Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

Notas, precauciones y avisos

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

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

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

Administrator Guide

2017 - 05

Rev. A02

Contents

1

Introducción

La Endpoint Security Suite Enterprise para Mac Administrator Guide (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 Data Protection 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 costes de administración y la complejidad de TI.

- Endpoint Security Suite Enterprise para Mac: un conjunto de software para el cifrado de cliente de datos y la prevención avanzada de amenazas.
- Política de proxy: se utiliza para distribuir políticas
- Servidor de seguridad: se utiliza para las activaciones de software de cifrado de cliente
- Enterprise Server o Dell Enterprise Server - VE: 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 servidor Dell, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Dell Enterprise Server - VE).

  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.

Cliente Dell Encryption y cifrado FileVault

La opción de administrar el cifrado FileVault, junto con el cliente Dell Encryption, está disponible en Endpoint Security Suite Enterprise para Mac. La opción más adecuada dependerá de los requisitos de cifrado de la empresa. Para obtener más información sobre las políticas de cifrado, consulte Cifrado Mac > Cifrado de volúmenes de Dell.

Cómo ponerse en contacto con Dell ProSupport

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

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

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:

Encryption Client

Hardware del cliente Encryption

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

NOTA: El disco del sistema debe particionarse con el esquema Tabla de particiones GUID (GPT) y tener formato Mac OS X Extended (registrados).

Hardware

- 30 MB de espacio libre en el disco
- Tarjeta de interfaz de red 10/100/1000 o Wi-Fi

Encryption Client Software

The following table details supported software.

NOTE: If you intend to perform a major operating system upgrade when using the Dell Encryption client (not FileVault encryption), a decrypt and uninstall operation will be needed followed by regular installation of the Encryption client for Mac on the new operating system.

Operating Systems (64-bit kernels)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption Client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

NOTE: If you are using a network user account to authenticate, that account must be set up as a mobile account in order to fully configure FileVault 2 management.

The following table details the operating systems supported when accessing Dell-encrypted external media.

NOTE: External Media Shield supports FAT32, exFAT, or HFS Plus (Mac OS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes. See Enable HFS Plus.

NOTE: External media must have 55 MB available, plus open space on the media that is equal to the largest file to be encrypted, to host External Media Shield.

Encrypted Media

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media

- Microsoft Windows 7 SP0-SP1
  - Enterprise
  - Professional
  - Ultimate
  - Home Premium
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 (Consumer)
- Microsoft Windows 8.1 - Windows 8.1 Update 1
  - Enterprise
  - Pro
- Microsoft Windows 10
  - Enterprise
  - Pro

Mac Operating Systems (64-bit kernels) Supported to Access Encrypted Media

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

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
- 2 GB RAM
- 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

NOTA: Esta versión solo se aplica a Advanced Threat Prevention, no al cliente Encryption.

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6

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

3

Tareas para el cliente Encryption

Instalar/actualizar el cliente Encryption

Esta sección le guiará a través del proceso de instalación/actualización y activación del 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 para Mac. Para atender a tantos clientes como sea posible, permitimos la modificación del archivo com.dell.ddp.plist para ofrecer compatibilidad en esos casos. En cuanto Apple lanza una nueva versión, comenzamos a probarla para asegurarnos de que es compatibles 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 el servidor Dell y sus componentes ya están instalados.

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

  Enterprise Server Installation and Migration Guide (Guía de instalación y migración de Enterprise Server)

  Enterprise Server – Virtual Edition Quick Start Guide and Installation Guide (Guía de instalación y Guía de inicio rápido de Enterprise Server – Virtual Edition)
- Asegúrese de que dispone de las URL del servidor de seguridad y de la política de proxy. Necesitará ambas para la instalación y la activación del software cliente.
- Si la implementación utiliza una configuración distinta de la predeterminada, asegúrese de que sabe el número de puerto del servidor de seguridad. Lo necesitará para la instalación y la activación del 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 el servidor Dell. La cuenta de usuario de dominio se utilizará para la activación del software cliente. No es necesario configurar los extremos de Mac para la autenticación de dominio (red).

- Para aplicar el cifrado en el equipo cliente, seleccione primero la opción de cifrado adecuada para su organización.

Dell Encryption	Cifrado con FileVault
Seleccione esta opción para realizar lo siguiente: • Cifrar todas las particiones en la unidad de inicio • Omitir la Autenticación previa al inicio • Utilizar cifrado de 256 bits **NOTA: Si utiliza Dell Encryption, deberá deshabilitar la Protección de integridad del sistema (SIP). Consulte Instalación/actualización interactiva y activación, paso 4.**	Seleccione esta opción para realizar lo siguiente: • Cifrar unidades Fusion Drive • Utilizar la Autenticación previa al inicio • Implementar una solución compatible con Apple **NOTA: Si el Mac incluye una unidad Fusion Drive, deberá habilitar FileVault para cifrar esa unidad.**

La configuración de la política de cifrado debe reflejar la opción de cifrado que seleccionó. Antes de configurar las políticas de cifrado, asegúrese de que comprende las políticas *Cifrar mediante FileVault para Mac* y *Volúmenes destinados a cifrado*. Para utilizar el cifrado de Dell Encryption o FileVault, la política *Cifrado de volúmenes de Dell* debe estar *Activada*.

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

Instalación/actualización interactiva y activación

Para instalar/actualizar y activar el software cliente, siga los pasos descritos 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; inmediatamente después de haber finalizado la instalación tendrá que reiniciar el equipo.

1. Desde el medio de instalación de Dell, monte el archivo Dell-Data-Protection-<version>.dmg.
2. Haga doble clic en el instalador del paquete. Aparecerá el siguiente mensaje:
   Este paquete ejecutará un programa para determinar si el software puede instalarse.
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.
   Si utiliza Dell Encryption con Mac OS X v10.11 o posterior, aparece un diálogo que dice *La Protección de integridad del sistema de Mac OS está activada.* Debe deshabilitar la Protección de integridad del sistema (SIP).

   Realice los pasos siguientes:

   a. Consulte http://www.dell.com/support/Article/us/en/19/SLN299063 para desactivar SIP.
   b. En el asistente, haga clic en **Aceptar** y continúe con *Configuración de Dell Data Protection*.
6. En el campo `Dirección de dominio:`, introduzca el dominio completo para los usuarios de destino, como por ejemplo *department.organization.com*.
7. En el campo **Nombre para mostrar (opcional):**, considere elegir el nombre del dominio de NetBIOS (anterior a Windows 2000) —que normalmente se escribe en mayúsculas— para establecer el *Nombre para mostrar*.
   Si lo establece, se mostrará este campo en lugar de la Dirección de dominio en el cuadro de diálogo *Activación*. Esto proporciona coherencia con el nombre de dominio que se muestra en los cuadros de diálogos de *Autenticación* en los dominios administrados por equipos Windows.
8. En el campo **Servidor de seguridad:**, introduzca el nombre de host del servidor de seguridad.
   Si en su implementación se utiliza una configuración distinta de la predeterminada, actualice los campos del puerto y la casilla de verificación **Utilizar SSL**.

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

9 En el campo **Política de proxy:**, el nombre de host de la política de proxy se rellenará automáticamente con un host de política de proxy que coincida con el host 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 se muestra con una flecha verde apuntando hacia el 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, introduzca las credenciales de la cuenta del administrador (necesarias para la aplicación Mac OS X Installer) y, a continuación, 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.

