# Dell Endpoint Security Suite Enterprise for Mac

Guía del administrador v2.9

Marzo 2021
Rev. A02

## Notas, precauciones y advertencias

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

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

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

# Tabla de contenido

# 1

# Introducción

La Guía del administrador de Endpoint Security Suite Enterprise para Mac proporciona la información necesaria para implementar e instalar el software cliente.

**Temas:**



## Descripción general

Endpoint Security Suite Enterprise para Mac ofrece Advanced Threat Prevention en el sistema operativo, capas de memoria y cifrado, todo ello administrado de forma centralizada desde Dell Server. Gracias a la administración centralizada, los informes de cumplimiento consolidados y las alertas de amenazas de la consola, las empresas pueden reforzar y comprobar con facilidad el cumplimiento de todos sus extremos. Nuestra experiencia en seguridad se integra en el producto con características como políticas predefinidas y plantillas de informes, que ayudan a las empresas a reducir los costos de administración y la complejidad de TI.

- Endpoint Security Suite Enterprise for Mac: un conjunto de software para el cifrado de cliente de datos y Advanced Threat Prevention.
- Política de proxy: se utiliza para distribuir políticas
- Servidor de seguridad: se utiliza para las activaciones de software de cifrado de cliente
- Security Management Server o Security Management Server Virtual: proporciona una administración centralizada de las políticas de seguridad, se integra con los directorios empresariales existentes y crea informes. A efectos del presente documento, ambos servidores se citan como Dell Server, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Security Management Server Virtual).

  Estos componentes de Dell interactúan sin ningún problema para ofrecer un entorno móvil seguro sin perjudicar la experiencia del usuario.

Endpoint Security Suite Enterprise para Mac cuenta con dos archivos .dmg: uno para el cliente Encryption y otro para Advanced Threat Prevention. Puede instalar los dos o solo uno de ellos.

## Cifrado con FileVault

Dell Encryption puede administrar el cifrado completo del disco de Mac FileVault. La política *Cifrado de volúmenes de Dell* debe estar **activada** para que se realice el cifrado y para que funcionen otras configuraciones de la política. Para obtener información sobre políticas adicionales, consulte *AdminHelp*.

Solo se admite el cifrado FileVault, administrado por Endpoint Security Suite Enterprise. Si una computadora tiene la política *Cifrado de volúmenes de Dell* establecida en **Activado** y *Cifrado a través de FileVault para Mac* establecido en **Desactivado**, aparecerá un mensaje de conflicto de política en el cliente Encryption. El administrador debe establecer ambas políticas en **Activado**.

## Cómo comunicarse 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.

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

# 2

# Requisitos

En este capítulo se enumeran los requisitos de hardware y software. Asegúrese de que el entorno de implementación cumple los requisitos antes de continuar con las tareas de implementación.

**Temas:**



# Cliente Encryption

## Hardware del cliente Encryption

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

| Hardware |
| --- |
| • 30 MB de espacio libre en el disco |
| • Tarjeta de interfaz de red 10/100/1000 o Wi-Fi |
| • El disco del sistema debe estar particionado con el esquema de particiones de la tabla de partición de GUID (GPT) y se puede formatear con uno de los siguientes:<br>○ Mac OS X Extended Journaled (HFS+): se convierte en el almacenamiento principal para aplicar FileVault.<br>○ Sistema de archivo de Apple (APFS) |

## Software del cliente Encryption

La tabla a continuación muestra qué software es compatible.

| Sistemas operativos (kernel de 64 bits) |
| --- |
| • macOS High Sierra 10.13.6 |
| • macOS Mojave 10.14.5 - 10.14.6 |
| • macOS Catalina 10.15.5 - 10.15.6 |

**NOTA:** Dell Encryption no es compatible con macOS Big Sur.

**NOTA:**

Si utiliza una cuenta de usuario de red para autenticarse, debe establecerla como una cuenta móvil para configurar completamente la administración de FileVault 2.

**Medios cifrados**

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

**NOTA:**

Encryption External Media es compatible con lo siguiente:

- FAT32
- exFAT
- Archivos de medios con el formato HFS Plus (MacOS Plus) que tienen esquemas de particiones de la Tabla de particiones GUID (GPT) o el Registro de arranque maestro (MBR). Consulte Activar HFS Plus.

**NOTA:**

El medio externo debe tener 55 MB disponibles, además de una cantidad de espacio libre igual al tamaño del archivo más grande que se vaya a cifrar, para alojar Encryption External Media.

| **Sistemas operativos Windows (32 y 64 bits) compatibles para el acceso a medios cifrados** |
|---|
| • Microsoft Windows 7 SP1<br>- Enterprise<br>- Professional<br>- Ultimate |
| • Microsoft Windows 8.1 - Windows 8.1 Actualización 1<br>- Enterprise<br>- Pro |
| • Microsoft Windows 10<br>- Education<br>- Enterprise<br>- Pro versión 1607 (Anniversary Update/Redstone 1) a la versión 1909 (Actualización de noviembre del 2019/19H2) |
| **Sistemas operativos de Mac (kernel de 64 bits) compatibles para el acceso a medios cifrados** |
| • macOS High Sierra 10.13.6<br>**NOTA:**<br>Encryption External Media en macOS High Sierra 10.14.x requiere Encryption Enterprise versión 8.16 o una posterior. |
| • macOS Mojave 10.14.5 - 10.14.6 |
| • macOS Catalina 10.15.5 - 10.15.6 |

# Advanced Threat Prevention

A fin de evitar errores de instalación, desinstale las aplicaciones antivirus, antimalware y antispyware de otros proveedores antes de instalar el cliente Advanced Threat Prevention.

## Hardware de Advanced Threat Prevention

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

| **Hardware** |
|---|
| • 500 MB de espacio libre en el disco, dependiendo del sistema operativo<br>• 2 GB RAM<br>• Tarjeta de interfaz de red 10/100/1000 o Wi-Fi |

# Software de Advanced Threat Prevention

La tabla a continuación muestra qué software es compatible.

| Sistemas operativos (kernel de 64 bits) |
| --- |
| • Mac OS X Mavericks 10.9.5<br>• Mac OS X Yosemite 10.10.5<br>• macOS Sierra 10.12.6<br>**NOTA:**<br>Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5 y macOS Sierra 10.12 solo son compatibles con Advanced Threat Prevention, no con el cliente Encryption. |
| • macOS High Sierra 10.13.6<br>**NOTA:**<br>Consulte Software del cliente Encryption para conocer las versiones específicas de macOS High Sierra compatibles con el cliente Encryption. |
| • macOS Mojave 10.14.5 - 10.14.6<br>**NOTA:**<br>Puede instalar el agente ATP en macOS Mojave; sin embargo, las funciones Protección de memoria y Control de secuencia de comandos se desactivan de forma automática y no se admiten actualmente. |
| • macOS Catalina 10.15.3 - 10.15.4 |

**NOTA:**

No hay compatibilidad con los sistemas de archivos que distinguen entre mayúsculas y minúsculas.

# 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 |

# Compatibilidad

En la siguiente tabla se detalla la compatibilidad con Windows, Mac y Linux.

n/a: la tecnología no es pertinente para esta plataforma.

Campo en blanco: la política se admite en Endpoint Security Suite Enterprise.

| Funciones | Políticas | Windows | macOS | Linux | |
| --- | --- | --- | --- | --- | --- |
| **Acciones de archivo** | | | | | |
| | Cuarentena automática (no segura) | x | x | x | |

| Funciones | Políticas | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| | Cuarentena automática (anormal) | x | x | x | |
| | Carga automática | x | x | x | |
| | Lista segura de políticas | x | x | x | |
| **Acciones de memoria** | | | | | |
| | Protección de memoria | x | x | x | |
| **Explotación** | | | | | |
| | Dinamización de pilas | x | x | x | |
| | Protección de pilas | x | x | x | |
| | Sobrescribir código | x | n/d | | |
| | Extracción de RAM | x | n/d | | |
| | Contenido malicioso | x | | | |
| **Inyección del proceso** | | | | | |
| | Distribución remota de memoria | x | x | n/d | |
| | Asignación remota de memoria | x | x | n/d | |
| | Escritura remota en la memoria | x | x | n/d | |
| | Escritura remota de PE en la memoria. | x | n/d | n/d | |
| | Sobrescribir remotamente el código | x | n/d | | |
| | Desasignación remota de memoria | x | n/d | | |
| | Creación remota de hebras | x | x | | |
| | APC remota programada | x | n/d | n/d | |
| | Inserción de DYLD | | x | x | |
| **Escalamiento** | | | | | |
| | Lectura de LSASS | x | n/d | n/d | |
| | Asignación de cero | x | x | | |
| **Configuración de protección** | | | | | |
| | Control de ejecución | x | x | x | |
| | Evitar la interrupción del servicio desde el dispositivo | x | x | | |
| | Eliminar los procesos en ejecución no seguros y sus subprocesos | x | x | x | |
| | Detección de amenazas en segundo plano | x | x | x | |

| Funciones | Políticas | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| | Detectar nuevos archivos | x | x | x | |
| | Tamaño máximo de archivo de almacenamiento para escanear | x | x | x | |
| | Excluir carpetas específicas | x | x | x | |
| | Copiar muestras de archivos | x | | | |
| **Control de la aplicación** | | | | | |
| | Cambiar ventana | x | | x | |
| | Exclusiones de carpetas | x | | | |
| **Configuración del agente** | | | | | |
| | Activar carga automática de archivos de registro | x | x | x | |
| | Activar las notificaciones de escritorio | x | | | |
| **Control de la secuencia de comandos** | | | | | |
| | Secuencia de comandos activa | x | | | |
| | PowerShell | x | | | |
| | Macros de Office | x | | n/d | |
| | Bloquear el uso de la consola PowerShell | x | | | |
| | Aprobar los scripts en estas carpetas (y subcarpetas) | x | | | |
| | Nivel de registro | x | | | |
| | Nivel de protección automática | x | | | |
| | Actualización automática | x | | | |
| | Ejecutar una detección (de la UI de agente) | x | | | |
| | Eliminar cuarentena (UI de agente y de consola) | x | | | |
| | Modo desconectado | x | | x | |
| | Datos detallados de la amenaza | x | | | |
| | Lista segura de certificados | x | x | n/d | |
| | Copiar muestras de malware | x | x | x | |
| | Configuración de proxy | x | x | x | |
| | Comprobación de la política del manual (UI de agente) | x | x | | |

3

# Tareas para el cliente Encryption

**Temas:**



# Instalar/actualizar el cliente Encryption

Esta sección le guiará a través del proceso de instalación/actualización y activación de el cliente Encryption para Mac.

Existen dos métodos para instalar o actualizar el cliente Encryption para Mac. Seleccione **una** de las opciones siguientes:

- Instalación/actualización interactiva y activación: este es el método más sencillo para instalar o actualizar el paquete de software cliente. Sin embargo, este método no permite realizar personalizaciones. Si tiene previsto utilizar Boot Camp o una versión de sistema operativo que todavía no es completamente compatible con Dell (a través de modificaciones en el .plist), debe utilizar el método de instalación/actualización mediante la línea de comandos. Para obtener información sobre cómo utilizar Boot Camp, consulte Cómo utilizar Boot Camp.
- Instalación/actualización mediante la línea de comandos: este es un método de instalación/actualización avanzado que solo deben emplear los administradores con experiencia en sintaxis de la línea de comandos. Si tiene previsto utilizar Boot Camp o una versión de sistema operativo que todavía no es completamente compatible con Dell (a través de modificaciones en el .plist), debe utilizar este método para instalar o actualizar el paquete de software cliente. Para obtener información sobre cómo utilizar Boot Camp, consulte Cómo utilizar Boot Camp.

  Para obtener más información sobre las opciones de los comandos del instalador, consulte la Biblioteca de referencia de Mac OS X en http://developer.apple.com. Dell recomienda encarecidamente utilizar herramientas de implementación remota, como Apple Remote Desktop, para distribuir el paquete de instalación del cliente.

  **NOTA:**

  Apple a menudo lanza nuevas versiones de sus sistemas operativos en el tiempo que pasa entre los lanzamientos de las versiones de Endpoint Security Suite Enterprise for Mac. Para admitir tantos clientes como sea posible, se permite realizar una modificación en el archivo com.dell.ddp.plist para apoyar estos casos. La prueba de estas versiones comienza tan pronto como Apple lanza una nueva versión, a fin de garantizar su compatibilidad con el cliente Encryption para Mac.

## Requisitos previos

Dell recomienda seguir las mejores prácticas de TI durante la implementación del software cliente. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados para las pruebas iniciales e implementaciones escalonadas para los usuarios.

Antes de empezar este proceso, asegúrese de que se cumplen los requisitos previos siguientes:

- Asegúrese de que Dell Server y sus componentes ya están instalados.

  A continuación encontrará varias guías. Si todavía no ha instalado Dell Server, siga las instrucciones de la guía más adecuada.

  *Guía de instalación y migración de Security Management Server*

  *Guía de inicio rápido y guía de instalación de Security Management Server Virtual*

- Asegúrese de que dispone de las URL del servidor de seguridad y de la política de proxy. Se necesitan ambas para instalar y activar el software cliente.
- Si la implementación utiliza una configuración distinta de la predeterminada, asegúrese de que sabe el número de puerto del servidor de seguridad. Se necesita para instalar y activar el software cliente.
- Asegúrese de que el equipo de destino cuenta con conectividad de red con el servidor de seguridad y la política de proxy.
- Asegúrese de que tiene configurada una cuenta de usuario de dominio en la instalación de Active Directory para utilizarla con Dell Server. La cuenta de usuario de dominio se utiliza para activar el software cliente. No es necesario configurar los extremos de Mac para la autenticación de dominio (red).

Antes de establecer políticas de cifrado, la política *Cifrado de volúmenes de Dell* debe estar *activada*. Asegúrese de que comprende las políticas *Cifrar mediante FileVault para Mac* y *Volúmenes destinados a cifrado*.

Para obtener más información sobre las políticas de cifrado, consulte Cifrado Mac > Cifrado de volúmenes de Dell.

# Actualización o instalación interactiva

Para instalar o actualizar y activar el software cliente, siga los pasos descritos a continuación. Debe tener una cuenta de administrador para llevar a cabo estos pasos.

**Instalación interactiva**

**NOTA:**

Antes de comenzar, guarde el trabajo del usuario y cierre otras aplicaciones; deberá reiniciar la computadora inmediatamente después de haber finalizado la instalación.

1. Desde el medio de instalación de Dell, monte el archivo Dell-Encryption-Enterprise-<version>.dmg.
2. Haga doble clic en el instalador del paquete. Aparecerá el siguiente mensaje:
   *Con este paquete, se ejecutará un programa para determinar si el software se puede instalar.*
3. Haga clic en **Continuar** para proceder.
4. Lea el texto de bienvenida y haga clic en **Continuar**.
5. Revise el contrato de licencia, haga clic en **Continuar** y, a continuación, en **Aceptar** para mostrar su conformidad con los términos del contrato de licencia.
6. En el campo *Dirección de dominio*, ingrese el dominio calificado de los usuarios de destino, como *department.organization.com*.
7. En el campo *Nombre para mostrar (opcional)*, considere establecer el *Nombre para mostrar* al nombre NetBIOS del dominio (anterior a Windows 2000), que normalmente se escribe en mayúsculas.

   Si lo establece, se mostrará este campo en lugar de la Dirección de dominio en el cuadro de diálogo *Activación*. Este nombre proporciona coherencia con el nombre de dominio que se muestra en los cuadros de diálogos de *Autenticación* en los dominios administrados por computadoras Windows.

8. En el campo *Servidor de seguridad*, ingrese el nombre de host del servidor de seguridad.

   Si en su implementación se utiliza una configuración distinta de la predeterminada, actualice la casilla de verificación *Utilizar SSL* y los puertos.

   Cuando se haya establecido una conexión, el indicador de conectividad del servidor de seguridad cambiará de rojo a verde.

9. En el campo *Proxy de política*, el nombre de host del proxy de la política se completará automáticamente con un host que coincide con el del servidor de seguridad. Este host se utiliza como política de Proxy si no se especifica ningún host en la configuración de la política.

   Cuando se haya establecido una conexión, el indicador de conectividad de la política de Proxy cambiará de rojo a verde.

10. Cuando complete el diálogo Configuración de Dell y se establezca la conexión al servidor de dispositivos y a la política de proxy, haga clic en **Continuar** para mostrar el tipo de instalación.
11. Algunas instalaciones en equipos específicos muestran el cuadro de diálogo *Seleccionar un destino* antes de mostrar el diálogo *Tipo de instalación*. Si es así, seleccione el disco del sistema actual en la lista de discos que se muestra. El icono del disco del sistema actual muestra una flecha verde que apunta al disco. Haga clic en **Continuar**.
12. Después de que aparezca el tipo de instalación, haga clic en **Instalar** para continuar con la instalación.
13. Cuando se le solicite, ingrese las credenciales de la cuenta de administrador. (La aplicación MacOS X Installer requiere credenciales).
14. Haga clic en **Aceptar**.

    **NOTA:**

Inmediatamente después de finalizar la instalación, reinicie el equipo. Si tiene archivos abiertos en otras aplicaciones y no están listos para un reinicio, haga clic en **Cancelar**, guarde el trabajo y cierre otras aplicaciones.

15. Haga clic en **Continuar con la instalación**. Empezará la instalación.
16. Cuando se complete la instalación, haga clic en **Reiniciar**.
17. Con una nueva instalación de Endpoint Security Suite Enterprise, se muestra un cuadro de diálogo que dice *Extensión de sistema bloqueada*.

