Endpoint Security Suite Enterprise for Linux

Guía del administrador v2.1

Notas, precauciónes y advertencias

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

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

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

2018 - 11

Rev. A01

Contenido

1

Introducción

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

Descripción general

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

Servidor de administración de seguridad o Servidor virtual de administración de seguridad: proporciona una administración centralizada de las políticas de seguridad, se integra con los directorios empresariales existentes y crea informes. A efectos del presente documento, ambos servidores se citan como Dell Server, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Servidor virtual de administración de seguridad).

Advanced Threat Prevention para Linux tiene un archivo tar.gz, que contiene las tres RPM.

Cómo ponerse en contacto con Dell ProSupport

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

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

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

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

2

Requisitos

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.

Hardware

La siguiente tabla indica el hardware mínimo compatible.

Hardware

- Como mínimo 500 MB de espacio de disco libre
- 2 GB RAM
- Tarjeta de interfaz de red 10/100/1000 o Wi-Fi

NOTA: IPv6 no es compatible actualmente.

Software

La tabla a continuación muestra qué software es compatible.

Sistemas operativos (kernel de 64 bits)

- CentOS Linux v7.1 a v7.5
- Red Hat Enterprise Linux v7.1 a v7.5

Puertos

- El puerto 443 (https) se utiliza para la comunicación y debe estar abierto en el firewall para que los agentes puedan comunicarse con la consola de administración. 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 las computadoras cliente puedan acceder a lo siguiente:

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
Comunicación del Core Server	HTTPS	TCP	8888	Permite la comunicación del Core Server	Entrada/Salida

- Para obtener más información, consulte SLN303898.

Endpoint Security Suite Enterprise for Linux y Dependencias

Endpoint Security Suite Enterprise for Linux utiliza Mono y dependencias para que se pueda instalar y activar en el sistema operativo Linux. El instalador descargará e instalará las dependencias necesarias. Después de la extracción del paquete, puede ver qué dependencias se están aprovechando mediante el uso del siguiente comando:

```
./showdeps.sh
```

Compatibilidad

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

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

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

Funciones	Políticas	Windows	macOS	Linux
Acciones de archivo				
	Cuarentena automática (no segura)	x	x	x
	Cuarentena automática (anormal)	x	x	x
	Carga automática	x	x	x
	Lista segura de políticas	x	x	x
Acciones de memoria				
	Protección de memoria	x	x	x
Explotación				
	Dinamización de pilas	x	x	x
	Protección de pilas	x	x	x
	Sobrescribir código	x	n/d	
	Extracción de RAM	x	n/d	
	Contenido malicioso	x		
Inyección del proceso				
	Distribución remota de memoria	x	x	n/d
	Asignación remota de memoria	x	x	n/d
	Escritura remota en la memoria	x	x	n/d
	Escritura remota de PE en la memoria.	x	n/d	n/d

Funciones	Políticas	Windows	macOS	Linux
	Sobrescribir remotamente el código	x	n/d	
	Desasignación remota de memoria	x	n/d	
	Creación remota de hebras	x	x	
	APC remota programada	x	n/d	n/d
	Inserción de DYLD		x	x
Escalamiento				
	Lectura de LSASS	x	n/d	n/d
	Asignación de cero	x	x	
Configuración de protección				
	Control de ejecución	x	x	x
	Evitar la interrupción del servicio desde el dispositivo	x	x	
	Eliminar los procesos en ejecución no seguros y sus subprocesos	x	x	x
	Detección de amenazas en segundo plano	x	x	x
	Detectar nuevos archivos	x	x	x
	Tamaño máximo de archivo de almacenamiento para escanear	x	x	x
	Excluir carpetas específicas	x	x	x
	Copiar muestras de archivos	x		
Control de la aplicación				
	Cambiar ventana	x		x
	Exclusiones de carpetas	x		
Configuración del agente				
	Activar carga automática de archivos de registro	x	x	x
	Activar las notificaciones de escritorio	x		
Control de la secuencia de comandos				
	Secuencia de comandos activa	x		
	PowerShell	x		
	Macros de Office	x		n/d

Funciones	Políticas	Windows	macOS	Linux
	Bloquear el uso de la consola PowerShell	x		
	Aprobar los scripts en estas carpetas (y subcarpetas)	x		
	Nivel de registro	x		
	Nivel de protección automática	x		
	Actualización automática	x		
	Ejecutar una detección (de la UI de agente)	x		
	Eliminar cuarentena (UI de agente y de consola)	x		
	Modo desconectado	x		x
	Datos detallados de la amenaza	x		
	Lista segura de certificados	x	x	n/d
	Copiar muestras de malware	x	x	x
	Configuración de proxy	x	x	x
	Comprobación de la política del manual (UI de agente)	x	x	

Tareas

Ha finalizado la instalación

Esta sección lo guía a través de la instalación de Endpoint Security Suite Enterprise para Linux.