14 Haga clic en **Continuar con la instalación**. Empezará la instalación.

15 Cuando se complete la instalación, haga clic en **Reiniciar**.

16 Continúe para Activar el cliente Encryption para Mac.

Instalación/actualización mediante la línea de comandos

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

NOTA: Si utiliza Dell Encryption con Mac OS X v10.11.x, deberá desactivar SIP. Consulte http://www.dell.com/support/Article/us/en/19/SLN299063.

1 Desde el medio de instalación de Dell, monte el archivo Dell-Data-Protection-<version>.dmg.

2 Copie el paquete **Instalar Dell Data Protection** y el archivo **com.dell.ddp.plist** en la unidad local.

3 En la consola de administración remota, modifique las siguientes políticas si es necesario. La configuración de políticas anula los ajustes del archivo .plist. Utilice los ajustes de .plist si la consola de administración remota no cuenta con ninguna política.

- **Modo de contraseña de firmware**: si tiene previsto utilizar Boot Camp en equipos Mac cifrados o desea utilizar una versión del sistema operativo que Dell todavía no admite por completo, **debe** establecer esta política como *Opcional* para **no** utilizar la protección por contraseña del firmware. Para obtener más información, consulte Acerca de la protección por contraseña del firmware opcional.

  NOTA:
  Cuando la política FirmwarePasswordMode se establece en **Opcional**, solo desactiva el cumplimiento de la protección por contraseña del firmware del software cliente. **No** elimina ninguna protección por contraseña ya existente del firmware. Una vez que haya completado estos pasos, la instalación haya terminado y el equipo se haya reiniciado, podrá quitar la contraseña existente en el firmware mediante la Utilidad de contraseñas de firmware de Mac OS X.

- **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 el servidor Dell. Por ejemplo, en un centro educativo, se pediría a los profesores que activen sus equipos en el servidor Dell, pero no se le pediría a todos los estudiantes individuales que utilicen los equipos 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 equipo Mac, deben activarse todos los usuarios en el servidor Dell, de modo que la empresa no pueda editar esta propiedad. Sin embargo, si un usuario desea aprovisionar medios de EMS, se debe autenticar en el servidor Dell.