    Para el consentimiento de kext, se muestra uno o ambos de los siguientes cuadros de diálogo.

| Extensión bloqueada del sistema | Extensión bloqueada del sistema |
|---|---|
| a. Haga clic en **Aceptar**.<br>b. Haga clic en **Aceptar**.<br>c. Para aprobar estas extensiones, seleccione **Preferencias del sistema > Seguridad y privacidad**.<br>d. Haga clic en **Permitir** junto a *Software de sistema del desarrollador Credant Technologies (Dell, Inc., anteriormente Credant Technologies).*<br>e. Haga clic en **Aceptar**. | Complete estos pasos si no se pudo cargar la extensión del sistema para el montaje de volúmenes FDEEM.<br>a. Haga clic en **Abrir las preferencias del sistema**.<br>b. Haga clic en **Aceptar**.<br>c. En la pestaña **General**, haga clic en **Permitir** junto a *Software del sistema del desarrollador de Credant Technologies (Dell, Inc., anteriormente Credant Technologies).*<br>d. Haga clic en **Aceptar**. |

    Es posible que el botón Permitir esté disponible durante 30 minutos o menos después de realizar la instalación. Si omite este paso, el cuadro de diálogo seguirá apareciendo cada 25 minutos hasta que se complete el proceso.
18. Continúe para Activar el cliente Encryption para Mac.

**macOS 10.15 y versiones posteriores con medios extraíbles**

Si una empresa utiliza medios extraíbles con macOS 10.15 y versiones posteriores, los usuarios deben activar el acceso completo al disco para medios externos. Para obtener más información, consulte Habilitar el acceso completo al disco para medios extraíbles.

# Instalación/actualización mediante la línea de comandos

Para instalar el software cliente mediante la línea de comandos, siga estos pasos.

**Instalación con la línea de comandos**

1. Desde el medio de instalación de Dell, monte el archivo Dell-Encryption-Enterprise-<version>.dmg.
2. Copie el paquete **instalación de Dell Endpoint Security Suite Enterprise** y el archivo de **com.dell.ddp.plist** en la unidad local.
3. En la Management Console, modifique las siguientes políticas si es necesario. La configuración de políticas anula los ajustes del archivo .plist. Utilice la configuración de .plist si la consola de administración no cuenta con ninguna política.
   - **Lista de usuarios sin autenticación**: en algunos casos, es posible que desee editar esta política para que usuarios o clases de usuarios concretos no tengan que activarse en Dell Server. Por ejemplo, en un centro educativo, se pediría a los profesores que activen sus computadoras en Dell Server, pero no se le pediría a todos los estudiantes individuales que utilicen las computadoras del laboratorio. El administrador del laboratorio podría utilizar esta política y la cuenta que ejecuta la herramienta de cliente de modo que los estudiantes puedan iniciar sesión sin que se les solicite la activación. Para obtener más información sobre la herramienta de cliente, consulte Herramienta de cliente. Si una empresa necesita saber qué cuenta de usuario está asociada con cada computadora Mac, deben activarse todos los usuarios en Dell Server, de modo que la empresa no pueda editar esta propiedad. Sin embargo, si un usuario desea aprovisionar Encryption External Media, se debe autenticar en Dell Server.
4. Abra el archivo .plist y edite los valores de cualquier marcador adicional:

   **NOTA:**

   Apple a menudo lanza nuevas versiones de sus sistemas operativos en el tiempo que pasa entre los lanzamientos de las versiones de Endpoint Security Suite Enterprise for Mac. Para atender a tantos clientes como sea posible, Dell permite la modificación del archivo .plist para ofrecer compatibilidad en esos casos. En cuanto Apple lanza una nueva versión, Dell comienza a probarla para asegurarse de que es compatible con el cliente Encryption para Mac.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name
can log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer
version of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
   </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an existing
```

```
port]
    </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
  <key>EMSTreatsUnsupportedFileSystemAs</key>
  <string>ignore</string> [For handling Mac OS Extended media. Possible values are
ignore, provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to
unShielded Media. unshieldable - If the EMS Access to unShielded Media policy is set to
Block, the media is ejected. If the EMS Access to unShielded Media policy is not set to
Block, it is usable as provisioningRejected. The key and value are case sensitive.]
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5. Guarde y cierre el archivo .plist.
6. Para cada equipo de destino, copie el paquete en una carpeta temporal y el archivo com.dell.ddp.plist en **/Library/Preferences.**
7. Utilice el comando de **instalación** para realizar la instalación del paquete con la línea de comandos:
   **`sudo installer -pkg "Install Dell Endpoint Security Suite Enterprise.pkg" -target /`**
8. Reinicie el equipo utilizando la siguiente línea de comandos: **`sudo shutdown -r now`**

   **NOTA:**

   La Protección de integridad del sistema (SIP) se fortaleció en macOS High Sierra (10.13) para exigir que los usuarios aprueben las nuevas extensiones de kernel de otros fabricantes. Para obtener información acerca del permiso de extensiones de kernel en macOS High Sierra, consulte el Artículo SLN307814 de la base de conocimientos (KB).
9. Continúe para Activar el cliente Encryption para Mac.

**macOS 10.15 y versiones posteriores con medios extraíbles**

Si una empresa utiliza medios extraíbles con macOS 10.15 y versiones posteriores, los usuarios deben activar el acceso completo al disco para medios externos. Para obtener más información, consulte Habilitar el acceso completo al disco para medios extraíbles.

# Habilitar el acceso completo al disco para medios extraíbles

Si una empresa utiliza medios extraíbles con macOS 10.15 y versiones posteriores, los usuarios deben activar el acceso completo al disco para medios externos. Los usuarios ven una de estas indicaciones:

- Después de instalar el software cliente, en una pantalla se le indicará que debe proporcionar el consentimiento del acceso completo al disco para medios externos. Haga clic en el botón **Ir a Seguridad y privacidad** y continúe con los pasos que se indican a continuación.
- Si no se solicita después de la instalación, se les solicitará a los usuarios que habiliten el acceso completo al disco cuando montan los medios extraíbles por primera vez. Se muestra un mensaje en el que se indica que Dell Encryption External Media o EMS Explorer solicitan acceso a los archivos en un volumen extraíble. Haga clic en **Aceptar** y continúe con los pasos que se indican a continuación.

Para obtener más información, consulte el artículo de la base de conocimientos SLN319972.

1. En *Preferencias del sistema > Seguridad y privacidad*, haga clic en la pestaña **Privacidad**.
2. En el panel izquierdo, seleccione **Acceso completo al disco**.
   No se muestra la aplicación *Dell Encryption External Media*.
3. En la parte inferior, haga clic en el icono de bloqueo y proporcione las credenciales de una cuenta de administrador local.
   En el panel izquierdo > **Archivos y carpetas**, el usuario puede comprobar los componentes de medios externos (EMS) para proporcionar los permisos necesarios.
4. En el panel izquierdo, seleccione **Acceso completo al disco**.

   Ahora se muestra la aplicación *Dell Encryption External Media*. Sin embargo, cuando la solicitud de aprobación está pendiente, la casilla de verificación para dicha aplicación no se selecciona.
5. Otorgue el permiso seleccionando la casilla de verificación.

   Si no se muestra la aplicación *Dell Encryption External Media*.

a. Haga clic en el icono de signo más (+) en el panel derecho.
b. Vaya a **/Library/Dell/EMS** y seleccione **Dell Encryption External Media**.
c. Haga clic en **Abrir**.
d. En **Acceso completo al disco**, seleccione la casilla de verificación de *Dell Encryption External Media*.

6. Cierre **Seguridad y privacidad**.

# Activar el cliente Encryption

El proceso de activación asocia las cuentas de usuario de red de Dell Server con la computadora Mac y recupera las políticas de seguridad de cada cuenta, envía actualizaciones de inventario y de estado, permite la recuperación de flujos de trabajo y proporciona informes de conformidad exhaustivos. El software cliente realiza el proceso de activación para cada cuenta de usuario que encuentra en el equipo a medida que los usuarios inician sesión en su cuenta de usuario.

Después de instalar el software cliente y que el Mac se haya reiniciado, el usuario inicia sesión:

1. Ingrese el nombre del usuario y la contraseña administrados por Active Directory.

   Si se agota el tiempo de espera del diálogo de la contraseña, hacer clic en **Actualizar** en la pestaña Políticas. En Ver la política y el estado del cifrado en el equipo local, consulte el paso 1.

2. Seleccione el Dominio en el que se iniciará sesión.

   Si Dell Server está configurado para ser compatible con varios dominios y se debe utilizar un dominio diferente para la activación, utilice el nombre principal de usuario (UPN), que tiene la forma *<username>@<domain>*.

3. Opciones disponibles:
   - Haga clic en **Activar**.
     - Si la activación es correcta, se mostrará un mensaje para indicar que la activación ha tenido éxito. El cliente Encryption para Mac es totalmente operativo y se administra mediante Dell Server.

       **NOTA:**

       Si se muestra una alerta sobre un recurso necesario de Encryption External Media, haga clic en el botón **Ir a Seguridad y privacidad** y, luego, haga clic en **Permitir** para permitir cualquier extensión de sistema que se requiera en su organización. Debe permitir que esta extensión de Encryption External Media funcione correctamente.
     - Si la activación falla, el software cliente permite tres intentos para ingresar las credenciales de dominio correctas. Si los tres intentos fallan, se mostrará otra vez la solicitud de las credenciales del dominio en el próximo inicio de sesión del usuario.
   - Haga clic en **Ahora no** para descartar el cuadro de diálogo, que se mostrará de nuevo en el siguiente inicio de sesión del usuario.

     **NOTA:**

     Si el administrador necesita descifrar una unidad en una computadora, tanto desde una ubicación remota ejecutando un script como en persona, el software cliente solicitará al usuario que permita el acceso del administrador y que ingrese su contraseña.

     **NOTA:**

     Si se establece el equipo para el cifrado de FileVault y los archivos se cifran, asegúrese de que inicia sesión en una cuenta desde la que después pueda iniciar el sistema.

4. Realice una de estas opciones:
   - Si el cifrado **no** se había activado antes de la activación, continúe con el proceso de cifrado.
   - Si el cifrado **sí** se había activado antes de la activación, vaya a Ver la política y el estado del cifrado.

# Ver la política y el estado del cifrado

Puede ver la política y el estado del cifrado en la computadora local o en la consola de administración.

## Ver la política y el estado del cifrado en el equipo local

Para ver la política y el estado del cifrado en el equipo local, siga los pasos a continuación.

1. Abra *Preferencias del sistema* y haga clic en **Dell Encryption Enterprise**.

2. Haga clic en la pestaña **Políticas** para ver el conjunto de políticas actuales configuradas para el equipo. Utilice esta vista para confirmar las políticas de cifrado específicas que están en vigor en este equipo.

   **NOTA:**

   Haga clic en **Actualizar** para comprobar si ha habido actualizaciones de políticas.

   En la consola de administración, se indican las políticas de Mac en estos grupos de tecnología:

   - **Cifrado de Mac**
   - **Cifrado de medios extraíbles**

   Las políticas que establezca dependen de los requisitos de cifrado de su empresa.

   Esta tabla enumera las opciones de política.

| **Cifrado Mac > Cifrado de volúmenes de Dell**<br>Para High Sierra y versiones posteriores, ambas políticas deben estar habilitadas. Para Sierra y versiones anteriores, consulte las versiones anteriores de la documentación. | |
|---|---|
| Cifrado de volúmenes de Dell | *Activado* o *Desactivado*<br>Es la "política maestra" para todas las demás políticas del Cifrado de volúmenes de Dell. Esta política debe establecerse en *Activado* para que se apliquen otras políticas de cifrado de volúmenes de Dell.<br>El valor *Activado* permite habilitar el cifrado y lo inicia para los volúmenes que no están cifrados, según lo que se indica en las políticas *Volúmenes destinados para el cifrado* **o** *Cifrado mediante FileVault para Mac*. El valor predeterminado es *Activado*.<br>El valor Desactivado permite deshabilitar el cifrado e iniciar un barrido de descifrado en los volúmenes completa o parcialmente cifrados. |
| Cifrar mediante FileVault para Mac | Si tiene previsto utilizar el cifrado de FileVault, asegúrese de establecer primero el Cifrado de volúmenes de Dell en *Activado*.<br>Compruebe que la política *Cifrado mediante FileVault para Mac* está seleccionada en la consola de administración.<br>Cuando está activada, se utiliza FileVault para cifrar el volumen del sistema, incluidos los Fusion Drives, según la configuración de la política *Volúmenes destinados a cifrado*. |
| **Cifrado Mac > Configuración global de Mac** | |
| Volúmenes destinados a cifrado | *Solo el volumen del sistema* o *Todos los volúmenes fijos*<br>*Solo el volumen del sistema* protege solamente el volumen del sistema que se encuentra en ejecución.<br>**Todos los volúmenes fijos** protege todos los volúmenes con formato Mac OS Extended de todos los discos fijos, así como el volumen del sistema que se encuentra en ejecución. |

3. Para obtener descripciones de todas las políticas, consulte *AdminHelp*, que está disponible en la consola de administración. Para localizar una política específica en *AdminHelp*:
   a. Haga clic en el ícono Búsqueda.
   b. En *Buscar*, ingrese el nombre de la política entre comillas.
   c. Haga clic en el enlace de tema que se muestra. El nombre de la política que ha ingresado entre comillas está resaltado en el tema.
4. Haga clic en la pestaña **Volúmenes del sistema** para comprobar el estado de los volúmenes destinados al cifrado.

| **Estado** | **Descripción** |
|---|---|
| Excluido | El volumen se excluye del cifrado. Esta opción se aplica a volúmenes no cifrados cuando se ha desactivado el cifrado, a volúmenes externos, a volúmenes con formatos distintos a Mac OS X Extended (registrados en diario) y a volúmenes que no son del sistema cuando la política *Volúmenes destinados a cifrado* se establece en Solo el volumen del sistema. |

| Estado | Descripción |
|---|---|
| Preparación del volumen para el cifrado en curso | El software cliente está iniciando actualmente el proceso de cifrado para el volumen, pero no ha empezado el barrido de cifrado. |
| No puede cambiarse el tamaño del volumen | El software cliente no puede iniciar el cifrado porque no puede cambiarse el tamaño del volumen de forma adecuada. Tras recibir este mensaje, póngase en contacto con Dell ProSupport y proporcione los archivos de registro. |
| Necesita reparaciones antes de que empiece el cifrado | El volumen ha fallado la verificación de la Utilidad de disco.<br>Para reparar un volumen, siga las instrucciones que se indican en el artículo HT1782 en el sitio de soporte técnico de Apple (http://support.apple.com/kb/HT1782). |
| Preparación del cifrado finalizada. Reinicio pendiente | El cifrado se inicia después del reinicio. |
| Conflicto de política de cifrado | El disco no puede ponerse bajo la política porque está cifrado con unos valores incorrectos. Consulte Cifrar mediante FileVault para Mac. |
| Espera de las claves de custodia con Dell Server en curso | Para garantizar que todos los datos cifrados se puedan recuperar, el cliente no empieza el proceso de cifrado hasta que todas las claves de cifrado se custodien de un modo correcto en Dell Server. El cliente sondeará en busca de conectividad con el servidor de seguridad mientras se encuentre en este estado hasta que las claves estén en custodia. |
| Cifrado | Está en curso un barrido de cifrado. |
| Cifrado | El barrido de cifrado ha finalizado. |
| Descifrado | Está en curso un barrido de descifrado. |
| Restauración del estado original en curso | El software cliente está restaurando el esquema de particiones a su estado original al término del proceso de *Descifrado*. Esta acción es el equivalente del estado *Preparación del volumen para el cifrado en curso* del barrido de descifrado. |
| Descifrado | El barrido de descifrado ha finalizado. |

| Color | Descripción |
|---|---|
| Verde | Parte cifrada |
| Rojo | Parte no cifrada |
| Amarillo | Parte que se está volviendo a cifrar<br>Por ejemplo, por un cambio en los algoritmos de cifrado. Los datos siguen estando protegidos. Solo se trata de una transición a un tipo diferente de cifrado. |

La pestaña Volúmenes del sistema muestra todos los volúmenes conectados al equipo que residen en discos con formato de Tabla de particiones GUID (GPT). En la tabla siguiente se muestran ejemplos de configuraciones de volumen para unidades internas.

**NOTA:**

Las placas de identificación y los íconos pueden diferir ligeramente según su sistema operativo.

| Placa de Identificación | Tipo y estado del volumen |
|---|---|
|  | El volumen del sistema Mac OS X actualmente iniciado. La placa de identificación X-folder indica la partición de inicio actual. |

| Placa de Identificación | Tipo y estado del volumen |
|---|---|
|  | Un volumen configurado para el cifrado. La placa de identificación Seguridad y privacidad indica una partición protegida por FileVault. |
|  | Un volumen que no es de inicio configurado para el cifrado. La placa de identificación Seguridad y privacidad indica una partición protegida por FileVault. |
|  | Varias unidades y sin cifrado.<br>**NOTA:**<br>El ícono del volumen sin una placa de identificación indica que no se ha hecho nada en el disco. Este disco no es de inicio. |

5. Haga clic en la pestaña **Medios extraíbles** para ver el estado de los volúmenes destinados a cifrado. En la tabla siguiente se muestran ejemplos de configuraciones de volumen para medios extraíbles.

   Las placas de identificación y los íconos pueden diferir ligeramente según su sistema operativo.

| Placa de Identificación | Estado |
|---|---|
|  | Un ícono de volumen atenuado indica un dispositivo sin montar. Los motivos pueden incluir:<br>• El usuario quizá ha preferido no aprovisionarlo.<br>• El medio puede estar bloqueado.<br>**NOTA:**<br>Una placa de identificación con una barra/círculo rojo en este ícono indica una partición que se excluye de la protección porque no se admite. Se incluyen volúmenes con formato FAT32. |
|  | El ícono de volumen saturado indica un dispositivo montado. La placa de identificación de no escritura indica que es de solo lectura. Se habilita el cifrado, pero los medios no se aprovisionan y el Acceso de Encryption External Media a medios no cifrados se establece en Solo lectura. |
|  | Medios cifrados mediante Encryption External Media, denotados por un distintivo de Dell. |

# Visualización de la política y el estado en la consola de administración

Para ver la política y el estado del cifrado en la consola de administración, realice los siguientes pasos.

