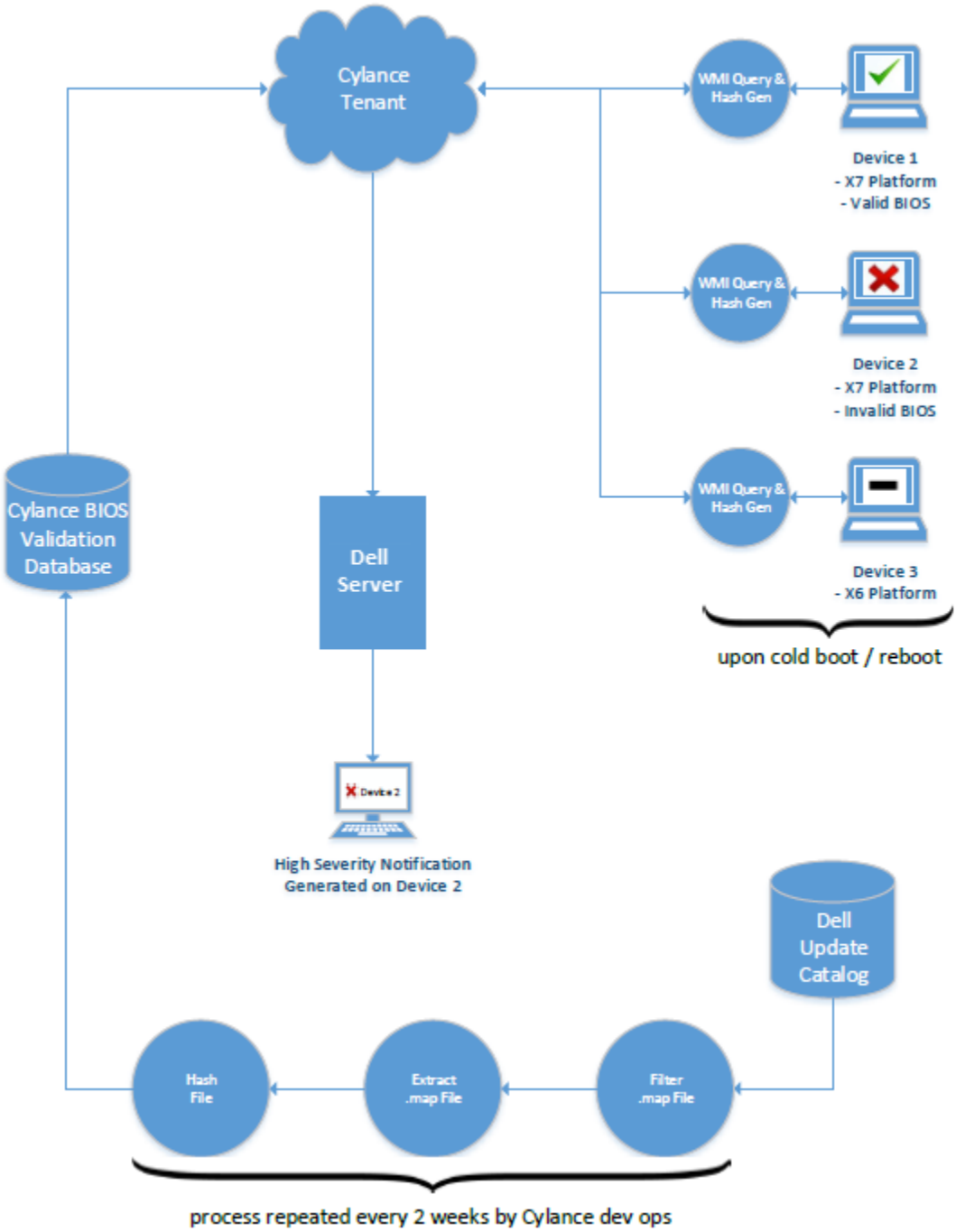


El siguiente diagrama muestra el proceso de comunicación de agentes de Advanced Threat Prevention.



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.



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 *cuando se creó este documento* era 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 deba ingresar su contraseña de administrador. Introduzca `Broadcom` como contraseña y haga clic en **Intro** si aparece este diálogo.

Aparecerán varios mensajes de estado.

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

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

13

Glosario

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.

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

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

Medios externos de cifrado este servicio incluido en el cliente Dell Encryption aplica políticas a los medios extraíbles y los dispositivos externos de almacenamiento.

Código de acceso de Medios externos de cifrado: este servicio dentro del Dell Server permite la recuperación de dispositivos protegidos de Medios externos de cifrado cuando el usuario olvida su contraseña y ya no puede iniciar sesión. La finalización de este proceso permite al usuario restablecer la contraseña configurada en el soporte.

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.

Terminal: una computadora administrada por el Dell Server.

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.

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 pueda administrar su empresa de forma más rápida y fácil.

Usuario del servidor: el 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 la computadora o el dominio, y no cuenta con un nombre de usuario ni con una contraseña que puedan utilizarse físicamente. A la cuenta se le asigna un valor de UCID exclusivo en la consola de administración.