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 para 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/> [We recommend 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>FirmwarePasswordMode</key>
  <string>Required</string> [If using Boot Camp, this value must be Optional. For more
information, see About Optional Firmware Password Protection.]
  <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 Data Protection.pkg" -target /
```

8 Reinicie el equipo utilizando la siguiente línea de comandos: `sudo shutdown -r now`

9 Continúe para Activar el cliente Encryption para Mac.

Activar el cliente Encryption

El proceso de activación asocia las cuentas de usuario de red del servidor Dell con el equipo 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.

NOTA: Para obtener instrucciones sobre cómo activar un Mac que no es del dominio, consulte el artículo de Knowledge Base SLN302497.

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

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

Si se agota el tiempo de espera del diálogo de la contraseña, pulse **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 el servidor Dell 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 el servidor Dell.
  - Si la activación falla, el software cliente permite tres intentos para introducir 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 un equipo Mac, tanto desde una ubicación remota, con la ejecución de una secuencia de comandos, como en persona, el software cliente solicitará al usuario que permita el acceso del administrador y solicitará al usuario que introduzca 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 el equipo cifrado o en la Remote Management Console.

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, a continuación, haga clic en **Dell Data Protection**.

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.

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

La Remote Management Console enumera políticas de Mac en estos grupos de tecnología:

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

En función de los requisitos de cifrado de su empresa, puede establecer políticas para el cifrado de Dell o de FileVault. Esta tabla enumera las opciones de política para cada uno de ellos.

Cifrado Mac > Cifrado de volúmenes de Dell

Cifrado de volúmenes de Dell	*Activado* o *Desactivado* 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. El valor *Activado* habilita el cifrado y lo iniciará para los volúmenes que no están cifrados, conforme a la política *Volúmenes destinados a cifrado* **o** la política *Cifrar mediante FileVault para Mac*. El valor predeterminado es *Activado*.

	El valor Desactivado deshabilitará el cifrado e iniciará 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*. Compruebe que la política *Cifrar mediante FileVault para Mac* está seleccionada en el servidor Dell. 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. **NOTA: Si utiliza Dell Encryption (no FileVault) y esta política está habilitada, se produce un conflicto de política.** **NOTA:** Si tiene previsto migrar desde Dell Encryption a FileVault Encryption, consulte Migración desde cifrado de volúmenes de Dell a cifrado de FileVault.

Cifrado Mac > Configuración global de Mac

Volúmenes destinados a cifrado	*Solo el volumen del sistema* o *Todos los volúmenes fijos* *Solo el volumen del sistema* protege solamente el volumen del sistema que se encuentra en ejecución. **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 Remote Management Console. Para localizar una política específica en *AdminHelp*:

a Haga clic en el icono Búsqueda.

b En el campo Búsqueda, introduzca el nombre de la política con comillas.

c Haga clic en el enlace de tema que se muestra. El nombre de la política que ha introducido 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.
Preparando volumen para el cifrado...	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. 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 empezará tras el reinicio.

Estado	Descripción
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.
Esperando la custodia de claves con el servidor Dell...	Para garantizar que todos los datos cifrados se puedan recuperar, el software cliente no empezará el proceso de cifrado hasta que las claves de cifrado se custodien de un modo correcto en el servidor Dell. El software cliente sondeará en busca de conectividad con el servidor de seguridad mientras se encuentre en este estado, hasta que las claves se custodien.
Cifrando...	Está en curso un barrido de cifrado.
Cifrado	El barrido de cifrado ha finalizado.
Descifrando...	Está en curso un barrido de descifrado.
Restaurando a estado original...	El software cliente está restaurando el esquema de particiones a su estado original al final del proceso de "Descifrando...". Esta acción es el equivalente en el barrido de descifrado del estado "Preparando volumen para el cifrado".
Descifrado	El barrido de descifrado ha finalizado.

Color	Descripción
Verde	Parte cifrada
Rojo	Parte no cifrada
Amarillo	Parte que se está volviendo a cifrar 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 iconos 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. Dell Encryption no admite la Protección de integridad del sistema (SIP). Si esta condición incompatible se especifica en la política y se habilita SIP, se muestra un error junto a la unidad en la pestaña Volúmenes del sistema. Para desactivar SIP, consulte Instalación/actualización interactiva y activación, paso 4.
	Un volumen configurado para el cifrado. Esta etiqueta indica que se trata de una partición con cifrado de Dell.
	Un volumen configurado para el cifrado. La placa de identificación Seguridad y privacidad indica una partición protegida por FileVault.

Placa de Identificación	Tipo y estado del volumen
	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. **NOTA: El icono del volumen sin una placa de identificación indica que no se ha hecho nada en el disco. Este disco no es de inicio.**
	Varias unidades en las que solo el volumen del sistema está cifrado. Este es un ejemplo de una partición con cifrado de Dell.

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 iconos pueden diferir ligeramente según su sistema operativo.

Placa de Identificación	Estado
	Un icono de volumen atenuado indica un dispositivo sin montar. Los motivos pueden incluir: • El usuario quizá ha preferido no aprovisionarlo. • El medio puede estar bloqueado. **NOTA: Una placa de identificación con una barra/círculo rojo en este icono indica una partición que se excluye de la protección porque no se admite. Se incluyen volúmenes con formato FAT32.**
	El icono 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 EMS a medios sin blindaje se establece en Solo lectura.
	Medios cifrados con EMS, indicado con una placa de identificación de Dell.

Ver la política y el estado en la Remote Management Console

Para ver la política y el estado del cifrado en la Remote Management Console, siga los pasos a continuación.

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

2 En el panel izquierdo, haga clic en **Poblaciones > Extremos**.

3 Para la Estación de trabajo, haga clic en una opción del campo Nombre de host o, si conoce el Nombre de host del extremo, introdúzcalo en el campo Búsqueda. También puede introducir un filtro para buscar el extremo.

NOTA: Puede emplearse el carácter comodín (*), aunque no se requiere al inicio o al final del texto. Puede introducir Nombre común, Nombre principal universal o 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: El número que aparece por Cambios pendientes en las políticas es acumulativo. Puede incluir cambios realizados en otros extremos, o realizados mediante otros administradores que están utilizando la misma cuenta.

c Introduzca 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

NOTA: Solo se admiten para el cifrado los volúmenes Mac OS X Extended (registrados) y los discos del sistema que están particionados con esquemas de partición de Tabla de particiones GUID (GPT).

Utilice este proceso para activar el cifrado en un ordenador 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 todos los equipos Mac en el nivel de política de Enterprise. Para obtener instrucciones adicionales acerca de la activación del cifrado en el nivel de política de *Enterprise*, consulte *AdminHelp*.

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

2 En el panel izquierdo, haga clic en **Poblaciones** > **Extremos**.

3 Para la Estación de trabajo, haga clic en una opción de la columna Nombre de host o, si conoce el Nombre de host del extremo, introdúzcalo en el campo Búsqueda. También puede introducir un filtro para buscar el extremo.

NOTA: Puede emplearse el carácter comodín (*), aunque no se requiere al inicio o al final del texto. Puede introducir Nombre común, Nombre principal universal o 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 se haya habilitado el cifrado de FileVault, ninguna de las demás políticas del grupo estará en vigor. Consulte Cifrado Mac > Cifrado de volúmenes de Dell.

7 Si FileVault está deseleccionado, cambie otras políticas como desee.

Para obtener descripciones de todas las políticas, consulte *AdminHelp*, que está disponible en la Remote Management Console.

8 Cuando termine, haga clic en **Guardar**.

9 En el panel izquierdo, haga clic en **Administración** > **Confirmar**.

El número que aparece por Cambios pendientes en las políticas es acumulativo. Puede incluir cambios realizados en otros extremos, o realizados mediante otros administradores que están utilizando la misma cuenta.

10 Introduzca una descripción de los cambios en la casilla Comentarios y haga clic en **Confirmar políticas**.

11 Para ver la configuración de políticas en el equipo local después de que el servidor Dell envíe la política, en el panel Políticas de las Preferencias de Dell Data Protection, haga clic en **Actualizar**.

Proceso de cifrado

El proceso de cifrado varía en función de estos factores:

- El inicio del volumen de arranque en el que se ha habilitado el cifrado.
- Si se ha seleccionado el cifrado con Dell Encryption o el cifrado con FileVault.