1. Como administrador de Dell, inicie sesión en la Consola de administración.
2. En el panel izquierdo, haga clic en **Poblaciones > Extremos**.
3. En el caso de una estación de trabajo, haga clic en una opción del campo *Nombre de host* o, si conoce el nombre de host del terminal, ingréselo en *Buscar*. También puede ingresar un filtro para buscar el extremo.

   **NOTA:**

   Puede emplearse el carácter comodín (*), aunque no se requiere al inicio o al final del texto. Ingrese el nombre común, el nombre principal universal o el sAMAccountName.

4. Haga clic en el extremo correspondiente.
5. Haga clic en la pestaña **Detalles y acciones**.

   En el área Detalle del extremo se muestra información sobre el equipo Mac.

   El área de detalle Shield muestra información sobre el software cliente, incluidas las horas de inicio y finalización del barrido de cifrado del equipo.

   Para consultar las políticas vigentes, haga clic en **Ver políticas vigentes**.
6. Haga clic en la pestaña **Políticas de seguridad**. Desde esta pestaña, puede expandir los tipos de políticas y cambiar políticas individuales.
   a. Cuando termine, haga clic en **Guardar**.
   b. En el panel izquierdo, haga clic en **Administración** > **Confirmar**.

      **NOTA:**

      La cifra que se muestra junto a Cambios pendientes de políticas es acumulativa. Puede incluir cambios realizados en otros extremos, o realizados mediante otros administradores que están utilizando la misma cuenta.
   c. Ingrese una descripción de los cambios en la casilla *Comentarios* y haga clic en **Confirmar políticas**.
7. Haga clic en la pestaña **Usuarios**. En este área se muestra una lista de los usuarios activados en este equipo Mac. Haga clic en el nombre del usuario para ver la información de todos los equipos en los que este usuario esté activado.
8. Haga clic en la pestaña **Grupos de extremos**. En este área se muestran todos los grupos de extremos a los que pertenece este equipo Mac.

# Volúmenes del sistema

## Habilitar cifrado

Se permite el cifrado en los siguientes elementos:

- Volúmenes del sistema de archivos Apple (APFS) que comparten medios físicos con el volumen de inicio.
- Volúmenes Mac OS X Extended (registrados) y discos del sistema que están particionados con el esquema de partición de Tabla de particiones GUID (GPT)

Utilice este proceso para activar el cifrado en una computadora cliente si el cifrado **no** estaba activado ya. Este proceso solo habilita el cifrado para un único equipo. Si lo desea, puede elegir habilitar el cifrado para todas las computadoras Mac en el nivel de Enterprise. Para obtener instrucciones adicionales acerca de la habilitación del cifrado en el nivel de *Enterprise*, consulte AdminHelp.

1. Como un administrador de Dell, inicie sesión en la Management Console.
2. En el panel izquierdo, haga clic en **Poblaciones** > **Extremos**.
3. En el caso de una estación de trabajo, haga clic en una opción de la columna Nombre de host o, si conoce el nombre de host del terminal, ingréselo en *Buscar*. También puede ingresar un filtro para buscar el extremo.

   **NOTA:**

   Puede emplearse el carácter comodín (*), aunque no se requiere al inicio o al final del texto. Ingrese el nombre común, el nombre principal universal o el sAMAccountName.
4. Haga clic en el extremo correspondiente.
5. En la página *Políticas de seguridad*, haga clic en el grupo de tecnología **Cifrado Mac**.

   De manera predeterminada, la política maestra *Cifrado de volúmenes de Dell* está *Activada*.
6. Si un Mac cuenta con un Fusion Drive, seleccione la casilla de la política *Cifrar mediante FileVault para Mac*.

   **NOTA:**

   Esta política requiere que la política *Cifrado de volúmenes de Dell* también esté establecida en *Activada*. Sin embargo, cuando FileVault Encryption está activado, ninguna de las demás políticas del grupo estará en vigor. Consulte Cifrado Mac > Cifrado de volúmenes de Dell.
7. Si anula la selección de FileVault (macOS Sierra e inferior), cambie otras políticas como desee.

Para obtener descripciones de todas las políticas, consulte *AdminHelp*, que está disponible en la consola de administración.

8. Cuando termine, haga clic en **Guardar**.
9. En el panel izquierdo, haga clic en **Administración** > **Confirmar**.

   La cifra que se muestra junto a Cambios pendientes de políticas es acumulativa. Puede incluir cambios realizados en otros extremos, o realizados mediante otros administradores que están utilizando la misma cuenta.

10. Ingrese una descripción de los cambios en la casilla Comentarios y haga clic en **Confirmar políticas**.
11. Para ver la configuración de políticas en la computadora local después de que Dell Server envíe la política, en el panel Políticas de las Preferencias de Dell Encryption Enterprise, haga clic en **Actualizar**.

# Proceso de cifrado

El proceso de cifrado varía según el estado del volumen de arranque cuando el cifrado está activado.

**NOTA:**

Para mantener la integridad de los datos del usuario, el software cliente no empieza a cifrar un volumen hasta que el proceso de verificación sea correcto en ese volumen. Si la verificación falla en un volumen, el software cliente lo notifica al usuario e informa sobre el error en las Preferencias de Dell Data Protection. Si tiene que reparar un volumen, siga las instrucciones que se indican en el artículo HT1782 en el sitio de soporte técnico de Apple (http://support.apple.com/kb/HT1782). El software cliente vuelve a intentar la verificación en el siguiente reinicio del equipo.

Seleccione una de estas opciones:

- FileVault Encryption de un volumen sin cifrado
- Administrar un volumen cifrado con FileVault existente

## FileVault Encryption de un volumen sin cifrado

Con el cifrado FileVault, aparece un usuario adicional sin nombre en la PBA. No elimine este usuario, ya que permite que Dell Server aplique la política en el dispositivo. Si se elimina el usuario de PBA, el usuario deberá tomar medidas para comenzar a descifrar lo que exige la política.

1. Tras la instalación y la activación, deberá iniciar sesión en la cuenta desde la que desea arrancar después de que el cifrado de FileVault esté activado.
2. Espere a que finalice la validación de la unidad y la verificación del volumen.
3. Ingrese la contraseña para la cuenta.

   **NOTA:**

   Si permite que se agote el tiempo de espera de este cuadro de diálogo, deberá reiniciar o iniciar sesión para que se vuelva a mostrar el cuadro de diálogo de la contraseña.

4. Haga clic en **Aceptar**.
5. Asegúrese de que cada usuario tenga un token seguro. Consulte https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.

   Si la cuenta con la que el usuario inició sesión es una cuenta de red no móvil, se mostrará un cuadro de diálogo. Una vez que la unidad de arranque ya esté cifrada, solo el usuario que había iniciado sesión durante la inicialización de FileVault podrá iniciar la unidad.

   Esta cuenta debe ser una cuenta local o una cuenta de red móvil. Para cambiar las cuentas de red no móviles a cuentas móviles, vaya a **Preferencias del sistema > Usuarios y grupos**. Realice uno de los siguientes pasos:

   - Modifique la cuenta para que sea una cuenta móvil.

     O bien

   - Inicie sesión en una cuenta local e inicialice FileVault desde esa ubicación.

6. Haga clic en **Aceptar**.
7. Cuando finalice la preparación del cifrado, reinicie el equipo.

   **NOTA:**

En función de las políticas de experiencia del usuario establecidas en la consola de administración, es posible que el software cliente solicite al usuario que reinicie la computadora.

8. Después de que la computadora se reinicie, deberá conectarse a la red para que el software cliente custodie la información de recuperación en Dell Server.

   El software cliente puede empezar y completar el proceso de cifrado, además de informar el estado del cifrado en la consola de administración, antes de que el usuario inicie sesión. Esto permite aplicar la conformidad en todos los equipos Mac, sin necesidad de la interacción del usuario.

## Modificación de la política para agregar usuarios de FileVault

Para proteger los datos de un disco, FileVault los cifra automáticamente. En un volumen de arranque de FileVault administrado, a fin de permitir que varios usuarios desbloqueen el disco, puede modificar una política en la consola de administración y utilizar su diccionario de nombres y valores de registro de OpenDirectory para que los usuarios puedan agregarse a sí mismos al disco de FileVault.

1. En las políticas avanzadas de *Configuración global de Mac* de la consola de administración, diríjase a la política *Lista de usuarios de PBA de FileVault 2*.
2. En el campo de la política *Lista de usuarios de PBA de FileVault 2*, ingrese una regla que coincida con los usuarios desea especificar. Por ejemplo, al hacer coincidir `<string>*</string>` con cualquier clave debería aplicarse a todos los usuarios que tiene el servidor de OpenDirectory vinculado.

   Las etiquetas distinguen entre mayúsculas y minúsculas y el valor completo se debe formar correctamente como elemento de diccionario y de arreglo en una lista de propiedades. Las claves de diccionario se unen mediante AND. Los valores de arreglo se unen mediante OR, de modo que si se hace coincidir cualquier elemento de un arreglo se aplicará a todo el arreglo.

   **NOTA:**

   Si una regla no se forma correctamente, se muestra un mensaje de error en la pestaña *Dell Encryption Enterprise > Preferencias*.

   El siguiente <dict> muestra ejemplos para dos claves:

```
<dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
     <string>;Kerberosv5;;user1@LKDC:*</string>
     <string>;Kerberosv5;;user2@LKDC:*</string>
     <string>;Kerberosv5;;user3@LKDC:*</string>
     <string>;Kerberosv5;;z*@LKDC:*</string>
    </array>
    <key>dsAttrTypeStandard:NFSHomeDirectory</key>
    <string>/Users/*</string>
</dict>
```

   - Las entradas de clave *AuthenticationAuthority* de muestra especifican un patrón de *user1*, *user2* y *user3* o cualquier Id. de usuario que comienza con *z*. Para ver el diálogo que proporciona la sintaxis correcta para cada usuario, pulse las teclas **Control-Opción-Comando** del cliente. Copie la sintaxis del usuario y péguela en la consola de administración.

     **NOTA:**

     En este ejemplo, los asteriscos del principio representan la parte final de los registros de la autoridad de autenticación. Por lo general, para evitar no especificar menos de lo necesario, incluya el registro completo en lugar de un asterisco al principio, ya que el asterisco representa cualquier información tras los dos puntos en el registro de OpenDirectory.

   - La clave NFSHomeDirectory requiere que cualquier usuario que pase la primera clave tenga también un directorio principal en */Users/*.

     **NOTA:**

     Si no existe la carpeta principal para un usuario deberá crearla.

3. Reinicie los equipos.
4. Notifique a los usuarios que deben habilitar el arranque de FileVault para su cuenta de usuario. El usuario debe tener una cuenta móvil o local. Las cuentas de red se convierten automáticamente en cuentas móviles.

Para que un usuario active su cuenta de FileVault:

1. Abra **Preferencias del sistema** y haga clic en **Dell Encryption Enterprise**.
2. Haga clic en la pestaña **Volúmenes del sistema**.
3. Presione la tecla Control y haga clic en la opción de volumen del sistema y seleccione **Agregar usuarios de FileVault al inicio de FileVault**.

4. En *Buscar*, ingrese un nombre de usuario o desplácese hacia abajo. Las cuentas de usuario se muestran solo si se cumplen los criterios establecidos por la política.

   Para usuarios locales y móviles, se muestra el botón *Activar usuario*.

   Para usuarios de la red, se muestra el botón *Convertir y activar usuario*.

   **NOTA:**

   Un indicador verde aparece junto a las cuentas de usuario que pueden iniciar FileVault.

5. Haga clic en **Activar usuario** o en **Convertir y activar usuario**.
6. Ingrese la contraseña para la cuenta seleccionada y haga clic en **Aceptar**. Se muestra un indicador de progreso.
7. Después de un diálogo de operación correcta, haga clic en **Listo**.

## Administrar un volumen cifrado con FileVault existente

Si la computadora ya tiene un volumen cifrado con FileVault y el cifrado de FileVault está activado en la consola de administración, Dell Encryption puede hacerse cargo de la administración del volumen.

Si Dell Encryption detecta que el volumen de arranque ya está cifrado, se mostrará el cuadro de diálogo Dell Encryption Enterprise. Para permitir que Dell Encryption asuma la administración del volumen, siga estos pasos.

1. Seleccione **Clave de recuperación personal** *o* **Credenciales de la cuenta de inicio**.

   **NOTA:**

   En el caso de macOS High Sierra y el sistema de archivos de Apple (APFS), debe seleccionar **Credenciales de cuenta de arranque**.

   - **Clave de recuperación personal: si tiene la clave de recuperación personal que recibió cuando la unidad se cifró con FileVault.**
     a. Ingrese la clave.

        Si un usuario no tiene la clave actual, puede solicitarla al administrador.

     b. Haga clic en **Aceptar**.

        **NOTA:**

        Una vez completado el proceso de adquisición, se genera y custodia una nueva clave de recuperación personal. La clave de recuperación anterior se invalida y se elimina.
   - **Credenciales de la cuenta de inicio: si dispone del nombre de usuario y la contraseña de una cuenta que está autorizada actualmente para iniciar desde el volumen.**
     a. Ingrese el nombre de usuario y la contraseña.

     b. Haga clic en **Aceptar**.

2. Cuando se muestra un cuadro de diálogo que indica que Dell administra ahora el cifrado del volumen, haga clic en **Aceptar**.

   Si Dell Encryption detecta que un volumen que no es de inicio ya está cifrado, se muestra una solicitud de frase de contraseña.

3. (Solo volúmenes cifrados con FileVault que no sean de inicio) Para permitir que Dell Encryption asuma la administración del volumen, ingrese la frase de contraseña para acceder al volumen. Esta es la contraseña que se asignó al volumen cuando se cifró originalmente por FileVault.

   Cuando Dell administre el cifrado del volumen, la contraseña antigua ya no será válida. Su administrador de Dell podría recuperar una clave de recuperación para su volumen en el caso de que necesitara ayuda para la recuperación.

   Si prefiere no ingresar la contraseña, podrá acceder al contenido del volumen y este se cifrará con FileVault, pero Dell no administrará el cifrado.

**NOTA:**

En la consola de administración, el administrador podrá ver que ahora se administra el terminal con Dell Server.

# Reciclado de claves de recuperación de FileVault

Si tiene problemas de seguridad con un paquete de recuperación o si algún riesgo afecta a un volumen o a las claves, puede reciclar el material de la clave de ese volumen.

Puede reciclar las claves de unidades de inicio y de unidades que no son de inicio en Mac OS X.

Para reciclar el material de la clave:

1. Descargue un paquete de recuperación desde la consola de administración y cópielo en el escritorio de la computadora.
2. Abra *Preferencias del sistema* y haga clic en **Dell Encryption Enterprise**.
3. Haga clic en la pestaña **Volúmenes del sistema**.
4. Arrastre el paquete de recuperación del paso 1 en la partición adecuada.

   Un cuadro de diálogo le solicitará si desea reciclar las claves de FileVault.

5. Haga clic en **Aceptar**.

   El cuadro de diálogo confirma que las claves se han reciclado correctamente.

6. Haga clic en **Aceptar**.

   **NOTA:**

   Ahora, las claves del paquete de recuperación para esta unidad son obsoletas. Deberá descargar un nuevo paquete de recuperación desde la consola de administración.

# Experiencia del usuario

Para disfrutar de la máxima seguridad, el software de cliente desactiva la función *Inicio de sesión automático* en los equipos con Mac OS X.

Asimismo, el software cliente requiere automáticamente el uso de la función de Mac OS X *solicitar contraseña cuando el equipo entra en suspensión o aparece el protector de pantalla.* Antes de aplicarse la autenticación, también se permite una cantidad de tiempo configurable en el modo de suspensión/protector de pantalla. El software cliente permite que un usuario establezca un valor hasta cinco minutos antes de que se aplique la autenticación.

Los usuarios pueden utilizar el equipo normalmente mientras se lleva a cabo el barrido de cifrado. Se cifran todos los datos en el volumen del sistema actualmente iniciado, incluido el sistema operativo mientras éste siga funcionando.

Si el equipo se reinicia o entra en modo de suspensión, el barrido de cifrado hace una pausa y se reanuda automáticamente tras el reinicio o la activación.

El software cliente no admite el uso de las imágenes de hibernación que utiliza la función *Suspensión segura* de Mac OS X para activar el equipo si la batería se descarga totalmente durante la suspensión.

Para que no afecte al usuario, el software cliente actualiza automáticamente el modo de suspensión del sistema para deshabilitar la hibernación y aplicar esta configuración. El equipo aún puede entrar en suspensión, pero el estado actual del sistema se mantendrá solo en memoria. Por lo tanto, la computadora se reiniciará totalmente si durante la suspensión se apagó por completo, lo que podría producirse si se agota o se reemplaza la batería.

## Copiar una regla de la lista de aceptación

Un elemento de menú oculto permite que un usuario copie una regla de la lista de aceptación para medios extraíbles.

1. Abra **Preferencias del sistema** y haga clic en **Dell Encryption Enterprise**.
2. Seleccione la pestaña **Medios extraíbles**.
3. Haga clic con el botón derecho del mouse en una fila de archivos, y simultáneamente pulse la tecla de comando.

   Se mostrará el elemento de menú oculto.

4. Haga clic en **Copiar una regla de la lista de aceptación** en el caso del medio extraíble actual. La regla de la lista de aceptación se copia en el Portapapeles.
5. Acceda al Portapapeles, copie la regla de la lista de aceptación y envíela al administrador.

Si la política de *Cifrado de los medios de Mac* se establece en **Activada**, se cifrarán los datos, incluidas las unidades Thunderbolt.

A fin de excluir un dispositivo o un grupo de estos para impedir que se escriban datos cifrados en la unidad Thunderbolt o en Encryption External Media, puede utilizar la regla de la lista de aceptación para modificar los valores.

Utilice la regla completa para especificar una unidad concreta para la lista de aceptación, por ejemplo:

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=001CC0EC3447AA308699119F

**NOTA:**

Deberá sustituir los valores de ejemplo con la información de su unidad.

**NOTA:**

Debe activar HFS Plus. Consulte Activar HFS Plus.