Requisitos previos

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

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

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

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

  Guía de instalación y migración de Servidor de administración de seguridad

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

Instalación con la línea de comandos

Para instalar el cliente Endpoint Security Suite Enterprise mediante la línea de comandos, siga estos pasos.

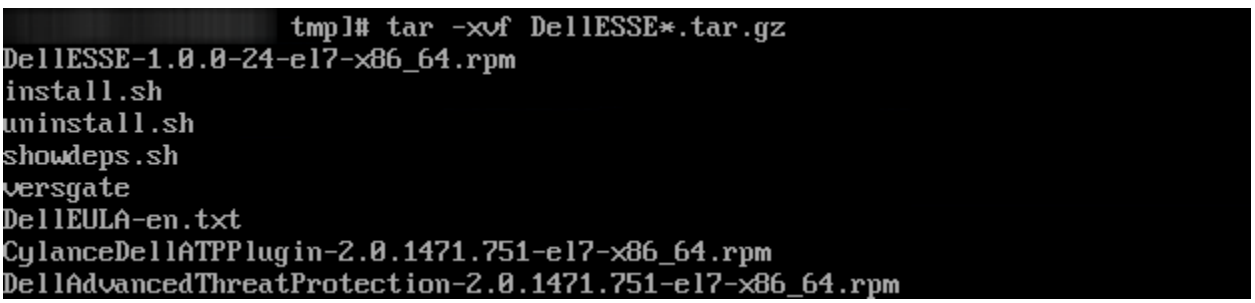
Se debe usar el comando **sudo** para invocar privilegios administrativos durante la instalación. Cuando se le solicite, ingrese sus credenciales.

La aprobación de la huella digital se muestra solo durante la primera instalación.

1 Busque y descargue el paquete de instalación (DellESSE-1.x.x-xxx.tar.gz) mediante su cuenta FTP de Dell.

2 Extraiga el tar.gz con el siguiente comando:

```
tar -xvf DellESSE*.tar.gz
```



3 El siguiente comando ejecuta las secuencias de comandos de instalación para las RPM y dependencias necesarias:

```
sudo ./install.sh
```

4 En *el host Dell Security Management Server* ingrese el nombre completo de host de Dell Server para administrar el usuario de destino. Por ejemplo, server.organization.com.

5 En *el puerto Dell Security Management Server*, verifique que el puerto se configure en 8888.

```
Dell Endpoint Security Suite Enterprise (ESSE) Installation
Dell Security Management Server Host?
Dell Security Management Server Port?
```

6 Ingrese **y** cuando se le solicite instalar el paquete DellESSE y sus dependencias.

```
 libXfixes      x86_64 5.0.3-1.el7             base                       18
 libXrender     x86_64 0.9.10-1.el7            base                       26
 libXxf86vm     x86_64 1.1.4-1.el7             base                       18
 libexif        x86_64 0.6.21-6.el7            base                      347
 libjpeg-turbo x86_64 1.2.90-5.el7             base                      134
 libpng         x86_64 2:1.5.13-7.el7_2        base                      213
 libtiff        x86_64 4.0.3-27.el7_3          base                      170
 libxcb         x86_64 1.12-1.el7              base                      211
 libxshmfence   x86_64 1.2-1.el7               base                      7.2
 lyx-fonts      noarch 2.2.3-1.el7             epel                      159
 mesa-libEGL    x86_64 17.0.1-6.20170307.el7 base                         82
 mesa-libGL     x86_64 17.0.1-6.20170307.el7 base                        155
 mesa-libgbm    x86_64 17.0.1-6.20170307.el7 base                         32
 mesa-libglapi x86_64 17.0.1-6.20170307.el7 base                         41
 pixman         x86_64 0.34.0-1.el7            base                      248

Transaction Summary
================================================================================
Install  1 Package (+27 Dependent packages)

Total size: 96 M
Total download size: 3.8 M
Installed size: 104 M
Is this ok [y/d/N]:
```

7 Ingrese **y** si se le pregunta por la aprobación de la *Huella digital.*

```
Total                                                   452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a0 0eb5
 Package        : centos-release-7-3.1611.el7.centos.x86_64 (@anaconda)
 From           : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

8 Ingrese **y** cuando se le solicite instalar el paquete *DellAdvancedThreatProtection*.

```
Dependencies Resolved

================================================================================
 Package  Arch   Version      Repository                                   Size
================================================================================
Installing:
 DellAdvancedThreatProtection
         x86_64 2.0.1461-739 /DellAdvancedThreatProtection-2.0.1461.739-el7-x86_64 149 M

Transaction Summary
================================================================================
Install  1 Package

Total size: 149 M
Installed size: 149 M
Is this ok [y/d/N]:
```

9 Ingrese **y** cuando se le solicite instalar el paquete *CylanceDellATPPlugin*.