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:

- Cifrado con Dell Encryption en una unidad no cifrada
- Cifrado con FileVault en un volumen sin cifrado
- Administrar un volumen cifrado con FileVault existente

Cifrado con Dell Encryption en una unidad no cifrada

Después de que el software cliente reciba la política de cifrado, realiza una validación con la Utilidad de disco de los volúmenes destinados a cifrado y, a continuación, configura esos volúmenes para el cifrado.

1 La barra de progreso indica el estado de la verificación. Cuando la verificación finaliza, los volúmenes de destino están configurados para el cifrado.

Este proceso puede ralentizar la capacidad de respuesta del equipo durante unos minutos. Para cada volumen en el que el cifrado esté pendiente, se muestra al usuario un cuadro de diálogo que indica que la operación está teniendo lugar.

2 Cuando finalice la preparación del cifrado, reinicie el equipo.

NOTA: En función de las políticas de experiencia del usuario establecidas en la Remote Management Console, es posible que el software cliente solicite al usuario que reinicie el equipo.

3 Después de que el equipo se reinicie, deberá conectarse a la red para que el software cliente custodie la información de recuperación en el servidor Dell.

El software cliente puede empezar y completar el proceso de cifrado, así como el informe sobre el estado del cifrado en la Remote Management Console, todo ello antes de que el usuario inicie sesión. Esto permite aplicar la conformidad en todos los equipos Mac, sin necesidad de la interacción del usuario.

Cifrado con FileVault en un volumen sin cifrado

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 Introduzca 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**.

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.

5 Haga clic en **Aceptar**.

6 Cuando finalice la preparación del cifrado, reinicie el equipo.

> **NOTA: En función de las políticas de experiencia del usuario establecidas en la Remote Management Console, es posible que el software cliente solicite al usuario que reinicie el equipo.**

7 Después de que el equipo se reinicie, deberá conectarse a la red para que el software cliente custodie la información de recuperación en el servidor Dell.

El software cliente puede empezar y completar el proceso de cifrado, así como el informe sobre el estado del cifrado en la Dell Remote Management Console, todo ello 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 añadir usuarios de FileVault

Para proteger los datos de un disco, FileVault los cifra automáticamente. En un volumen de inicio de FileVault administrado, para permitir que varios usuarios desbloqueen el disco, puede modificar una política en la consola de administración remota 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 remota, desplácese hasta 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*, introduzca 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 Data Protection > 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 la clave *AuthenticationAuthority* especifican un patrón de *user1*, user2 y *user3* o cualquier Id. de usuario que comience 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 el servidor.

  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 finales que deben activar el inicio 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, a continuación, haga clic en **Dell Data Protection**.

2 Haga clic en la pestaña **Volúmenes del sistema**.

3 Haga clic en la opción de volumen del sistema y seleccione **Agregar usuarios de FileVault al inicio de FileVault**.

4 En el campo Buscar, introduzca un nombre del 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 Introduzca 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 el equipo ya tiene un volumen cifrado con FileVault y el cifrado de FileVault está habilitado en la Remote Management Console, Dell Encryption puede asumir la administración del volumen.

Si Dell Encryption detecta que el volumen de arranque ya está cifrado, se mostrará el cuadro de diálogo de Dell Data Protection. 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**.

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

  1 Introduzca la clave.

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

  2 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.**

  1 Introduzca el nombre de usuario y la contraseña.

  2 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, introduzca 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 selecciona no introducir la contraseña, podrá acceder al contenido del volumen y se cifrará con FileVault, pero Dell no administrará el cifrado.

NOTA: En la Remote Management Console, el administrador puede ver que el servidor Dell administra ahora el extremo.

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 Remote Management Console y cópielo en el escritorio del equipo.
2 Abra *Preferencias del sistema* y, a continuación, haga clic en **Dell Data Protection**.
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 Remote Management Console.

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 sigue pudiendo entrar en suspensión, pero el estado actual del sistema se mantendrá solo en memoria. Por lo tanto, el equipo se reiniciará totalmente si durante la suspensión se cierra del todo, lo que podría ocurrir si la batería se agota o se sustituye.

Copiar una regla de la lista blanca

Un elemento de menú oculto permite que un usuario copie una regla de la lista blanca para un medio externo.

1 Abra **Preferencias del sistema** y, a continuación, haga clic en **Dell Data Protection**.
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 blanca** para el medio externo actual. La regla de la lista blanca se copia en el Portapapeles.
5 Acceda al Portapapeles, copie la regla de la lista blanca 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.

Si desea excluir un dispositivo o un grupo de dispositivos para impedir que se escriban datos cifrados en la unidad Thunderbolt o en los medios EMS, puede utilizar la regla de la lista blanca para modificar los valores.

Utilice la regla completa para especificar una unidad concreta para la lista blanca, como 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 EMS cuando se conectan a través de Thunderbolt:

tbolt=1;bus=SATA

También puede incluir en la lista blanca o excluir medios de EMS en función de:

- **Tamaño del medio**

  Regla de la lista blanca para excluir medios grandes de la protección de EMS:

  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 EMS, utilice uno de los siguientes:

  tamaño >= 500000000

tamaño >= 500000K

tamaño >= 500M

- **Tipo de sistema de archivos**

  Regla de la lista blanca:

  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:

- Quizá tenga que mover datos cifrados del usuario a un Mac diferente como parte de una actualización de hardware.
- Quizá tenga que acceder a un disco cifrado por un error del sistema operativo que causa que el volumen del sistema ya no se inicie y tiene que ejecutar varios programas de utilidad para reparar el sistema operativo.
- Quizá tenga que acceder a datos cifrados del usuario porque el usuario efectuó un cambio de configuración no autorizado y tiene que solucionar la situación.

Esta sección le guiará a través del proceso de utilizar **una** de las tres operaciones de recuperación disponibles.

Elija **una** de las siguientes opciones:

- Montar volumen
- Aceptar nueva configuración del sistema
- Recuperación de FileVault: utilice esta opción solamente si el extremo que se va a recuperar está protegido con el cifrado de FileVault. FileVault se puede utilizar con el cliente Encryption si utiliza Mac OS X 10.10.5 o posterior. La recuperación de FileVault también se utiliza con Fusion Drive.

Montar volumen

Requisitos previos

- Un equipo o un volumen externo de recuperación sin cifrar que ejecutarán la utilidad de recuperación
- Un cable FireWire o Thunderbolt, en función de su hardware
- El ID de dispositivo/ID exclusivo del equipo destinado a la recuperación: en la mayoría de los casos, puede encontrar el equipo destinado a la recuperación en Remote Management Console buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para dicho usuario. 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 Remote Management Console.

2 En el panel izquierdo, haga clic en **Administración > Recuperar extremo**.

3 En el campo Búsqueda, introduzca el nombre de dominio completo del extremo 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 que está a punto de descargar.

NOTA: Debe recordar esta contraseña para acceder a las claves de recuperación.

6 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**.

Se ha descargado el archivo de recuperación <nombre_máquina.dominio>.csv.

NOTA: Si en este equipo se ha habilitado la protección por contraseña del firmware, se le solicitará la contraseña del firmware para acceder al Administrador de inicio de preinicio. Encontrará la contraseña del firmware del equipo en el paquete de recuperación descargado en Guardar el paquete de recuperación. Consulte Cómo activar Boot Camp en Mac OS X para obtener más información.

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-Data-Protection-<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 En la carpeta Utilidades que se encuentra en el medio de instalación de Dell, inicie la Utilidad de recuperación de Dell.

Se mostrará un mensaje que indica: "Es necesario cargar el kext [texto del kernel] de DDP para modificar los discos cifrados. Escriba la contraseña que permita esto".

10 Introduzca la contraseña del administrador o del usuario.

Aparecerá un mensaje que indica: "Necesita instalación: Recuperación necesita instalación".

11 Haga clic en **Instalar**.

12 Seleccione el volumen o la unidad que necesita recuperación y haga clic en **Continuar**.

La selección de la unidad recuperará todos los volúmenes en la unidad a la vez.

13 Seleccione el paquete de recuperación (que se guardó en el paso 6) y haga clic en **Abrir**.

14 Seleccione la opción **Montar volumen**.

15 Haga clic en **Continuar** para confirmar *Montar volumen*. Se mostrará un mensaje de finalización satisfactoria.