Para excluir a los dispositivos SATA de la aplicación de la política Mac Media Encryption cuando se conectan a través de Thunderbolt:

tbolt=1;bus=SATA

También puede incluir en la lista de aceptación o excluir medios de Encryption External Media en función de:

- **Tamaño del medio**

  Regla de la lista de aceptación para excluir medios grandes de la protección de Encryption External Media:

  tamaño <op> <especificador de tamaño>

  <op> puede ser =, <=, >=, <, >

  <especificador de tamaño> es de la forma entero decimal con un sufijo opcional de {K, M, G, T} alineado en 1000, no 1024. Por ejemplo, para excluir medios o una unidad mayor de 500000000 bytes de Encryption External Media, utilice uno de los siguientes:

  tamaño >= 500000000

  tamaño >= 500000K

  tamaño >= 500M

- **Tipo de sistema de archivos**

  Regla de la lista de aceptación:

  fstype=<fstype>

  <fstype> puede ser ExFAT, FAT o HFS+

Para excluir ambos, a continuación se muestra un ejemplo para medios de HFS+ de 1 TB y mayor:

size>=1T;fstype=HFS+

# Recuperación

En ocasiones, tendrá que acceder a los datos que se encuentran en los discos cifrados. Como administrador de Dell, puede acceder a los discos cifrados sin descifrarlos, lo que le ahorra un tiempo muy valioso.

Quizá tenga que acceder a los datos cifrados del usuario por muchos motivos, pero a continuación indicamos algunos casos típicos de uso:

- Alguien deja la empresa y nadie sabe la contraseña.
- Un usuario no puede recordar la contraseña.

En esta sección, se muestra el proceso para utilizar la Recuperación de FileVault cuando el cifrado de FileVault se encuentra en el terminal que se recuperará. FileVault puede se puede utilizar con si el cliente Encryption utiliza macOS Sierra 10.12.6. La recuperación de FileVault también se utiliza con Fusion Drive.

## Montar volumen

**Requisitos previos**

- Una computadora o un volumen externo de recuperación sin cifrar para ejecutar la utilidad de recuperación
- Un cable FireWire o Thunderbolt, en función de su hardware

- El ID de dispositivo/ID único de la computadora destinada para la recuperación: en la mayoría de los casos, puede encontrar la computadora destinada para la recuperación en la consola de administración buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para él. El formato del ID exclusivo/ID de dispositivo es "MacBook.Z4291LK58RH de Juan García".
- Medio de instalación de Dell

## Proceso

1. Como administrador de Dell, inicie sesión en la Consola de administración.
2. En el panel izquierdo, haga clic en **Administración > Recuperar extremo**.
3. En *Buscar*, ingrese el nombre de dominio calificado del terminal para recuperar y haga clic en el icono de búsqueda.
4. Haga clic en el vínculo **Recuperar** del dispositivo.
5. Si el extremo requiere una recuperación mejorada, se mostrará una solicitud para una contraseña. Asigne una nueva contraseña al paquete de claves de clave de cifrado que está a punto de descargar.

   **NOTA:**

   Debe recordar esta contraseña para acceder a las claves de recuperación.
6. A fin de guardar el paquete de recuperación en el volumen de recuperación o computadora externa que para que ejecute la utilidad de recuperación a fin de realizar la operación de recuperación, haga clic en **Descargar** y, a continuación, en **Guardar**.

   Se ha descargado el archivo de recuperación <nombre_máquina.dominio>.csv.
7. Inicie el equipo de destino desde un volumen de recuperación externo creado previamente. Para hacerlo puede, o bien iniciar el panel de Disco de inicio en Preferencias del sistema y seleccionar el volumen de recuperación, o bien mantener pulsada la tecla **Opción** mientras reinicia el equipo y seleccionar el volumen de recuperación en el Administrador de inicio de prearranque.

   O bien

   Inicie el equipo de destino para la recuperación en Modo de disco de destino. Para hacerlo puede, o bien iniciar el panel de Disco de inicio en Preferencias del sistema y hacer clic en **Modo disco de destino**, o bien mantener pulsada la tecla **T** mientras reinicia el equipo.

   **NOTA:**

   La protección por contraseña del firmware bloquea la capacidad de utilizar la tecla T en el inicio para entrar en Modo de disco de destino. Dispone de más información sobre el Modo de disco de destino en la página de Apple en http://support.apple.com/kb/HT1661.

   Conecte ahora este equipo al equipo host que realizará la operación de recuperación mediante un cable FireWire o Thunderbolt, en función de su hardware.
8. Monte el archivo Dell-Encryption-Enterprise-<versión>.dmg.

   **NOTA:**

   La Utilidad de recuperación debe ser de la misma versión o una versión más nueva a la del software de cliente instalado en el equipo destinado a la recuperación.
9. Seleccione el volumen o la unidad que necesita recuperación y haga clic en **Continuar**.

   Mediante la selección de la unidad, se recuperan todos los volúmenes en la unidad a la vez.
10. Seleccione el paquete de recuperación (que se guardó en el paso 6) y haga clic en **Abrir**.
11. Haga clic en **Cerrar**.

Ahora podrá abrir la ventana Finder y acceder a los datos del volumen cifrado como lo haría con un volumen normal. Todos los datos se cifrarán y descifrarán de forma transparente a medida que se transfieran archivos entre los volúmenes.

# Recuperación de FileVault

La recuperación de un volumen con cifrado FileVault administrado se determina según las estipulaciones de Apple. Este proceso se automatiza siempre que sea posible, aunque se necesita la ejecución de un par de pasos adicionales.

La utilidad de recuperación de Dell simplifica el uso de las herramientas de recuperación de Apple con secuencias de comandos para ayudar con el montaje de un volumen o, en algunos casos, para descifrarlos. La funcionalidad de recuperación de FileVault viene determinada por el sistema operativo instalado en Recovery HD y la partición de destino asociada.

Un volumen cifrado de FileVault se puede recuperar solo desde la partición de Recovery HD que se escribe en todas las unidades de disco que ejecuten Mac OS X 10.9.5 o posterior. Este requisito elimina la posibilidad de realizar una operación de recuperación directamente desde la utilidad de recuperación de Dell.

Existen dos métodos de recuperación, en función de si la clave de recuperación de FileVault es una clave de recuperación personal o institucional. Siempre existe una clave de recuperación válida. Si existe una clave de recuperación personal, Dell recomienda que utilice la entrada más reciente para dicha clave. Si esa clave no funciona, utilice entonces la cadena de claves de recuperación institucional.

- Clave de recuperación personal: el cifrado con FileVault existente lo administra Dell Server. Si la entrada más reciente en el paquete de recuperación contiene una entrada RecoveryKey, siga los pasos que se detallan en Clave de recuperación personal. A continuación, se presenta un ejemplo de RecoveryKey:

  ```
  RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
  ```

- Cadena de claves de recuperación (acción poco común): este método de recuperación se basa en el uso de una clave de recuperación institucional de FileVault.

  Si la entrada más reciente en el paquete de recuperación contiene una entrada KeychainKey, siga los pasos que se detallan en Cadena de claves de recuperación. A continuación, se presenta un ejemplo de KeychainKey:

  ```
  KeychainKey</key><data>a3ljaAABAAAAA...
  ```

## Clave de recuperación personal

Por lo general, la práctica recomendada es recuperar el volumen de arranque antes de recuperar los volúmenes que no son de arranque. De lo contrario, se monta cualquier otro volumen que se haya cifrado. Normalmente, se corrigen los problemas de los volúmenes que no son de arranque con la recuperación del volumen de arranque.

**Requisitos previos**

- Una unidad de inicio externa
- La Id. de dispositivo/Id. exclusiva del equipo destinado a la recuperación. En la mayoría de los casos, puede encontrar la computadora destinada para la recuperación en la consola de administración buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para él. El formato del ID de dispositivo/ID único es "MacBook.Z4291LK58RH de Juan García".
- Medio de instalación de Dell

**Consola de administración: almacenamiento del paquete de recuperación**

1. Abra la consola de administración.
2. En el panel izquierdo, haga clic en **Poblaciones > Extremos**.
3. Busque el dispositivo que se recuperará.
4. Haga clic en el nombre de dispositivo para abrir la página Detalle del extremo.
5. Haga clic en la pestaña **Detalles y acciones**.
6. En *Detalles de Shield*, haga clic en el vínculo **Claves de recuperación de dispositivos**.
7. Para guardar el paquete de recuperación en el volumen de recuperación o equipo externo que ejecutará la utilidad de recuperación para realizar la operación de recuperación, haga clic en **Descargar** y, a continuación, en **Guardar**.
8. Ingrese una ubicación para el paquete de recuperación y haga clic en **Guardar**.

**Proceso: instalación del archivo .dmg**

1. Copie el paquete de recuperación y el archivo **Dell-Encryption-Enterprise-<version>.dmg** en la unidad USB de inicio.
2. Mantenga presionada la tecla **Opción** mientras reinicia la computadora de destino y seleccione el volumen externo de instalación completa del sistema operativo en el administrador de inicio previo al arranque para arrancar dicha computadora desde un volumen externo de instalación completa del sistema operativo creado previamente. Para crear un volumen de inicio, consulte https://support.apple.com/en-us/HT202796.
3. Monte el archivo **Dell-Encryption-Enterprise-<versión>.dmg**.

**Proceso: inicio de la utilidad de recuperación de Dell y recuperación del volumen FileVault**

1. En la carpeta Utilidades que se encuentra en el medio de instalación de Dell, inicie la Utilidad de recuperación de Dell.

   Se muestra el diálogo *Utilidad de recuperación de Dell > Seleccione los volúmenes*.

   **NOTA:**

   La Utilidad de recuperación debe ser de la misma versión o una versión más nueva a la del software de cliente instalado en el equipo destinado a la recuperación.

2. En *Utilidad de recuperación Dell > Seleccionar volúmenes*, seleccione el volumen FileVault.
   - Cuando se recupera un sistema operativo, la práctica recomendada es arrancar una computadora con el mismo sistema operativo o superior.
   - Si tiene volúmenes cifrados que no son de inicio, normalmente recuperará primero la partición de inicio.
3. Haga clic en **Continuar**.
4. Encuentre y seleccione el paquete de recuperación (guardado anteriormente) y haga clic en **Abrir**.
5. Si aparece el cuadro de diálogo *Seleccionar registro de recuperación*, vea la columna *Fecha de custodia*, seleccione la fecha más reciente para el tipo de clave de recuperación personal y haga clic en **Continuar.**

   **NOTA:**

   Con una fecha de custodia anterior, puede que la clave ya no sea válida.

   Aparece el *Resultado de la operación de recuperación*.
   - Para unidades de inicio, la herramienta de recuperación proporciona una clave de recuperación personal que le permite iniciar con la recuperación FileVault de Apple estándar. Puede arrancar en la partición de destino e ingresar la clave de recuperación personal para realizar la autenticación de previa al arranque, algo que puede variar según el sistema operativo.
   - Para las unidades que no son de inicio, solo se muestra la clave de recuperación personal. Se proporciona el botón Desbloqueo para desbloquear y montar el volumen.
6. Realice una de estas opciones:
   - Recuperar el volumen de arranque (acción más común)
   - Recuperar un volumen que no es de arranque (acción poco común)

**Recuperar el volumen de arranque (acción más común)**

Para la mayoría de los casos de recuperación, utilice esta opción a fin de recuperar el volumen de arranque:
1. Digite la clave o haga clic en **Imprimir clave de recuperación**.
2. Haga clic en **Cerrar**.
3. Inicie el volumen que desea recuperar mediante el Administrador de inicio de arranque previo, si es necesario.

   En la computadora, se muestran íconos para varios usuarios o se solicita una contraseña.
4. Seleccione un usuario si corresponde y, a continuación, haga clic en **?**. en la pantalla de inicio de sesión.
5. Haga clic en la flecha que se muestra.
6. Escriba la clave de recuperación y pulse **Intro**.
7. En el cuadro de diálogo, ingrese la nueva contraseña de usuario.

**Opciones de recuperación de volúmenes que no son de arranque** (acción poco común): ejecute una de las siguientes acciones:

**Recuperar un volumen que no es de arranque**

Si se daña el volumen de arranque o se borran sus contenidos y existen volúmenes secundarios, puede montar estos volúmenes que no son de arranque.
1. Haga clic en **Desbloquear**. Se realiza el montaje del volumen.
2. Haga clic en **Cerrar**.

**Descifrar volumen: haga clic en el botón**
1. Haga clic en **Descifrar**. Un cuadro de diálogo y una barra de progreso indican el proceso de descifrado.
2. Una vez que se complete, haga clic en **Cerrar**.
3. Inicie el equipo en volumen descifrado para poder utilizarlo.

**Descifrar volumen: ejecute el comando desde el terminal**
1. Copie el comando en el área *Descifrar volumen*.
2. Haga clic en **Cerrar**.
3. Ejecute el comando en el terminal.

## Cadena de claves recuperación

Debe ejecutar la Utilidad de recuperación de Dell mientras se inicia en un volumen de recuperación no cifrado.

**Requisitos previos**

- Un equipo o un volumen externo de recuperación que ejecutará la utilidad de recuperación
- Una unidad USB
- Un cable FireWire
- Medio de instalación de Dell

**Consola de administración: almacenamiento del paquete de recuperación**

1. Abra la consola de administración.
2. En el panel izquierdo, haga clic en **Poblaciones > Extremos**.
3. Busque el dispositivo que se recuperará.
4. Haga clic en el nombre de dispositivo para abrir la página Detalle del extremo.
5. Haga clic en la pestaña **Detalles y acciones**.
6. En *Detalles de Shield*, haga clic en el vínculo **Claves de recuperación de dispositivos**.
7. Para guardar el paquete de recuperación en el volumen de recuperación o equipo externo que ejecutará la utilidad de recuperación para realizar la operación de recuperación, haga clic en **Descargar** y, a continuación, en **Guardar**.
8. Ingrese una ubicación para el paquete de recuperación y haga clic en **Guardar**.

**Proceso**

1. Conecte una unidad externa al sistema que se va a recuperar.

   La unidad externa debe tener un volumen de inicio Mac OS.
2. Para arrancar la unidad externa, mantenga presionada la tecla **Opción** y utilice el selector de arranque para seleccionar e iniciar el arranque de este volumen.
3. Copie el paquete de recuperación desde la Consola de administración.
4. Monte el archivo .dmg de instalación.
5. En la carpeta Utilidades, ejecute la Utilidad de recuperación de Dell.

   Se muestra el diálogo *Utilidad de recuperación de Dell > Seleccione los volúmenes*.
6. Seleccione el volumen FileVault que se va a recuperar y haga clic en **Continuar.**

   Se muestra el diálogo *Elija el paquete de recuperación*.
7. Seleccione el paquete de recuperación y haga clic en **Abrir**.

   Si existe más de una clave de recuperación para ese disco, se mostrará la pantalla *Seleccionar registro de recuperación*.
8. En la columna Fecha de custodia, seleccione la fecha más reciente para el tipo de recuperación de cadena de claves y haga clic en **Continuar.**

   **NOTA:**

   Con una fecha de custodia anterior, puede que la clave ya no sea válida.

   Se muestra el diálogo *Instrucciones de recuperación de FileVault*.
9. Lea las instrucciones y haga clic en **Continuar**.

   Se muestra el diálogo *Confirmar operación de recuperación*.
10. Resalte el volumen FileVault que se va a recuperar y haga clic en **Continuar.**

    Se muestra el diálogo *Elegir ubicación para los archivos de recuperación*, que le solicita que seleccione una ubicación para almacenar los archivos de recuperación.

    Esta ubicación debe ser la ubicación que utilice para la recuperación, ya que las secuencias de comandos contienen rutas de acceso absolutas a los archivos de datos. **No** copie estos archivos en Recovery HD.

    Dell recomienda que guarde estos archivos en la raíz de una unidad extraíble, como una unidad USB.

    **NOTA:**

    Asegúrese de que todos los usuarios tengan acceso de lectura/escritura al USB u otro disco que utilice para almacenar la clave de recuperación y que el disco tenga el espacio adecuado. Si no tiene derechos para un disco seleccionado o si el disco no tiene espacio, aparecerá un error indicándole que las claves de recuperación no se han almacenado.
11. Seleccione una ubicación y haga clic en **Guardar**.

Se muestra el diálogo *Resultado de la operación de recuperación*, que indica los archivos se han creado.

12. Haga clic en **Cerrar.**
13. Después de iniciarse el volumen de Recovery HD, ingrese el nombre y la ruta de acceso de la secuencia de comandos.

    **NOTA:**

    Si almacena los archivos cerca de la raíz de un volumen, se acortará la ruta de acceso que debe escribir.

    En la sección Resultado de la operación de recuperación, se muestra la clave.

    La utilidad de recuperación produce los archivos en la ubicación seleccionada y muestra los comandos exactos que se deben ejecutar desde el volumen de Recovery HD para montar o descifrar el volumen de FileVault.
14. Después de que se generen estos archivos, copie las cadenas de comandos que se muestran en el cuadro de diálogo final *Resultado de la operación de recuperación.*
15. Reinicie en Recovery HD mediante uno de estos modos:
    - Mantenga presionadas simultáneamente las teclas **Comando y R** antes del timbre de encendido/autoprueba y durante el arranque de la computadora.

      O bien
    - Para versiones anteriores de Apple, presione la tecla de **opción** y utilice el selector de arranque para seleccionar Recovery HD.

      Se muestra el diálogo *Utilidades Mac OS X*.
16. En el menú Herramientas, seleccione **Utilidades > Terminal**.
17. Para montar el volumen y copiar archivos desde el terminal o crear una imagen del disco desde la Utilidad de disco: en el terminal, escriba la ruta de acceso completa y el nombre de la secuencia de comandos **fv2mount.sh**, por ejemplo:

    **/Volumes/recoveryFOB/fv2mount.sh**
18. Reinicie el equipo.

# Medios extraíbles

## Formatos admitidos

Se admiten medios con formato FAT32, exFAT o HFS Plus (Mac OS Extended) con esquemas de partición de Tabla de particiones GUID (GPT) o Registro de arranque maestro (MBR). Debe activar HFS Plus.