16 Haga clic en **Cerrar**.

Ahora podrá abrir la ventana de 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 transfieren archivos entre los volúmenes.

Aceptar nueva configuración del sistema

Si un cambio de contraseña de firmware o de otra configuración del sistema invalidó la clave de cifrado en un equipo cifrado, elija esta opción para aceptar la configuración actualizada del sistema en el próximo reinicio y restaurar el acceso al equipo.

Como el cifrado está vinculado a una configuración específica del dispositivo, los cambios en la configuración invalidan la clave de cifrado del software cliente. Si selecciona que se acepte la nueva configuración del sistema, solo tiene que especificar en el software cliente que se

restablezca su seguridad basándose en la nueva configuración. Por ejemplo, quizá tenga que mover la unidad a un Mac diferente porque un usuario ha roto la pantalla. Con este método, puede especificar que el software cliente acepte esta "nueva" configuración como válida.

Requisitos previos

- Un equipo o un volumen externo de recuperación sin cifrar que ejecutarán la utilidad de recuperación
- Un cable FireWire o Thunderbolt, en función de su hardware
- El ID de dispositivo/ID exclusivo del equipo destinado a la recuperación: en la mayoría de los casos, puede encontrar el equipo destinado a la recuperación en Remote Management Console buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para dicho usuario. 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 Remote 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 Debajo de 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**.

> **NOTA: Si en este equipo se ha habilitado la protección por contraseña del firmware, se le solicitará la contraseña del firmware para acceder al Administrador de inicio de preinicio. Encontrará la contraseña del firmware del equipo en el paquete de recuperación descargado en el paso 7. Consulte Cómo activar Boot Camp en Mac OS X para obtener más información.**

8 Inicie el equipo de destino desde un volumen externo de instalación completa del SO creado previamente. Para hacerlo puede, o bien iniciar el panel de Disco de inicio en Preferencias del sistema y seleccionar el volumen de instalación completa del SO, o bien mantener pulsada la tecla **Opción** mientras reinicia el equipo y seleccionar el volumen de instalación completa del SO externo en el Administrador de inicio de prearranque. Para crear un volumen de inicio, consulte https://support.apple.com/en-us/HT202796.

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.**

9 Realice una de estas opciones:

- Conecte este equipo al equipo host que realizará la operación de recuperación mediante un cable FireWire o Thunderbolt, en función de su hardware.

  O bien

- Conmute el inicio a cualquier disco con una instalación completa del SO en él.

10 Monte el archivo Dell-Data-Protection-<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.**

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

Se mostrará un mensaje que indica: "Es necesario cargar el kext [texto del kernel] de DDP para modificar los discos cifrados. Escriba la contraseña que permita esto".

12 Introduzca la contraseña del administrador o del usuario.

Aparecerá un mensaje que indica: "Necesita instalación: Recuperación necesita instalación".

13 Haga clic en **Instalar**.

14 Seleccione el volumen o la unidad que necesita recuperación y haga clic en **Continuar**.
La selección de la unidad recuperará todos los volúmenes en la unidad a la vez.

Se mostrará la ventana del selector de archivos.

15 Seleccione el paquete de recuperación (que se guardó en el paso 7) y haga clic en **Abrir**.
Se muestra el diálogo *Seleccionar operación de recuperación*.

16 Seleccione la opción **Aceptar nueva configuración del sistema**.

17 Haga clic en **Continuar** para confirmar *Aceptar nueva configuración del sistema*.

18 Introduzca su contraseña para restablecer la propiedad y aceptar la nueva configuración del sistema.

19 Haga clic en **Aceptar**.

Aparecerá un mensaje de *Recuperación completada* cuando inicie en el volumen del sistema interno original. Este mensaje le solicitará que vuelva a reiniciar el equipo. El software cliente ya ha aceptado ahora la configuración actualizada del sistema y podrá acceder normalmente al equipo.

Recuperación de FileVault

La recuperación de un volumen administrado por y cifrado con FileVault es muy diferente a la recuperación de un volumen con cifrado de Dell. El proceso de recuperación lo decide Apple y está automatizado donde sea posible, pero requiere unos pocos pasos más.

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. Normalmente, utilice primero la clave de recuperación más reciente. 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 el servidor Dell. Se trata del método preferido.

  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: 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 inicio antes de recuperar los que no son de inicio. La recuperación del volumen de inicio normalmente corrige los problemas de los volúmenes que no son de inicio.

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 el equipo destinado a la recuperación en la Remote Management Console buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para dicho usuario. El formato del ID exclusivo/ID de dispositivo es "MacBook.Z4291LK58RH de Juan García".
- Medio de instalación de Dell

Proceso

1 Abrir la Remote 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 Debajo de 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 Introduzca una ubicación para el paquete de recuperación y haga clic en **Guardar**.

9 Copie el paquete de recuperación y el archivo **Dell-Data-Protection-<version>.dmg** en la unidad USB de inicio.

10 Inicie el ordenador de destino desde un volumen de instalación completa del SO externo manteniendo pulsada la tecla **Opción** mientras reinicia el equipo y, a continuación, seleccionando el volumen de instalación completa del SO externo en el Administrador de inicio de prearranque. Para crear un volumen de inicio, consulte https://support.apple.com/en-us/HT202796.

11 Monte el archivo Dell-Data-Protection-<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.

12 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*.

13 Seleccione el volumen FileVault.

- Para el descifrado y el montaje de la unidad, debe tener una partición de inicio versión 10.9.5 o posterior. De lo contrario, solo podrá obtener la clave de recuperación personal.
- Si tiene volúmenes cifrados que no son de inicio, normalmente recuperará primero la partición de inicio.

14 Haga clic en **Continuar.**

Se muestra el diálogo *Elija el paquete de recuperación*.

15 Seleccione el paquete de recuperación (que guardó en el paso 9) y haga clic en **Abrir**.

Se muestra el diálogo *Seleccione registro de recuperación*.

16 En la columna Fecha de custodia, seleccione la fecha más reciente para el tipo Clave de recuperación personal y haga clic en **Continuar.**

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

El Resultado de la operación de recuperación muestra la clave.

- 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 iniciar en la partición de destino e introducir la clave de recuperación personal para la autenticación de preinicio, algo que puede variar en función del SO.
- Para las unidades que no son de inicio, solo se muestra la clave de recuperación personal. Para montar un volumen que no sea de inicio, introduzca la clave de recuperación en el cuadro de diálogo de solicitud de contraseña del sistema operativo. Si previamente descartó el cuadro de diálogo, ahora puede seleccionar Desbloquear mediante Utilidad de disco para montar la partición cifrada.

17 Imprima o anote la clave.

18 Haga clic en **Cerrar**.

19 Inicie en el volumen de inicio externo manteniendo pulsada la tecla **Opción** durante el arranque.

20 Si es necesario, introduzca la contraseña de firmware. Seleccione el volumen de inicio externo.

21 Después de que se reinicie el sistema, haga clic en el signo **?** en la pantalla de inicio de sesión.

22 Haga clic en la flecha que se muestra.

23 Escriba la clave de recuperación y pulse **Intro**.

24 En el cuadro de diálogo, introduzca la nueva contraseña.

Cadena de claves recuperación

Debe ejecutar la Utilidad de recuperación de Dell mientras se inicia en un volumen de recuperación no cifrado. No ejecute la Utilidad de recuperación de Dell desde un volumen de inicio externo 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

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 Inicie en el volumen de inicio externo manteniendo pulsada la tecla **Opción** durante el arranque.

3 Si es necesario, introduzca la contraseña de firmware. Seleccione el volumen de inicio externo.

4 Monte el archivo .dmg.

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 externa como, por ejemplo, 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, introduzca el nombre y la ruta de acceso de la secuencia de comandos.

> **NOTA:**
> Si almacena los archivos junto a la raíz de un volumen, se acortará la ruta de acceso que debe escribir.

El Resultado de la operación de recuperación muestra la clave.

La utilidad de recuperación de Dell produce los archivos en la ubicación seleccionada y luego muestra los comandos exactos que debe 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 pulsadas simultáneamente las teclas **Comando** y **R** (Comando-R) antes del timbre de encendido/autoprueba y durante el inicio del equipo.
  O bien
- Pulse la tecla **Opción** y utilice el selector de inicio 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: Actualmente Mac no admite la grabación de CD/DVD para EMS. 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 una copia de seguridad de Time Machine se introducen automáticamente en la lista blanca para permitir que la copia de seguridad continúe.
  - 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 blanca y enviársela para especificar su unidad de Time Machine en la lista blanca. Consulte Copiar una regla de la lista blanca.

EMS y actualizaciones de políticas

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

Excepciones de cifrado

En los medios externos, no se cifran los atributos extendidos.

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 EMS, y después se monta en EMS, 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:

  a Anote la cantidad de espacio que debe liberar en el dispositivo. En el informe se muestra una lista de los archivos y su tamaño.

  b Vacíe la papelera. A medida que libere espacio, EMS cifrará automáticamente los archivos adicionales.

  c Si borra archivos o carpetas, recuerde volver a vaciar la papelera.

Mensajes de auditoría

Los mensajes de auditoría se envían al servidor Dell.

Para Endpoint Security Suite Enterprise para Mac, acceda a la Remote Management Console y seleccione **Poblaciones > Enterprise o extremos**. A continuación, seleccione la pestaña **Eventos de amenazas avanzadas**. Para obtener más información, consulte *AdminHelp*.

Recopilar archivos de registro para Endpoint Security Suite Enterprise

DellLogs.zip contiene los registros para el cliente Encryption 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 Data Protection.** 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 **Cifrado de volúmenes de Dell** del equipo en **Desactivada** en la Remote 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 Introduzca 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 del equipo, inicie la aplicación **Desinstalar Dell Data Protection** (ubicada en la carpeta Utilidades en el archivo Dell-Data-Protection-<version>.dmg del medio de instalación de Dell).

Los mensajes muestran el estado de la desinstalación.

El cliente Encryption para Mac ya está desinstalado y el equipo 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 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 del servidor Dell.

Requisitos previos

- El cliente Encryption para Mac debe estar instalado en el ordenador remoto.
- 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 Data Protection.

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 e iMac11.2 serán compatibles con la protección por contraseña para firmware opcional (como indica el *), pero iMac12.1 o versiones posteriores no lo serán.

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.

Si desea que la protección por contraseña del firmware de Mac OS X sea **necesaria**, siga el procedimiento de instalación/actualización del cliente normal que se describe en Instalar/actualizar el cliente Encryption para Mac.

Cómo utilizar Boot Camp

Compatibilidad de Mac OS X con Boot Camp

NOTA: Si utiliza Boot Camp, el sistema operativo Windows no se puede cifrar.

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 y 8 Pro (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 y posterior solo es compatible con Boot Camp 5.1.

Para utilizar Endpoint Security Suite Enterprise for Windows en Boot Camp en un equipo con Endpoint Security Suite Enterprise para Mac, el volumen del sistema se debe cifrar mediante el cliente Encryption para Mac, ya sea con cifrado del cliente de Dell o con FileVault2. Debe configurar su instalación de cliente para que **no** utilice la protección por contraseña del firmware. Consulte Instalación/actualización mediante la línea de comandos para obtener instrucciones.

NOTA:
Si la partición de Windows es un candidato EMS, asegúrese de incluirlo en la lista blanca o se cifrará. Consulte Copiar una regla de la lista blanca.

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.

Recuperar 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 el equipo destinado a la recuperación en la Remote Management Console buscando el nombre de usuario del propietario y visualizando los dispositivos cifrados para dicho usuario. El formato del ID exclusivo/ID de dispositivo 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 Desde la Remote Management Console, 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 iniciar el equipo desde la unidad de Boot Camp externa, pulse la tecla **Opción** mientras enciende el equipo.

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 de Dell Data Protection Encryption, 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 acceder a los 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 Introduzca 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 administrador de Dell, inicie sesión en la Remote 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 Debajo de 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 introduzca el comando que desee en la línea de comandos.

Ejemplo:

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

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

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/client

Tabla 1. Comandos de la herramienta del cliente

Comando	Propósito	Sintaxis	Resultados
Activar	Activa un cliente Mac con el servidor Dell, pero sin pasar por la interfaz de usuario. Para activar, se debe introducir un nombre de usuario de dominio y una contraseña válidos. 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 -a localAccount* domainAccount domainPassword **domainAccount** es la cuenta que se utiliza en la activación mediante la herramienta de cliente. **localAccount** es opcional y es el usuario actual si no se especifica ninguno. El comando de activación tiene este formato: client -a <usuario que se activará*> <domainUser> <domainPassword> Si utiliza la política *Lista de usuarios sin autenticación* para crear clases de usuarios que no necesitan activación desde el servidor Dell, de manera opcional, puede utilizar la herramienta de cliente para especificar una cuenta local diferente de aquella en la	0 = Correcto 2 = Error en la activación y el motivo del fallo 6 = No se ha encontrado el usuario

Comando	Propósito	Sintaxis	Resultados
		que ha iniciado la sesión. Consulte Política Lista de usuarios sin autenticación en el paso 3.	
Activar temporalmente	Activa un cliente Mac sin dejar huella.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Disco	Solicitar el estado del disco	-d	Se muestra el estado del disco, incluida el ID del disco, el estado del cifrado y las políticas 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 -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile **NOTA: La deviceId debe ser un UUID de volumen lógico o resolverse en exactamente un LVUUID. A menudo, también funciona con un punto de montaje o devnode.**	0 = Correcto 7= No se ha encontrado el LVUUID 10 = Error de credencial 11 = Error de custodia
Política	Solicitar las políticas del cliente Mac	-P	Visualización de las políticas
Servidor	Sondea el servidor Dell por si hay políticas actualizadas en nombre del cliente Mac **NOTA: El sondeo puede tardar varios minutos en terminar.**	-s	0 = Correcto Cualquier otro valor indica que el servidor Dell o el software cliente Mac estaba ocupado o no respondía.
Prueba	Comprobar el estado de activación del cliente Mac	-t localAccount*	0 (domainAccount) = Correcto 1 = No activado 6 = No se ha encontrado el usuario
Usuario	Solicitar información del usuario	-u localAccount*	Se muestra la información de la cuenta del usuario: 0 (información de la cuenta) = Correcto 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\ Data\ Protection.prefPane/Contents/Helpers/**client -p -plist**

Para recuperar las políticas desde el cliente e imprimirlas.

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

Para activar temporalmente el cliente e imprimir el resultado.

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

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

Library/PreferencePanes/Dell\ Data\ Protection.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

Tareas para Advanced Threat Prevention

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 el servidor Dell y sus componentes ya están instalados.

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

  Enterprise Server Installation and Migration Guide (Guía de instalación y migración de Enterprise Server)

  Enterprise Server – Virtual Edition Quick Start Guide and Installation Guide (Guía de instalación y Guía de inicio rápido de Enterprise Server – Virtual Edition)
- Asegúrese de que dispone del nombre de host y el puerto del servidor. Necesitará ambos para la instalación del software cliente.
- Asegúrese de que el equipo de destino cuenta con conectividad de red con el servidor Dell.
- 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:

Este paquete ejecutará un programa para determinar si el software puede instalarse.

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**, introduzca el nombre de host completo del servidor Dell que administrará el usuario de destino, por ejemplo server.organization.com.

7 En el campo **Puerto del servidor**, introduzca **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, introduzca las credenciales de la cuenta del administrador (necesarias para la aplicación Mac OS X Installer) y, a continuación, haga clic en **Aceptar**.

10 Una vez completada la instalación, haga clic en **Cerrar**.

El cliente Advanced Threat Prevention para Mac ya está instalado.

11 Consulte Verificar la instalación de Advanced Threat Prevention.

Si la instalación falla, compruebe si cuenta con un certificado válido en el servidor Dell. 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, introduzca 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 el equipo 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 de host completo del servidor Dell que administrará el usuario de destino, como por ejemplo 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>deviceserver.company.com</string>
  <key>ServerPort</key>
  <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 equipo 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, introduzca 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 el equipo se puede utilizar con normalidad.

Solucionar problemas de Advanced Threat Prevention para Mac

Desactivar el certificado SSL de confianza 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.

1 En el cliente, inicie una ventana de terminal.

2 Introduzca 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
```