**NOTA:**

MAC aún no admite la grabación de CD/DVD para Encryption External Media. Sin embargo, el acceso a unidades de CD/DVD no está bloqueado, incluso si se selecciona la política *Bloquear acceso a medios que no se pueden proteger con EMS*.

### Activar HFS Plus

Para activar HFS Plus, añada lo siguiente al archivo .plist.

<key>EMSHFSPlusOptIn</key>

<true/>

**NOTA:**

Dell recomienda que se pruebe esta configuración antes de introducirla en el entorno de producción.

HFS Plus no es compatible con:

- Versiones: los datos de versiones existentes se eliminan del disco.
- Vínculos físicos: durante un barrido de cifrado de los medios extraíbles, el archivo no se cifra. Un cuadro de diálogo recomienda expulsar los medios.
- Medios que contienen copias de seguridad de Time Machine:

- Los medios que se pueden reconocer como destino para un respaldo de Time Machine se introducen automáticamente en la lista de aceptación para permitir que los respaldos continúen.
- El resto de medios extraíbles con copias de seguridad de Time Machine se basan en la política que rige los medios no aprovisionados y sin protección. Consulte las políticas *Acceder a medios sin blindaje en EMS* y *Bloquear el acceso a medios que no se pueden proteger en EMS*.

  **NOTA:**

  Para una unidad nueva que todavía no cuenta con copias de seguridad, el usuario debe copiar su regla de la lista de aceptación y enviársela para especificar su unidad de Time Machine en la lista de aceptación. Consulte Copiar una regla de la lista de aceptación.

## Encryption External Media y actualizaciones de políticas

En el sistema en el que se aprovisionó (o se recuperó) el medio extraíble, las políticas se actualizarán en el medio extraíble en el momento del montaje.

## Excepciones de cifrado

Los atributos extendidos no se cifran en medios extraíbles.

## Errores en la pestaña Medios extraíbles

- En un equipo no protegido por Shield, no sustituya un archivo cifrado por una versión descifrada del archivo. Más adelante, esta acción podría impedir el descifrado. También podría mostrarse como un error en la pestaña Medios extraíbles.
- Si se invalida un marcador de fin de archivo, por ejemplo, si un archivo se sobrescribe con nuevo contenido fuera del control de Encryption External Media y después lo monta en Encryption External Media, se mostrará un error de fin de archivo en la pestaña Medios extraíbles.
- Si se convierten archivos, el medio debe tener más espacio libre que el tamaño del archivo más grande que se va a convertir. Si se muestra un triángulo amarillo de aviso en el área de estado de Medios extraíbles, haga clic en él. Si aparece un mensaje de *Espacio insuficiente*, haga lo siguiente:

  1. Tome en cuenta la cantidad de espacio que se debe liberar en el dispositivo. En el informe se muestra una lista de los archivos y su tamaño.
  2. Vacíe la papelera. Conforme libere espacio, Encryption External Media cifrará automáticamente los archivos adicionales.
  3. Si borra cualquier archivo o carpeta, asegúrese de volver a vaciar la papelera.

## Mensajes de auditoría

Los mensajes de auditoría se envían a Dell Server.

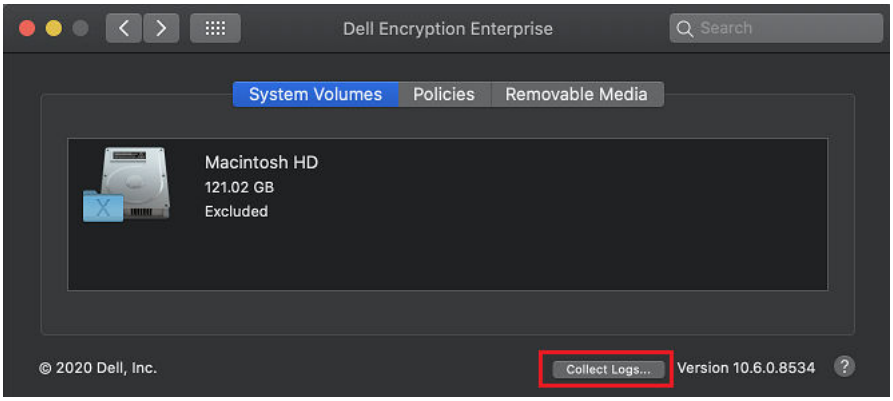
En el caso de Endpoint Security Suite Enterprise for Mac, realice lo siguiente para ver mensajes de auditoría:

1. Como un administrador de Dell, inicie sesión en la Management Console.
2. En el panel izquierdo, haga clic en **Poblaciones > Enterprise o Terminales**.
3. Seleccione la pestaña **Eventos de amenaza avanzada**.

Para obtener más información, consulte *AdminHelp*.

# Recopilar archivos de registro para Endpoint Security Suite Enterprise

En *Preferencias del sistema > Dell Encryption Enterprise > Volúmenes del sistema*, el botón *Recopilar registros* en la parte inferior derecha permite a un administrador generar previamente registros para la compatibilidad. Esta acción puede afectar el rendimiento mientras se recopilan los registros.




DellLogs.zip contiene los registros de Mac Encryption Enterprise y Advanced Threat Prevention. Para obtener información sobre cómo recopilar los registros, consulte http://www.dell.com/support/article/us/en/19/SLN303924.

# Desinstalar el cliente Encryption para Mac

Para desinstalar el software cliente puede ejecutar la aplicación **Desinstalar Dell Encryption Enterprise.** Para desinstalar el software cliente, siga los pasos que se indican a continuación.

**NOTA:**

Antes de ejecutar la aplicación de desinstalación, el disco debe estar descifrado totalmente.

1. Si el disco está cifrado, establezca la política de *Dell Volume Encryption* de la computadora como **Desactivada** en la Management Console y confirme la política.

   Se mostrará un cuadro de diálogo que solicitará el acceso a las Preferencias del sistema y el control del equipo para que el software cliente pueda descifrar el disco.

   a. Haga clic en **Abrir las preferencias del sistema**.

      Si la opción **Denegar** está seleccionada, la desinstalación y descifrado no podrán continuar.

   b. Ingrese la contraseña del administrador.
2. Después de que el disco se haya descifrado totalmente, reinicie el equipo (cuando se le solicite).
3. Tras el reinicio de la computadora, inicie la aplicación **Desinstalar Dell Encryption Enterprise** (ubicada en la carpeta Utilidades en Dell-Encryption-Enterprise-<version>.dmg del medio de instalación de Dell).

   Los mensajes muestran el estado de la desinstalación.

   El cliente Encryption para Mac ahora está desinstalado y la computadora se puede utilizar con normalidad.

# Activación como administrador

La Herramienta del cliente ofrece al administrador nuevos métodos para activar el software cliente en un equipo Mac y examinar el software cliente. Hay dos métodos de activación disponibles:

- Activación mediante el uso de las credenciales de administrador
- Activación temporal que emula al usuario sin dejar huella en el equipo.

Ambos métodos pueden utilizarse directamente mediante el shell o en una secuencia de comandos.

**NOTA:**

No active el software cliente en más de cinco equipos con la misma cuenta de red. Podría causar vulnerabilidades graves de seguridad y afectar al rendimiento de Dell Server.

**Requisitos previos**

- El cliente Encryption para Mac debe estar instalado en la computadora remota.
- No lo active mediante la interfaz de usuario del cliente antes de intentar activarlo desde una ubicación remota.

## Activar

Utilice este comando para activar el cliente como administrador.

Ejemplo:

**client -a** *username@domain.com password admin admin*

## Activar temporalmente

Utilice este comando para activar el cliente sin dejar huella en el equipo.

1. Abra un shell o utilice una secuencia de comandos para activar el software cliente:

   ***client*** *-at username@domain.com password*

2. Utilice la Herramienta del cliente para recuperar información sobre el software cliente, sus políticas, el estado del disco, la cuenta de usuario, etc. Para obtener más información sobre la Herramienta de cliente, consulte Herramienta de cliente.

   **NOTA:**

   Tras la activación, la información sobre el software cliente, incluidas las políticas, el estado del disco y la información del usuario, también está disponible en Preferencias del sistema de Dell Encryption Enterprise.

# Referencia del cliente Encryption

## Acerca de la protección por contraseña para firmware opcional

**NOTA:**

Los equipos Mac más recientes no admiten la Protección por contraseña del firmware. La Protección por contraseña del firmware se admite en los modelos siguientes:

- iMac10.*
- iMac11.*
- Macmini4.*
- MacBook7.*
- MacBookAir2.*
- MacBookPro7.*
- MacPro5.*
- XServe3.*

Por ejemplo, iMac10.1, iMac11.1 y iMac11.2 son compatibles con la protección por contraseña para firmware opcional (como se indica con el asterisco [*]), pero iMac12.1 o versiones posteriores no lo son.

**NOTA:**

Cuando la opción de clave FirmwarePasswordMode se establece en **Opcional**, solo desactiva el cumplimiento de la protección por contraseña del firmware del cliente. **No** elimina ninguna protección por contraseña ya existente del firmware. Puede quitar la contraseña existente del firmware mediante la Utilidad de contraseñas de firmware de Mac OS X.

Si tiene previsto utilizar Boot Camp (consulte Cómo activar Boot Camp en Mac OS X para obtener instrucciones) en equipos Mac cifrados, **debe** configurar el cliente para que **no** utilice la protección por contraseña del firmware.

Los equipos Mac utilizan la protección por contraseña del firmware para mejorar la seguridad del acceso al equipo. De manera predeterminada, en los equipos Mac la protección está *DESACTIVADA*. Durante la instalación del cliente, ya sea una nueva instalación o la actualización de una versión del cliente anterior, puede editar el archivo com.dell.ddp.plist existente para permitir que la clave *FirmwarePasswordMode* se establezca en *Necesaria* u *Opcional*. La opción *Necesaria* es el ajuste predeterminado que obliga a utilizar la protección por contraseña del firmware, mientras que el valor *Opcional* retira la obligación de utilizar la contraseña del firmware. Tras la instalación o actualización, el cliente evalúa el archivo de instalación com.dell.ddp.plist modificado durante el reinicio.

**NOTA:**

Para impedir que los usuarios cambien la posición de seguridad del equipo, el cliente no acepta cambios en la clave FirmwarePasswordMode tras la instalación del software cliente.

Para cambiar el valor de esta clave tras la instalación o la actualización, inicie un proceso de descifrado del disco y, a continuación, vuelva a habilitar el cifrado.

En el caso de que la protección por contraseña del firmware de Mac OS X sea **obligatoria**, siga el procedimiento normal de instalación/actualización del cliente que se describe en Instalación/actualización del cliente Encryption para Mac.

# Cómo utilizar Boot Camp

## Compatibilidad de Mac OS X con Boot Camp

**NOTA:**

Al utilizar Boot Camp, Dell Encryption Enterprise no cifra el sistema operativo Windows. Además, si existen dos o más particiones macOS de arranque en el dispositivo, Encryption Enterprise cifra solo el volumen principal.

Boot Camp es una utilidad que se incluye en Mac OS X y que le ayudará a instalar Windows en equipos Mac en una configuración de doble arranque. Boot Camp es compatible con los siguientes sistemas operativos Windows:

- Windows 7 y 7 Home Premium, Professional y Ultimate (64 bits)
- Windows 8.1 y 8.1 Pro (64 bits)

**NOTA:**

Windows 7 es compatible con Boot Camp 4 o 5.1. Windows 8.1 y posterior solo es compatible con Boot Camp 5.1.

Para utilizar Endpoint Security Suite Enterprise para Windows en Boot Camp en una computadora con Endpoint Security Suite Enterprise para Mac, el volumen del sistema se debe cifrar mediante el cliente Encryption para Mac con FileVault2. Consulte Instalación/actualización mediante la línea de comandos para obtener instrucciones.

**NOTA:**

Si la partición de Windows es un candidato para Encryption External Media, asegúrese de incluirlo en la lista de aceptación o se cifrará. Consulte Copiar una regla de la lista de aceptación.

**NOTA:**

Antes de implementar las políticas del cliente que habilitan el cifrado, deberá asegurarse de que Windows está instalado. Después de que el cliente empiece el proceso de cifrado, no permitirá las operaciones de partición de disco requeridas por Boot Camp.

## Recuperación de Endpoint Security Suite Enterprise para Windows en Boot Camp

Para recuperar Endpoint Security Suite Enterprise para Windows si se ejecuta en un volumen Boot Camp, también debe crear un volumen Boot Camp en una unidad externa.

**Requisitos previos**

- Una unidad de inicio externa
- La Id. de dispositivo/Id. exclusiva del equipo destinado a la recuperación. En la mayoría de los casos, puede encontrar la computadora destinada para la recuperación en la consola de administración buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para él. El formato del ID de dispositivo/ID único es "MacBook.Z4291LK58RH de Juan García".

**Proceso**

1. En una unidad externa, cree un volumen Boot Camp.

   Los pasos son similares a los de creación de un volumen Boot Camp en su sistema local. Consulte http://www.apple.com/support/bootcamp/.

2. En la consola de administración, copie el paquete de recuperación en alguno de los siguientes medios:
   - Unidad USB arrancable

O bien

- Partición FAT en el volumen Boot Camp externo

3. Apague el equipo con el volumen Boot Camp que se va a recuperar.
4. Conecte la unidad externa al equipo.

   Esta unidad contiene el volumen Boot Camp creado en el paso 1.

5. Para arrancar la computadora desde la unidad externa de Boot Camp, realice uno de los siguientes pasos:

   - Mantenga presionadas simultáneamente las teclas **Comando y R** antes del timbre de encendido/autoprueba y durante el arranque de la computadora.

     O bien

   - Para las versiones anteriores de Apple, presione la tecla de **opción** mientras enciende la computadora.

     Se muestra el diálogo *Utilidades Mac OS X*.

6. Seleccione el volumen de Boot Camp (Windows) que se encuentra en la unidad externa.
7. En la unidad USB o partición FAT, haga clic con el botón derecho del ratón en el paquete de recuperación (del paso 2) y seleccione **Ejecutar como administrador**.
8. Haga clic en **Sí**.
9. En el cuadro de diálogo Dell Encryption Enterprise, seleccione una opción:

   - *Mi sistema no arranca*: si el usuario no puede arrancar el sistema, seleccione la primera opción

     O bien

   - *Mi sistema no me permite el acceso a datos cifrados*: si el usuario no puede acceder a algunos archivos cifrados cuando inicia sesión en el sistema, seleccione la segunda opción.

10. Haga clic en **Siguiente**.

    Se mostrará la pantalla Información de copia de seguridad y recuperación.

11. Haga clic en **Siguiente**.
12. Seleccione el volumen Boot Camp que se va a recuperar.

    **NOTA:**

    Este **no** es el volumen Boot Camp externo.

13. Haga clic en **Siguiente**.
14. Ingrese la contraseña asociada a este archivo.
15. Haga clic en **Siguiente**.
16. Haga clic en **Recuperar.**
17. Haga clic en **Finalizar**.
18. Cuando se le solicite que reinicie, haga clic en **Sí**.
19. El sistema se reinicia y podrá iniciar sesión en Windows.

# Cómo recuperar una contraseña de firmware

Incluso si el equipo cliente se ha configurado para la aplicación de la contraseña de firmware, quizá no se necesite para la recuperación. Si el equipo que se va a recuperar se puede iniciar, establezca el destino de inicio en el panel de preferencias del sistema del Disco de inicio.

En caso de que la contraseña de firmware sea necesaria para efectuar la recuperación (si el equipo no es arrancable y se aplica la protección por contraseña del firmware), siga estos pasos.

Para recuperar una contraseña de firmware, primero deberá recuperar el paquete de recuperación que contiene las claves de cifrado del disco.

1. Como un administrador de Dell, inicie sesión en la Management Console.
2. En el panel izquierdo, haga clic en **Poblaciones > Extremos**
3. Busque el dispositivo que se recuperará.
4. Haga clic en el nombre de dispositivo para abrir la página Detalle del extremo.
5. Haga clic en la pestaña **Detalles y acciones**.
6. En *Detalles de Shield*, haga clic en el vínculo **Claves de recuperación de dispositivos**.

7. Para guardar el paquete de recuperación en el volumen de recuperación o equipo externo que ejecutará la utilidad de recuperación para realizar la operación de recuperación, haga clic en **Descargar**, y haga clic en **Guardar**.
8. Abra el paquete de recuperación para recuperar la contraseña de firmware del equipo destinado a la recuperación. La contraseña del firmware se encuentra en las etiquetas de la cadena después de la clave **FirmwarePassword**.

   Por ejemplo:

   <key>FirmwarePassword</key>

   <string>Bo$vun8WDn</string>

# Herramienta de cliente

La Herramienta del cliente es un comando de shell que se ejecuta en un extremo Mac. Se utiliza para activar el cliente desde una ubicación remota o para ejecutar una secuencia de comandos a través de una utilidad de administración remota. Como administrador, puede activar un cliente y, a continuación, hacer lo siguiente:

- Activarlo como administrador
- Activar temporalmente
- Recuperar información desde el cliente Mac

Para utilizar la Herramienta del cliente de manera manual, abra una sesión de SSH e ingrese el comando que desee en la línea de comandos.

Ejemplo:

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Ingrese **cliente** solamente para mostrar las instrucciones de uso.