Aparecerán los siguientes valores predeterminados:

```
Current Settings:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 Escriba **-help** para enumerar las opciones.

5 Para desactivar el certificado SSL de confianza en el cliente, cambie `DisableSSLCertTrust` 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 icono de Advanced Threat Prevention de Dell tiene una placa de identificación verde  en la barra de comandos.

2 Si hay un signo de exclamación en el icono, 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 las políticas del servidor Dell.

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 de Dell se crea en /Applications.

Recopilar archivos de registro para Endpoint Security Suite Enterprise

DellLogs.zip contiene los registros para el cliente Encryption 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 un equipo de extremo, el servidor Dell lo reconoce como agente.

Haga clic con el botón derecho del ratón en el icono 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 Remote Management Console de Dell.

Pestaña Vulnerabilidades de seguridad

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

Las políticas del servidor Dell 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 al servidor Dell.
- **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
- Carga malintencionada

Para obtener más información sobre las políticas de vulnerabilidades, consulte *AdminHelp*, disponible en la Remote Management Console de Dell.

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

Aprovisionar un inquilino para Advanced Threat Prevention

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

Requisitos previos

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

Aprovisionar un inquilino

1. Inicie sesión en Remote Management Console y vaya a **Administración de servicios**.
2. Haga clic en **Configurar servicio Advanced Threat Protection**. Importe sus licencias ATP si se produce un error en este punto.
3. La configuración guiada se inicia una vez que se han importado las licencias. Haga clic en **Siguiente** para empezar.
4. Lea y acepte el EULA (la casilla de verificación está **desactivada** de forma predeterminada) y haga clic en **Siguiente**.
5. Proporcione las credenciales de identificación a DDP Server para aprovisionar el inquilino. Haga clic en **Siguiente**. *No se permite aprovisionar un inquilino existente con marca Cylance.*