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/client

### Tabla 1. Comandos de la herramienta del cliente

| Comando | Propósito | Sintaxis | Resultados |
|---|---|---|---|
| Activar | Activa un cliente Mac con Dell Server, pero sin pasar por la interfaz de usuario. Para activar, se debe ingresar un nombre de usuario de dominio y una contraseña válidos.<br><br>Con la herramienta de cliente puede activar un usuario local distinto que el que ha iniciado sesión y asociar las credenciales de dominio con dicho usuario. | -a domainAccount domainPassword<br><br>-a localAccount* domainAccount domainPassword<br><br>**domainAccount** es la cuenta que se utiliza en la activación mediante la herramienta de cliente.<br><br>**localAccount** es opcional y es el usuario actual si no se especifica ninguno.<br><br>El comando de activación tiene este formato:<br><br>client -a <usuario que se activará*> <domainUser> <domainPassword><br><br>Si utiliza la política *Lista de usuarios sin autenticación* para crear clases de usuarios que no necesitan activación desde Dell Server, de manera opcional, puede utilizar la herramienta de cliente para especificar una cuenta local diferente de aquella en la que ha iniciado la sesión. Consulte Política Lista de usuarios sin autenticación en el paso 3. | 0 = Correcto<br><br>2 = Error en la activación y el motivo del fallo<br><br>6 = No se ha encontrado el usuario |
| Activar temporalmente | Activa un cliente Mac sin dejar huella. | -at domainAccount domainPassword<br><br>-at localAccount* domainAccount domainPassword | |
| Disco | Solicitar el estado del disco | -d | Se muestra el estado del disco, incluida el ID del disco, |

**Tabla 1. Comandos de la herramienta del cliente (continuación)**

| Comando | Propósito | Sintaxis | Resultados |
|---|---|---|---|
| | | | el estado del cifrado y las políticas<br>Si se devuelven llaves vacías, significa que ningún disco está cifrado. |
| Recuperación de cambio a FileVault | Reciclar las claves de recuperación para los volúmenes de FileVault | -fc deviceId recoveryPassphrase<br>-fc deviceId personalRecoveryKey<br>-fc deviceId pathToKeychain keychainPassword<br>-fc deviceId recoveryFile<br>**NOTA:**<br>La deviceId debe ser un UUID de volumen lógico o resolverse en exactamente un LVUUID. Generalmente, también funciona con un punto de montaje o devnode. | 0 = Correcto<br>7= No se ha encontrado el LVUUID<br>10 = Error de credencial<br>11 = Error de custodia |
| Política | Solicitar las políticas del cliente Mac | -P | Visualización de las políticas |
| Servidor | Sondea Dell Server por si hay políticas actualizadas en nombre del cliente Mac<br>**NOTA:**<br>El sondeo puede tardar varios minutos en terminar. | -s | 0 = Correcto<br>Cualquier otro valor indica que Dell Server o el software cliente Mac estaba ocupado o no respondía. |
| Prueba | Comprobar el estado de activación del cliente Mac | -t localAccount* | 0 (domainAccount) = Correcto<br>1 = No activado<br>6 = No se ha encontrado el usuario |
| Usuario | Solicitar información del usuario | -u localAccount* | Se muestra la información de la cuenta del usuario:<br>0 (información de la cuenta) = Correcto<br>6 = No se ha encontrado el usuario |
| Versión | Solicitar la versión del cliente Mac | -v | Se muestra la versión del cliente Mac, por ejemplo: 8.x.x.xxxx |

* La cuenta que ejecuta la herramienta de cliente se utiliza como localAccount, a menos que se especifique otra.

**La opción Plist**

La opción -plist imprime los resultados del comando con el que se combina. Sigue al comando y debe aparecer antes de sus argumentos para que los resultados se impriman como plist.

**Ejemplos**

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

Para recuperar las políticas desde el cliente e imprimirlas.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

Para activar temporalmente el cliente e imprimir el resultado.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -s ; echo$?**

Para sondear Dell Server en busca de políticas actualizadas en nombre del cliente y mostrarlas en pantalla.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

Para recuperar el estado del disco del cliente e imprimirlo.

**Códigos de retorno globales**

Sin error 0

Error de parámetro 4

Comando no reconocido 5

Tiempo de espera del socket agotado 8

Error interno 9

# 4

# Tareas

**Temas:**



# Instalar Advanced Threat Prevention para Mac

Esta sección le guiará por a través de la instalación de Advanced Threat Prevention.

Existen dos métodos para instalar Advanced Threat Prevention.

- Instalación interactiva: este método es el más sencillo. Sin embargo, este método no permite realizar personalizaciones.
- Instalación mediante la línea de comandos: se trata de un método de instalación/actualización avanzado que solo deben emplear los administradores con experiencia en sintaxis de la línea de comandos.

## Requisitos previos

Dell recomienda seguir las mejores prácticas de TI durante la implementación del software cliente. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados para las pruebas iniciales e implementaciones escalonadas para los usuarios.

Antes de empezar este proceso, asegúrese de que se cumplen los requisitos previos siguientes:

- Asegúrese de que Dell Server y sus componentes ya están instalados.

  A continuación encontrará varias guías. Si todavía no ha instalado Dell Server, siga las instrucciones de la guía más adecuada.

  *Guía de instalación y migración de Security Management Server*

  *Guía de inicio rápido y guía de instalación de Security Management Server Virtual*

- Asegúrese de disponer del nombre de host y el puerto de Dell Server. Necesita ambos para la instalación del software cliente.
- Asegúrese de que la computadora de destino cuente con conectividad de red con Dell Server.
- Si el certificado de servidor de un cliente se ha perdido o se ha autofirmado, debe deshabilitar el certificado SSL de confianza en el lado del cliente solamente.

# Instalación interactiva de Advanced Threat Prevention

Esta sección le guiará a través del proceso de instalación de Advanced Threat Prevention para Mac.

La instalación interactiva es el método más sencillo para instalar o actualizar el paquete de software cliente. Sin embargo, este método no permite realizar personalizaciones.

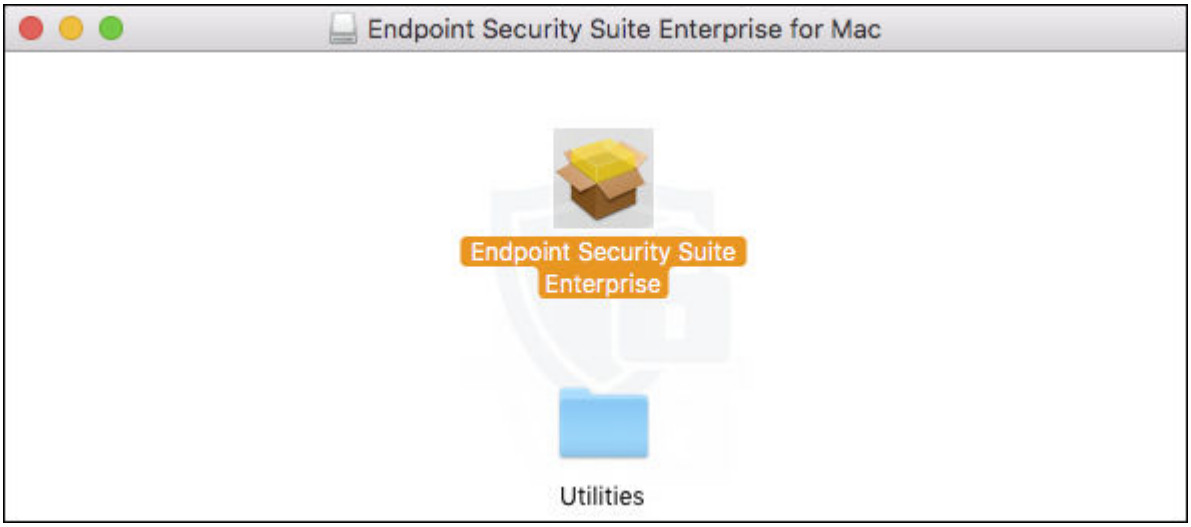
Para instalar el software cliente, siga los pasos que se indican a continuación. Debe tener una cuenta de administrador para llevar a cabo estos pasos.

**NOTA:**

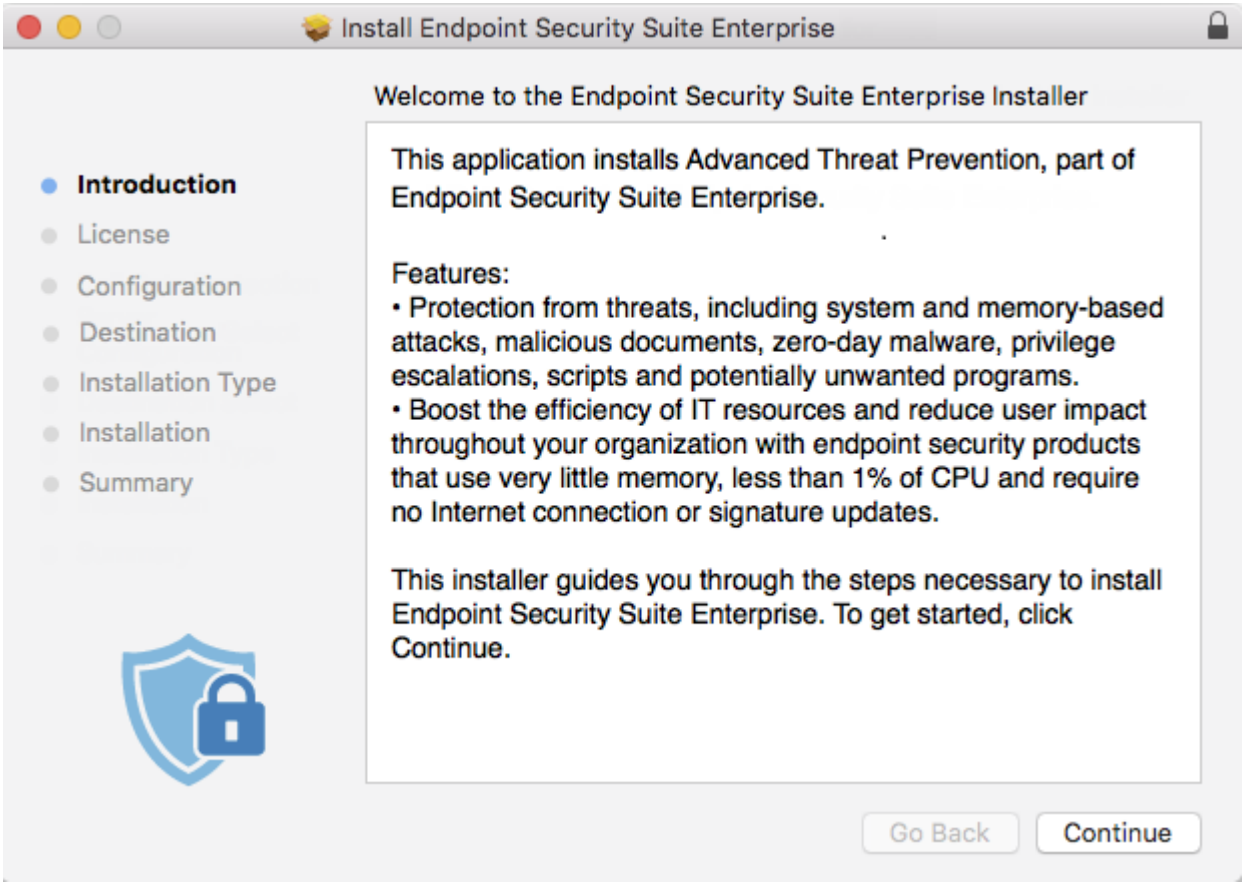
Antes de comenzar, guarde el trabajo del usuario y cierre otras aplicaciones.

1. Desde el medio de instalación de Dell, monte el archivo **Endpoint-Security-Suite-Enterprise-<version>.dmg**.

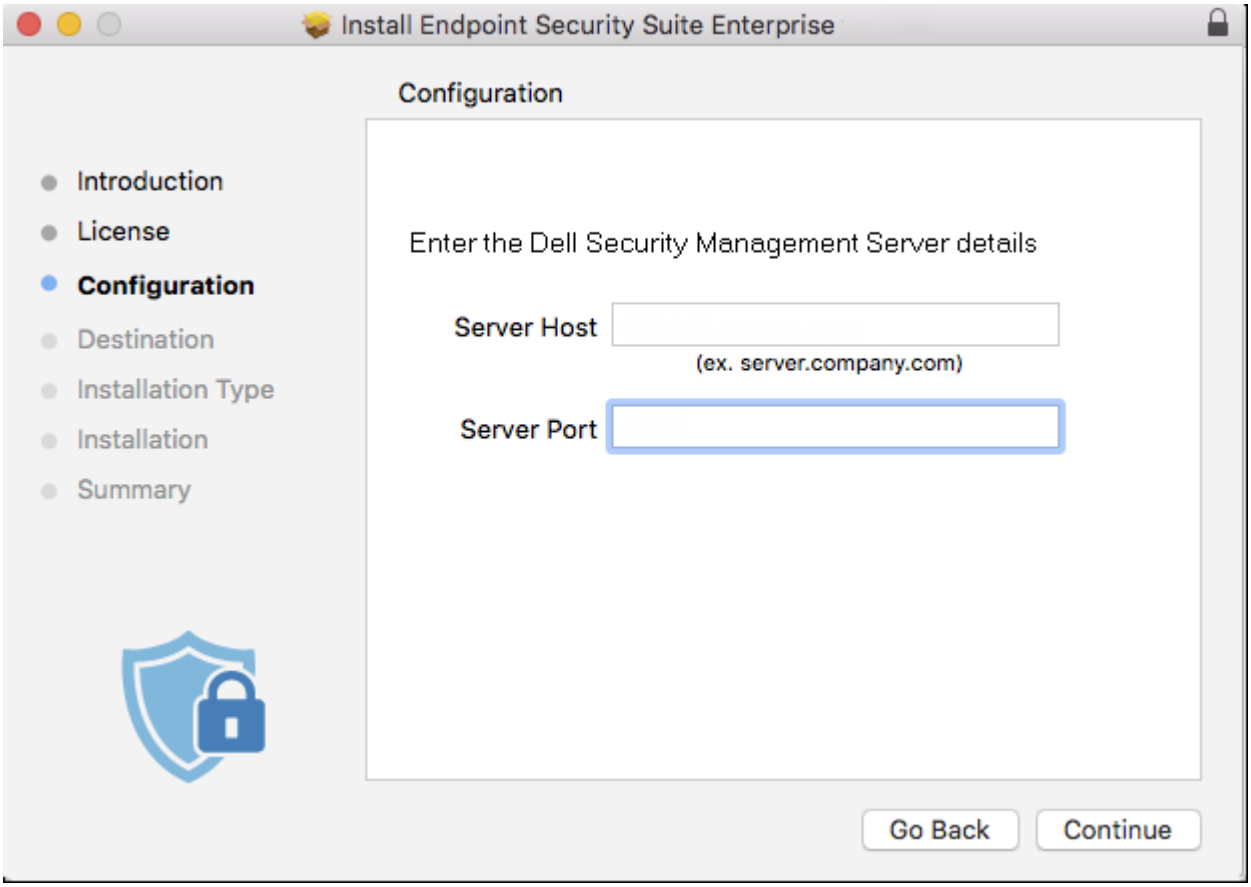
Se abrirá el paquete Endpoint Security Suite Enterprise para Mac.




2. Haga doble clic en el instalador del paquete **Endpoint Security Suite Enterprise**. Aparecerá el siguiente mensaje: *Con este paquete, se ejecutará un programa para determinar si el software se puede instalar.*
3. Haga clic en **Continuar**.
4. Lea el texto de bienvenida y haga clic en **Continuar**.




5. Revise el contrato de licencia, haga clic en **Continuar** y, a continuación, en **Aceptar** para mostrar su conformidad con los términos del contrato de licencia.
6. En el campo *Host de servidor*, ingrese el nombre completo del host de Dell Server para administrar el usuario de destino, como server.organization.com.




7. En el campo *Puerto del servidor*, ingrese **8888** y haga clic en **Continuar**.
   Cuando se haya establecido una conexión, el indicador de conectividad cambiará de rojo a verde.

   **NOTA:**

   El puerto es el puerto de servicio del servidor de Core y se puede configurar. El número de puerto predeterminado es 8888.
8. En la pantalla de instalación, haga clic en **Instalar**.
9. Cuando se le solicite, ingrese las credenciales de la cuenta del administrador (necesarias para la aplicación Mac OS X Installer) y, a continuación, haga clic en **Instalar software**.
10. Una vez completada la instalación, haga clic en **Cerrar**.
    El cliente Advanced Threat Prevention para Mac ya está instalado.
11. Cierre el paquete.
12. Consulte Verificar la instalación de Advanced Threat Prevention.

En caso de que el sistema no esté registrado en el servidor Dell, consulte los registros para determinar si tiene un certificado válido en el Dell Server. Consulte Desactivar el certificado SSL de confianza para Advanced Threat Prevention.

## Desinstalación interactiva del cliente Advanced Threat Prevention

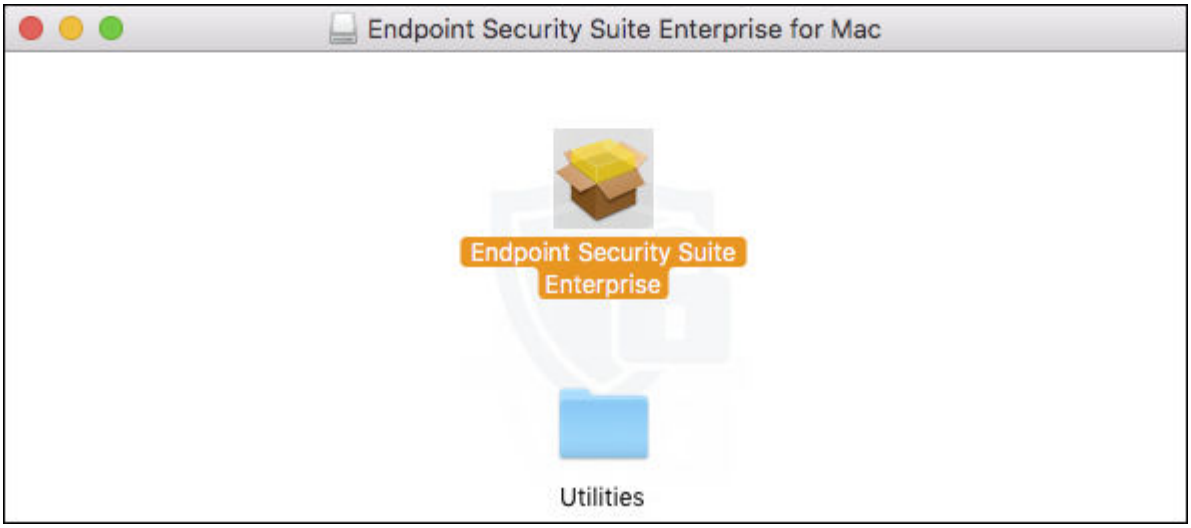
Para desinstalar el software cliente puede ejecutar la aplicación **Desinstalar Endpoint Security Suite Enterprise**. Para desinstalar el software cliente, siga los pasos que se indican a continuación.