6. Descargue el certificado. Esto es necesario para poder llevar a cabo una recuperación si se produce algún problema con DDP Server. No se realiza automáticamente ninguna copia de seguridad de este certificado con el "actualizador" de la versión 9.2. Realice una copia de seguridad del certificado en una ubicación segura de otro equipo. Seleccione la casilla para confirmar que ha realizado una copia de seguridad del certificado y haga clic en **Siguiente**.
7. La configuración ha terminado. Haga clic en **Aceptar**.

Configuración de actualización automática del agente Advanced Threat Prevention

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

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

Cómo recibir actualizaciones automáticas del agente

Para inscribirse y recibir actualizaciones automáticas del agente:

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

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

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

Cómo dejar de recibir actualizaciones automáticas del agente

Para dejar de recibir actualizaciones automáticas del agente:

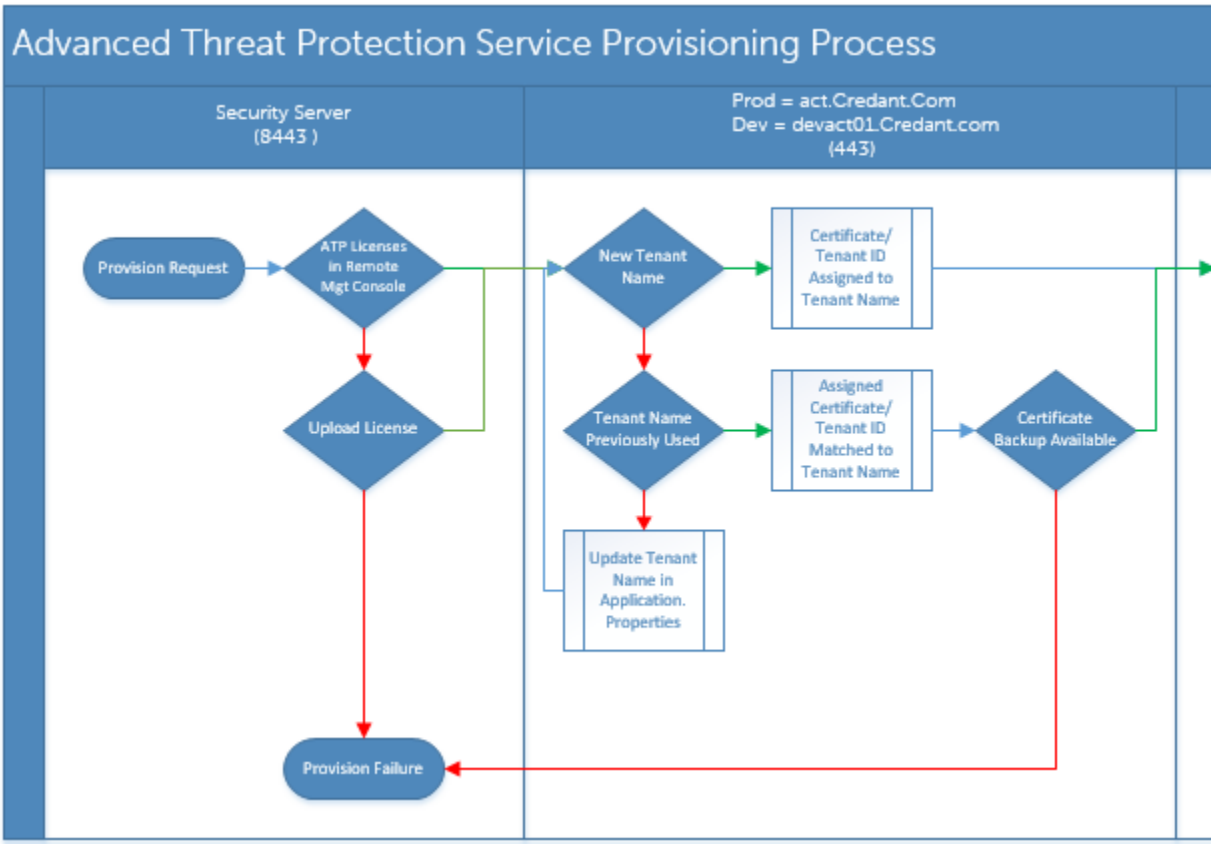
1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración** > **Administración de servicios**.

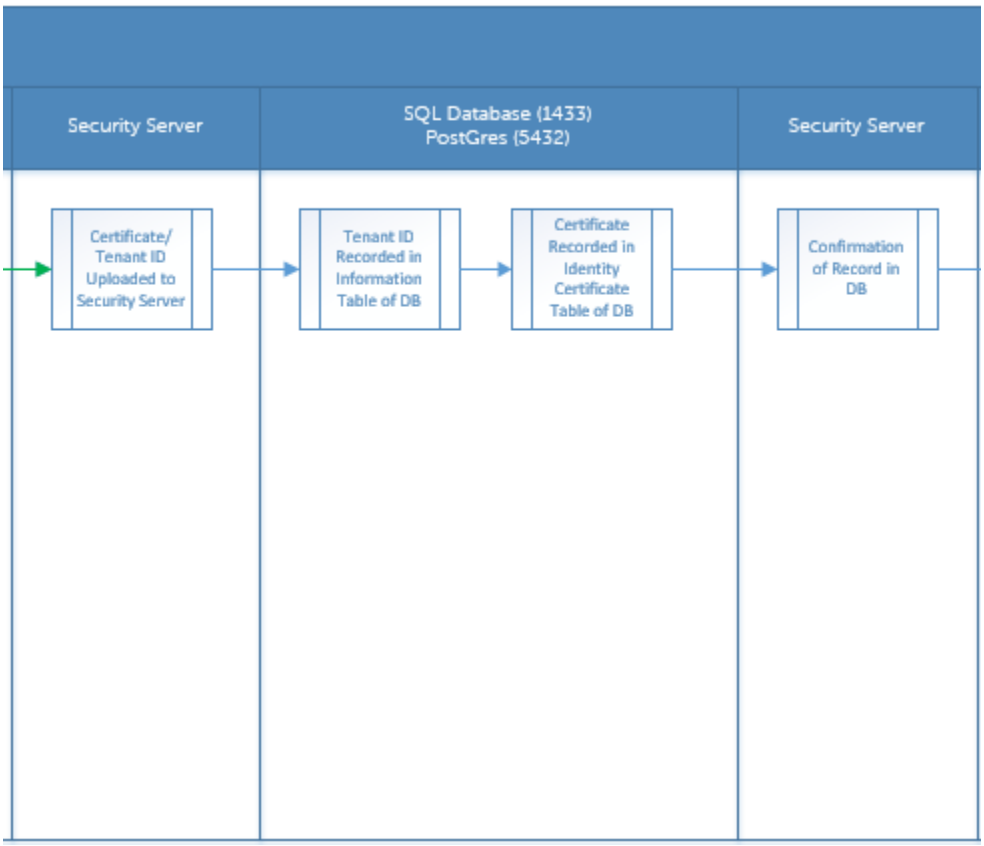
2 En la pestaña **Amenazas avanzadas**, bajo Actualización automática del agente, haga clic en el botón **Desactivar** y, a continuación, en el botón **Guardar preferencias**.

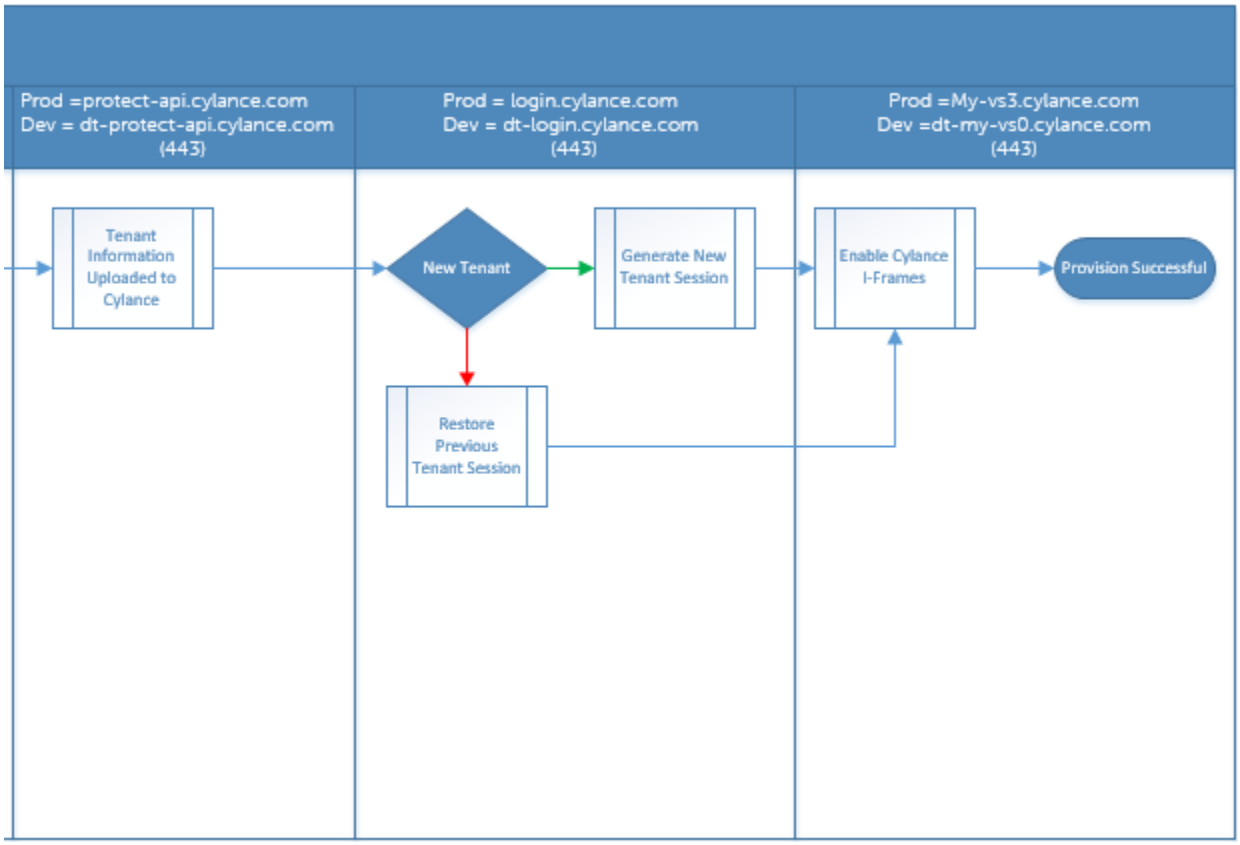
Solucionar problemas del cliente Advanced Threat Prevention

Comunicación de agentes y aprovisionamiento de Advanced Threat Prevention

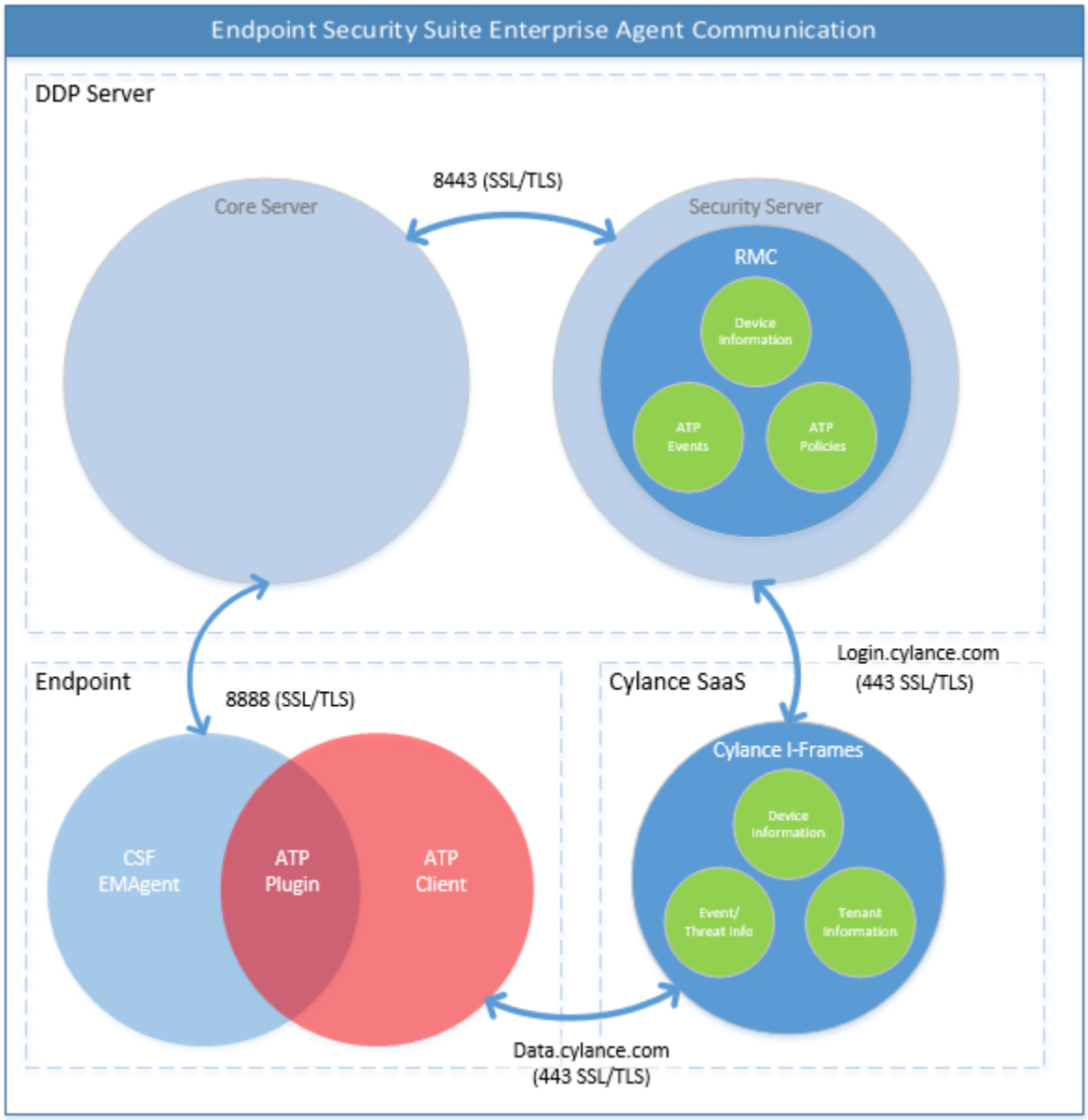
Los siguientes diagramas muestran el proceso de aprovisionamiento del servicio de Advanced Threat Prevention.


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


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



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


Endpoint Security Suite Enterprise Agent Communication
DDP Server
8443 (SSL/TLS)
Core Server
Security Server
RMC
Device Information
ATP Events
ATP Policies
Endpoint
8888 (SSL/TLS)
Cylance SaaS
Login.cylance.com
(443 SSL/TLS)
CSF EMAgent
ATP Plugin
ATP Client
Cylance I-Frames
Device Information
Event/ Threat Info
Tenant Information
Data.cylance.com
(443 SSL/TLS)

5

Glosario

Servidor de seguridad: se utiliza para las activaciones del cliente Encryption.

Política de proxy: se utiliza para distribuir políticas al software cliente Endpoint Security Suite Enterprise para Mac.

Remote Management Console: la consola de administrador para la implementación de toda la empresa.

Shield: en ocasiones, encontrará este término en la documentación y en la interfaz de usuario del cliente. "Shield" es un término que se utiliza para representar el software cliente.