1. Monte el archivo Endpoint-Security-Suite-Enterprise-<versión>.dmg.
2. En la carpeta Utilidades, inicie la aplicación **Desinstalar Endpoint Security Suite Enterprise**.
3. Haga clic en **Desinstalar**.
4. Cuando se le solicite, ingrese las credenciales de la cuenta del administrador (necesarias para la aplicación Mac OS X Installer) y, a continuación, haga clic en **Aceptar**.
   Los mensajes muestran el estado de la desinstalación.
5. En la confirmación de éxito, haga clic en **Aceptar**.
   Advanced Threat Prevention para Mac ya está desinstalado y la computadora se puede utilizar con normalidad.

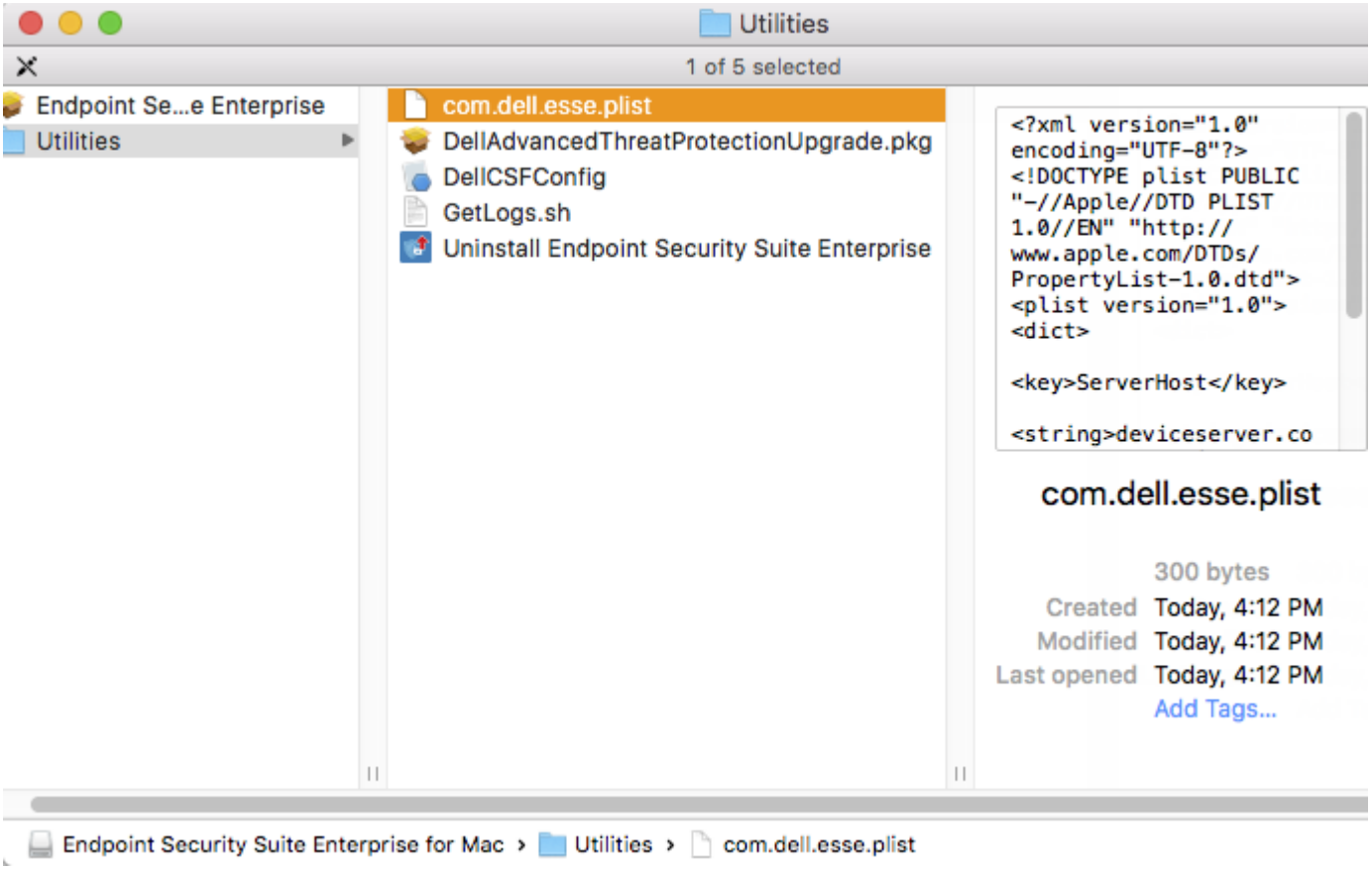
# Instalación de Advanced Threat Prevention mediante la línea de comandos

Para instalar el cliente Advanced Threat Prevention mediante la línea de comandos, siga estos pasos.

1. Desde el medio de instalación de Dell, monte el archivo Endpoint-Security-Suite-Enterprise-<version>.dmg. Se abrirá el paquete Endpoint Security Suite Enterprise para Mac.




2. Desde la carpeta Utilidades, copie el archivo **com.dell.esse.plist** en la unidad local.




3. Abra el archivo .plist.

4. Edite los valores de los marcadores con el nombre completo del host de Dell Server para administrar el usuario de destino, como server.organization.com, y el número de puerto **8888**:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>ServerHost</key>
  <string>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <array>
</dict>
</plist>
```

**NOTA:**

El puerto es el puerto de servicio del servidor de Core y se puede configurar. El número de puerto predeterminado es 8888.

5. Guarde y cierre el archivo.
6. Para cada computadora de destino, copie el instalador del paquete **Endpoint Security Suite Enterprise para Mac** en una carpeta temporal y el archivo **com.dell.esse.plist** modificado en **/Library/Preferences**.
7. Si se le solicita, ingrese sus credenciales.
8. Inicie una ventana de terminal.
9. Utilice el comando de **instalación** para realizar la instalación del paquete con la línea de comandos:
   **sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /**

   **NOTA:**

   La ruta -pkg es la ruta del instalador .pkg que se encuentra en el archivo .dmg.
10. Pulse **Intro**.
11. Consulte Verificar la instalación de Advanced Threat Prevention de ESSE.

## Desinstalación mediante la línea de comandos de Advanced Threat Prevention para Mac

Para desinstalar el cliente Advanced Threat Prevention mediante la línea de comandos, siga estos pasos.

1. Inicie una ventana de terminal.
2. Utilice el comando de **desinstalación** para llevar a cabo la desinstalación del paquete con la línea de comandos:
   **sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui**

   **NOTA:** Asegúrese de que el modificar --noui se incluye al final del comando.
3. Pulse **Intro**.
   Advanced Threat Prevention para Mac ya está desinstalado y la computadora se puede utilizar con normalidad.

# Solucionar problemas de Advanced Threat Prevention para Mac

## Desactivar el certificado SSL de confianza o la Comprobación de la política para Advanced Threat Prevention

Si el certificado de servidor de un cliente se ha perdido o se ha autofirmado, debe deshabilitar el certificado SSL de confianza en el lado del cliente solamente.

Si ejecuta certificados autofirmados en todo el entorno, desactive PolicyCheck.

Si tiene certificados autofirmados dentro de su entorno y no ha importado el certificado en la cadena de claves en sus dispositivos Mac, establezca DisableCertTrust y DisablePolicyCheck como Falso.

1. En el cliente, inicie una ventana de terminal.
2. Ingrese la ruta de acceso de DellCSFConfig.app:

   ```
   cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
   ```

3. Ejecute DellCSFConfig.app:

   ```
   sudo DellCSFConfig.app/Contents/MacOS/DellCSFConfig
   ```

   Aparecerán los siguientes valores predeterminados:

   ```
   Current Settings:
   ServerHost = deviceserver.company.com
   ServerPort = 8888
   DisableCertTrust = False
   DisablePolicyCheck = False
   DumpXmlInventory = False
   DumpPolicies = False
   ```

4. Escriba **-help** para enumerar las opciones.
5. Para desactivar el certificado SSL de confianza en el cliente, cambie `DisableCertTrust` a **Verdadero**.
6. Para desactivar la comprobación de la firma de la política en el cliente, cambie `DisablePolicyCheck` a **Verdadero**.

## Agregar inventario XML y cambios en las políticas a la carpeta de registros

Para agregar los archivos inventory.xml o policies.xml a la carpeta de registros:

1. Ejecute DellCSFConfig.app como se ha descrito más arriba.
2. Cambie DumpXmlInventory a **Verdadero**.
3. Cambie DumpPolicies a **Verdadero**.

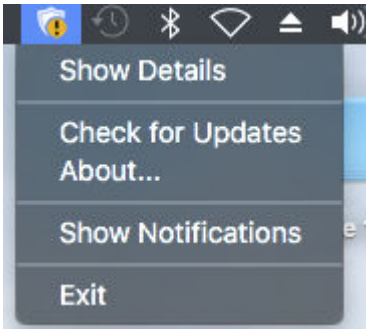
   Los archivos de políticas solo se vuelcan si se ha producido algún cambio en la política.

4. Para ver los archivos de registro inventary.xml y policies.xml, vaya a **/Library/Application\ Support/dell/Dell\ Data\ protección/**.

# Verificar la instalación de Advanced Threat Prevention

De forma opcional, puede verificar la instalación.

1. Confirme que el ícono de Advanced Threat Prevention tenga una placa de identificación verde  en la barra de comandos.
2. Si hay un signo de exclamación en el ícono, haga clic con el botón derecho del ratón y seleccione **Mostrar detalles**. Esto puede indicar que no está registrado.



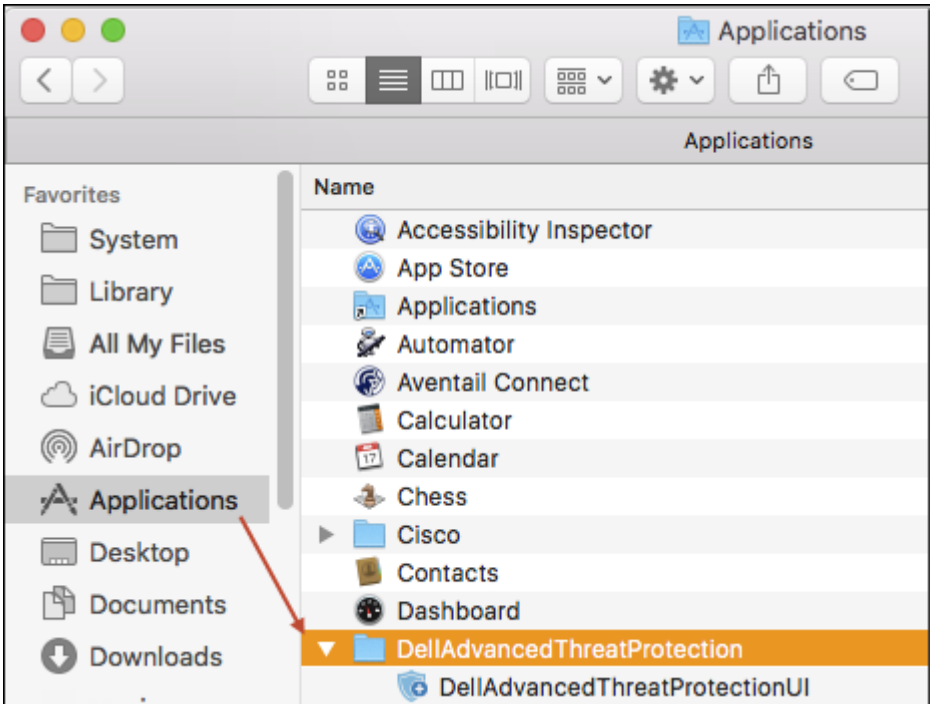

**Buscar actualizaciones**: busca actualizaciones del motor de Advanced Threat Prevention, no actualizaciones de políticas de Dell Server.

**Acerca de**: incluye lo siguiente.

- Versión
- Política: [en línea] indica las políticas basadas en servidor y [sin conexión] indica las políticas Airgap o basadas en desconexión

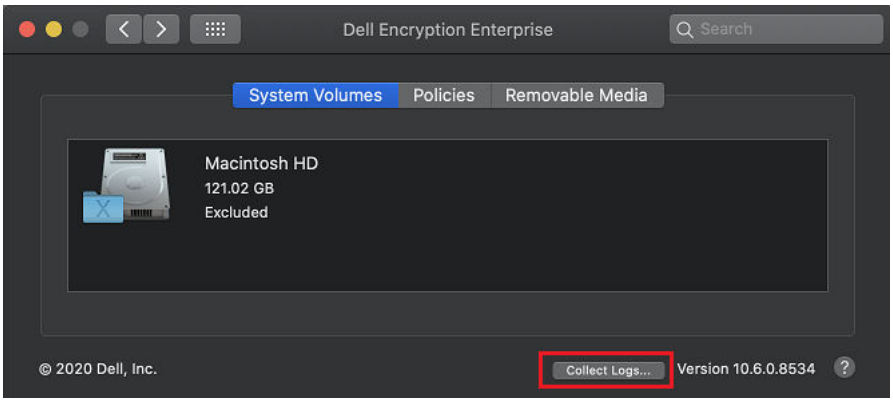
- Número de serie: utilice este número cuando se ponga en contacto con el servicio de asistencia. Se trata del identificador único de la instalación.

3. La carpeta de Advanced Threat Prevention se crea en /Aplicaciones.




# Recopilar archivos de registro para Endpoint Security Suite Enterprise

En *Preferencias del sistema* > *Dell Encryption Enterprise* > *Volúmenes del sistema*, el botón *Recopilar registros* en la parte inferior derecha permite a un administrador generar previamente registros para la compatibilidad. Esta acción puede afectar el rendimiento mientras se recopilan los registros.




DellLogs.zip contiene los registros de Mac Encryption Enterprise y Advanced Threat Prevention. Para obtener información sobre cómo recopilar los registros, consulte http://www.dell.com/support/article/us/en/19/SLN303924.

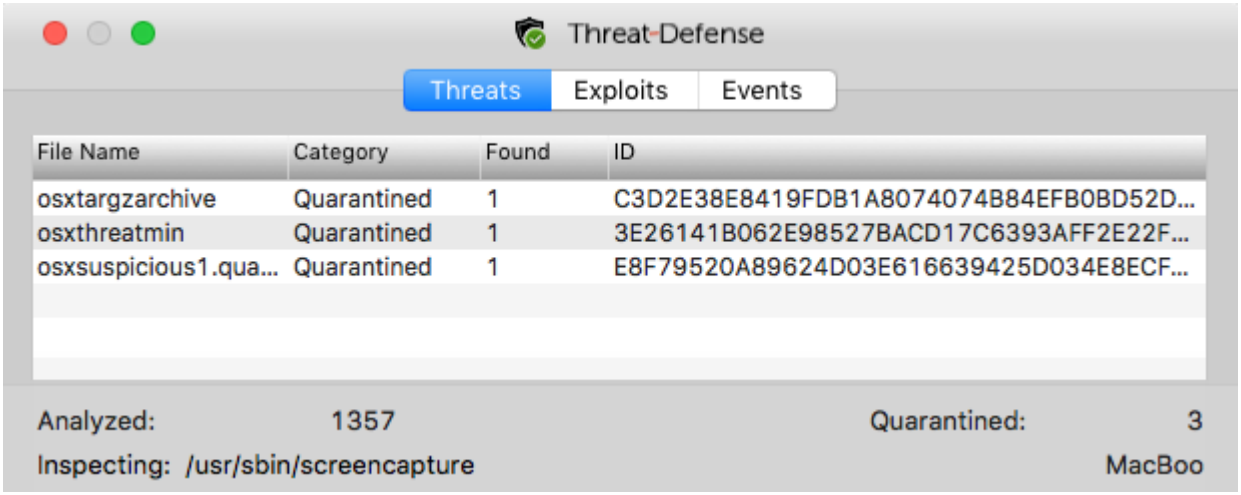
# Ver detalles de Advanced Threat Prevention

Una vez se haya instalado el cliente de Advanced Threat Prevention en una computadora de extremo, Dell Server lo reconoce como agente.

Haga clic con el botón derecho del ratón en el ícono de Advanced Threat Protection en la barra de comandos y seleccione **Mostrar detalles**. La pantalla de detalles de Advanced Threat Prevention cuenta con las siguientes pestañas.

## Pestaña Amenazas

La pestaña Amenazas muestra todas las amenazas detectadas en el dispositivo y la acción llevada a cabo. Las amenazas son una categoría de sucesos que se acaban de detectar como archivos o programas potencialmente inseguros y que requieren correcciones guiadas.



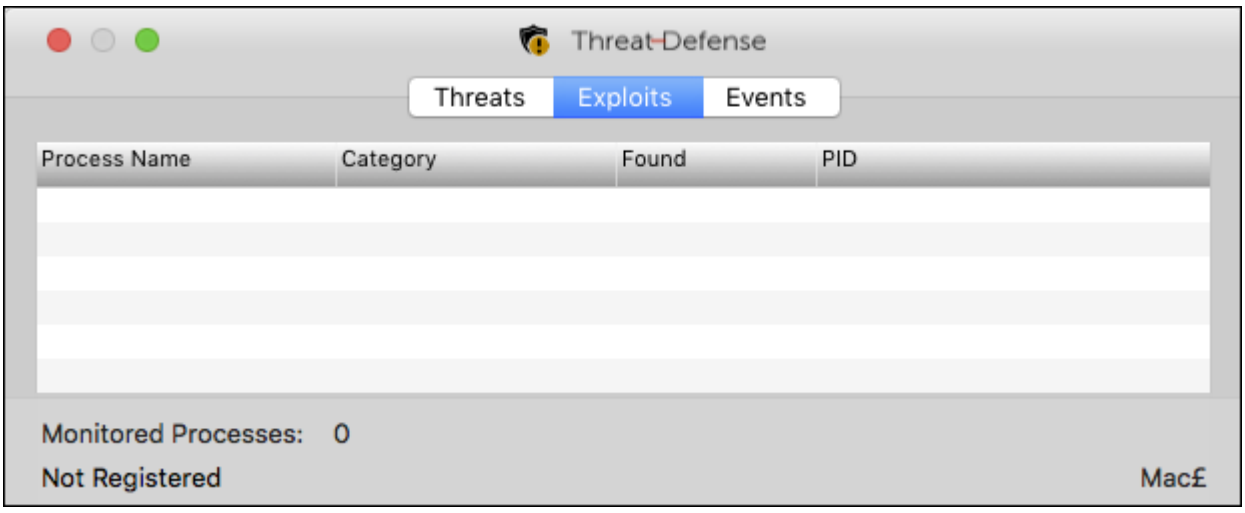

La columna Categoría puede incluir lo siguiente.

- **No seguro**: un archivo sospechoso que probablemente sea malware
- **Anómalo**: un archivo sospechoso que es posible que sea malware
- **En cuarentena**: un archivo que se ha trasladado de su ubicación original, guardado en la carpeta Cuarentena y cuya ejecución se ha impedido en el dispositivo.
- **Exento**: un archivo que tiene permiso para ser ejecutado en el dispositivo.
- **Borrado**: un archivo que se ha borrado en la organización. Los archivos borrados incluyen archivos exentos, archivos que se han agregado a la lista de seguridad y archivos que se han eliminado de la carpeta Cuarentena del dispositivo.

Para obtener más información sobre las clasificaciones de amenazas de Advanced Threat Prevention, consulte *AdminHelp*, disponible en la Management Console.

## Pestaña Vulnerabilidades de seguridad

La pestaña Vulnerabilidades de seguridad muestras las vulnerabilidades que se consideran amenazas.




Las políticas de Dell Server determinan la acción que se debe tomar cuando se detecta una vulnerabilidad:

- **Ignorar**: no se realiza ninguna acción contra las violaciones de memoria identificadas.
- **Alertar**: la violación de memoria se registra e informa a Dell Server.
- **Bloquear**: la llamada del proceso se bloquea si una aplicación intenta llamar a un proceso de violación de memoria. Se permite que la aplicación que realizó la llamada continúe ejecutándose.
- **Finalizar**: la llamada del proceso se bloquea si una aplicación intenta llamar a un proceso violación de memoria. Se finaliza la aplicación que realizó las llamadas.

Se detectan los siguientes tipos de vulnerabilidades de seguridad:

- Dinamización de pilas
- Protección de pilas
- Búsqueda de memoria del escáner
- Contenido malicioso

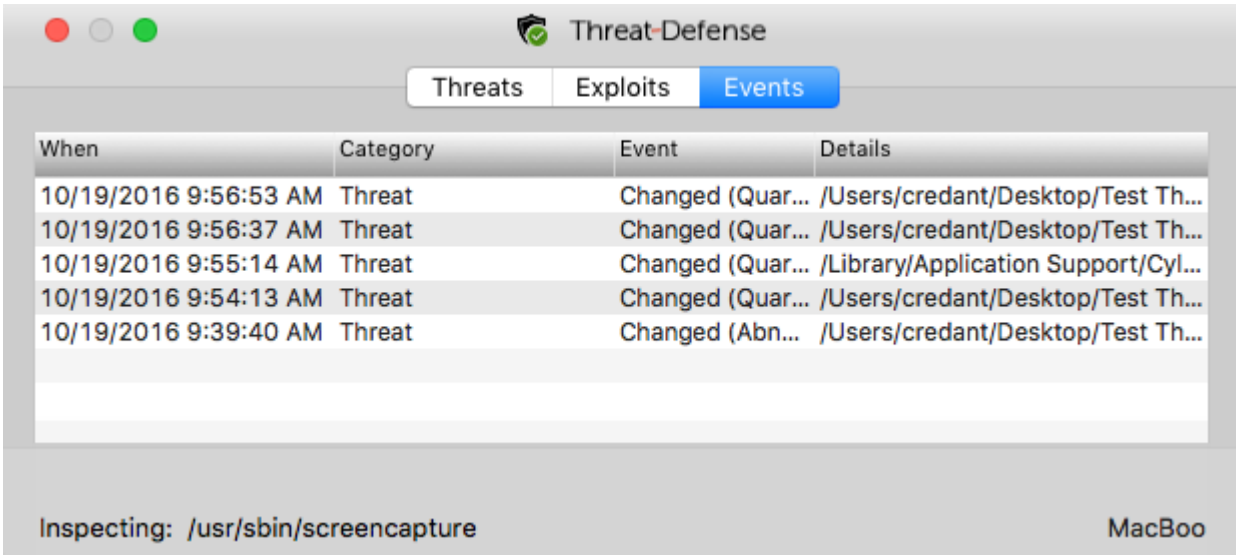
Para obtener más información sobre estas políticas, consulte *AdminHelp*, disponible en la Management Console.

## Pestaña Eventos

**NOTA:**

Un evento no necesariamente es una amenaza. Se genera un evento cuando un archivo o programa reconocido está en cuarentena, en la lista segura, o exento.

La pestaña Eventos muestra cualquier evento de amenaza que ocurre en el dispositivo y lo muestra según el tipo de evento que le asigna Advanced Threat Prevention. Los datos se eliminan cuando se reinicia el sistema.




Los ejemplos de tipos de eventos incluyen:

Amenaza encontrada

Amenaza eliminada

Amenaza en cuarentena

Amenaza eximida

Amenaza modificada

# 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**.

# 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**

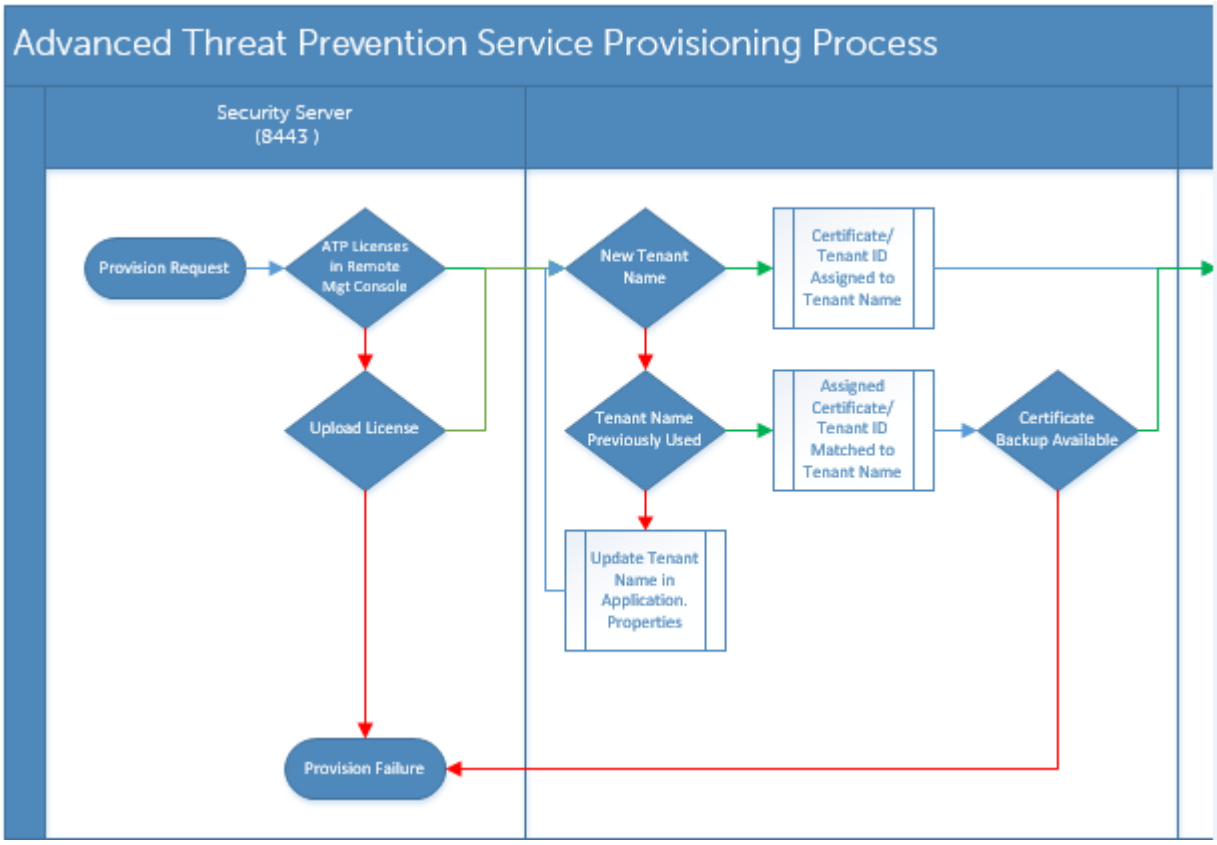
Para dejar de recibir actualizaciones automáticas del agente:

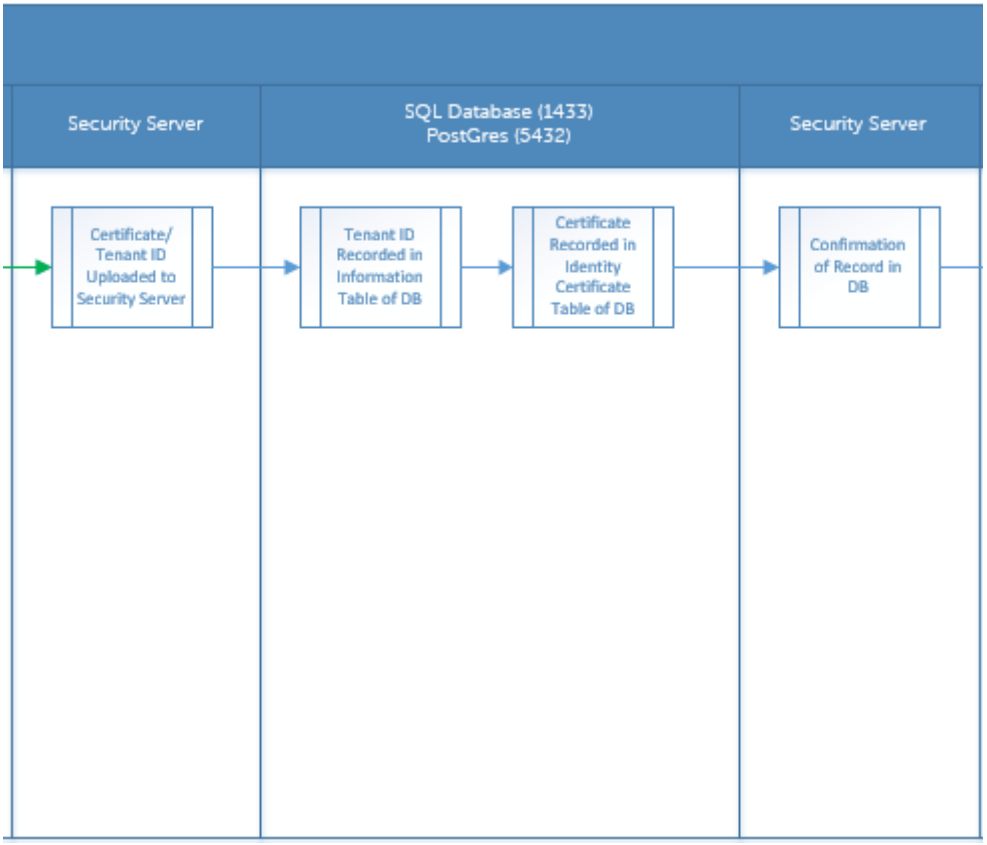
1. En el panel izquierdo de la consola de administración, haga clic en **Administración** > **Administración de servicios**.
2. En la pestaña *Amenazas avanzadas*, en *Actualización automática del agente*, haga clic en **Desactivar** y, a continuación, en **Guardar preferencias**.

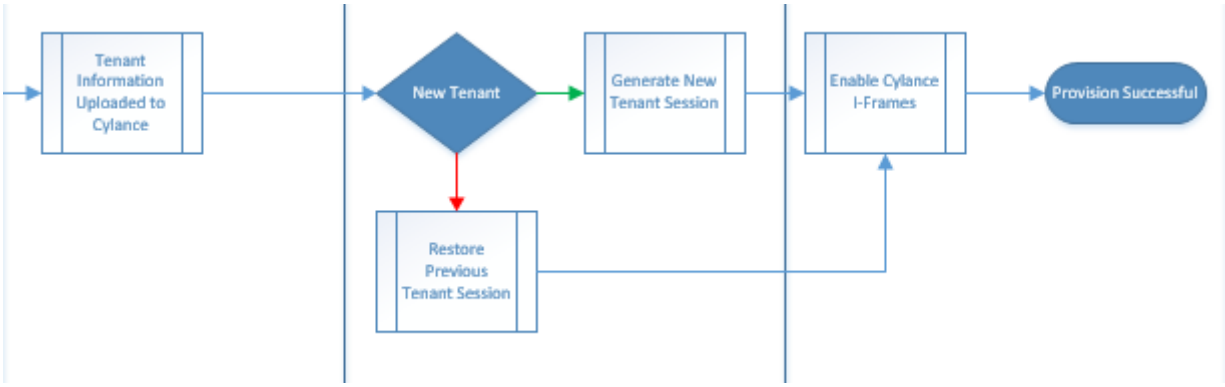
# Solución de problemas de Advanced Threat Prevention

## Comunicación de agentes y aprovisionamiento de Advanced Threat Prevention

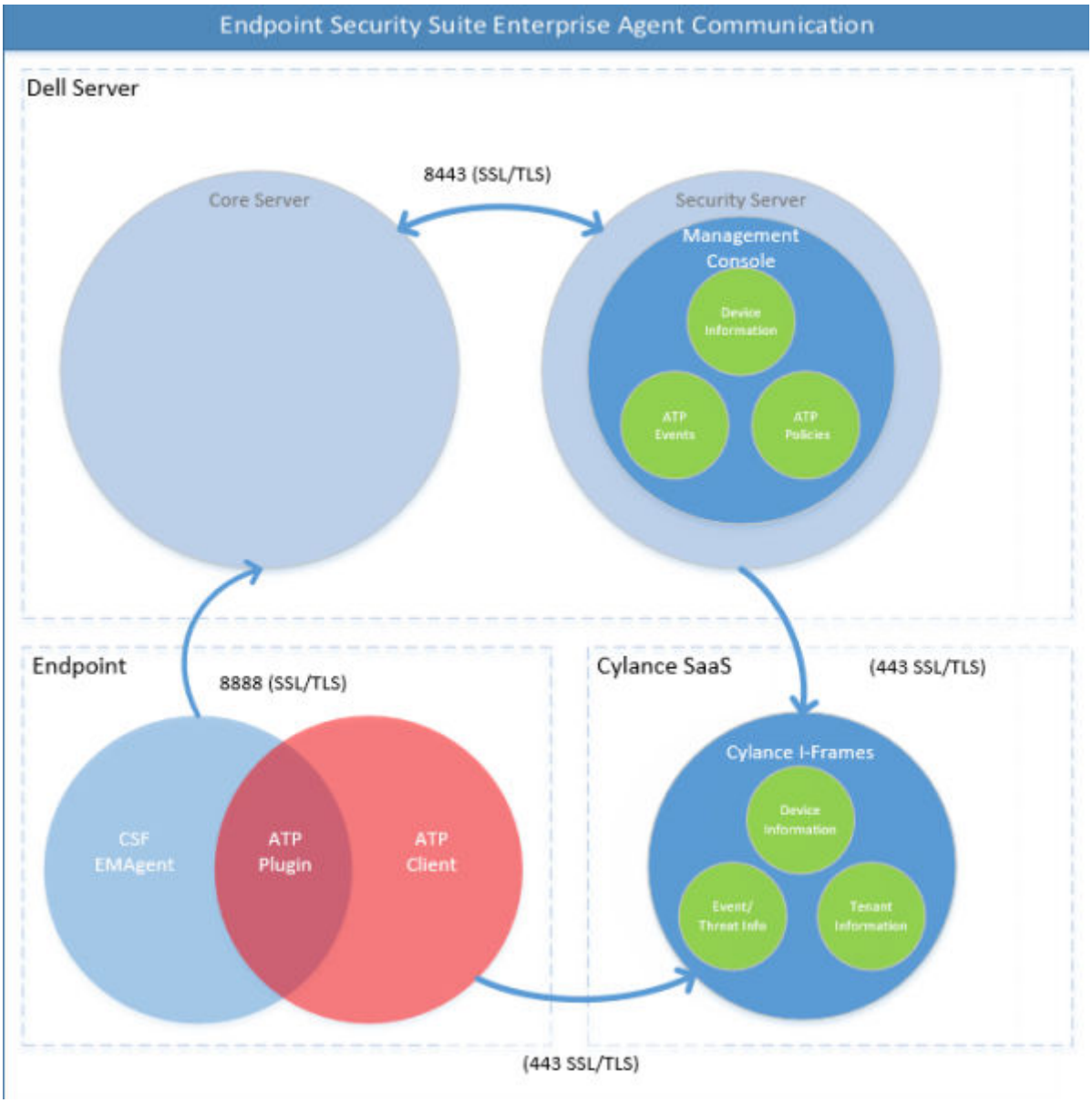
Los siguientes diagramas muestran el proceso de aprovisionamiento del servicio de Advanced Threat Prevention.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443 )
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Tenant Name Previously Used
Certificate/ Tenant ID Assigned to Tenant Name
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


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




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



# 5

# Glosario

**Security Server**: se utiliza para las activaciones de Dell Encryption.

**Policy Proxy**: se utiliza para distribuir las políticas del software cliente.

**Management Console**: la consola administrativa de Dell Server para la implementación de toda la empresa.

**Shield**: en ocasiones, encontrará este término en la documentación y en las interfaces de usuario. "Shield" es el término que se utiliza para representar a Dell Encryption.