```
Dependencies Resolved

================================================================================
 Package     Arch   Version Repository                                   Size
================================================================================
Installing:
 CylanceDellATPPlugin
             x86_64 2.2.4-0 /CylanceDellATPPlugin-2.0.1461.739-el7-x86_64 439 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 439 k
Installed size: 439 k
Is this ok [y/d/N]:
```

10 La instalación finalizó.

```
Installed:
  DellAdvancedThreatProtection.x86_64 0:2.0.1461-739

Complete!
```

11 Consulte Verificar la instalación de Endpoint Security Suite Enterprise para Linux.

Desinstalación con la línea de comandos

Para desinstalar Endpoint Security Suite Enterprise para Linux mediante la línea de comandos, siga estos pasos.

1 Acceda a una ventana terminal.

2 Desinstale el paquete con el siguiente comando:

```
sudo ./uninstall.sh
```

3 Pulse **Intro**.

Endpoint Security Suite Enterprise para Linux ya está desinstalado y la computadora se puede utilizar con normalidad.

Ver detalles

Después de haber instalado Endpoint Security Suite Enterprise para Linux, Dell Server lo reconoce como terminal.

atp -t

El comando **`atp - t`** muestra todas las amenazas detectadas en el dispositivo y la acción realizada. Las amenazas son una categoría de sucesos que se acaban de detectar como archivos o programas potencialmente inseguros y que requieren correcciones guiadas.

```
Quarantined 17E76B830F9F30A39F078F5A69AD87B3838DB73A28EC893BD06EAF95D6E464E2 /tmp/threats/LINUXTarGz
Archive
Quarantined 20FBC1FDFCDC96A7E21FB1C700A6517A6171173ZA0D31FC25A60609710ECBE09 /tmp/threats/LINUXAutoB
lockNoService
Quarantined 2D49A3F81AF3362FE806E417DF2807C960314FF4F271B5B1360964163CB49886 /tmp/threats/LINUXGBL2
Quarantined 52D74BD1555D7C82746112C44F4D9A916B9DA286DD5B14D7665D4167BB1EB5D8 /tmp/threats/LINUXRunni
ngAutoQ
Quarantined 70F193F3C20Z3A7542338142CA89F1076AZ38AB7BAAD4202BZDCEDA7286E43D9 /tmp/threats/LINUXTest1
Quarantined 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F0158E0D519CEC1D860E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC20640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED085ED842423A172B4BED7702E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F170A6413A0A7E84437098777111FB1CA6E31F /tmp/threats/LINUXAutoB
lockExecution
```

Estas entradas detallan la acción realizada, ID de hash y la ubicación de la amenaza.

- **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 Remote Management Console de Dell Server.

Verificar la instalación

De manera opcional, puede verificar que se realizó correctamente la instalación.

- En el cliente, acceda a una ventana terminal.
- Antes de que se reciba una secuencia de la política, el cliente se registra con Dell Server.
- El archivo */var/log/dell/ESSE/DellAgent.00.log* detalla la comunicación con Dell Server y la interacción complemento/servicio.
  El texto adjunto confirma que el cliente recibió las políticas desde Dell Server:

```
2017.12.12 14:26:02.794 [02390] (00009) I Comm    : Received Id=ba150b8e-b1d3-44
5a-81e9-426e77fbb043
2017.12.12 14:26:02.795 [02390] (00009) I Comm    : ReceivedEdition enterprisese
rver
2017.12.12 14:26:02.847 [02390] (00009) I Comm    : Successfully added memory ex
clusions to policy
2017.12.12 14:26:03.322 [02390] (00009) I Comm    : new policy seq# 9 received
2017.12.12 14:26:03.385 [02390] (00009) I Comm    : registered Centos7-3-64-MH w
ith server
2017.12.12 14:26:03.392 [02390] (00009) I Comm    : closing connection to https:
--More--(39%)
```

  El texto adjunto confirma que el servicio de Dell se detuvo para cargar el complemento Advanced Threat Prevention:

```
//cedmz.credce.com:8888/agent
2017.12.12 14:27:05.883 [02390] (00009) I Comm    : next contact with server sch
eduled for 12/12/2017 8:27:05 PM
2017.12.12 14:27:10.442 [02390] (00005) I Agent   : Dell Data Protection stopped
---date--- ----time---- --pid-- -thrid-   -subsys-  ----------------------------
--message-------------------------------
2017.12.12 14:27:12.968 [02551] (00005) I Agent   : service name is "DellMgmtAge
nt"
2017.12.12 14:27:12.970 [02551] (00005) I Agent   : product name is "Dell Data P
```

El texto adjunto confirma que se cargaron los tres complementos Endpoint Security Suite Enterprise para Linux:

```
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : machine name is "centosvm2.ddsdemos.com"
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : process is 64-bit
2018.02.18 10:51:36.952 [01077] (00005) I Agent   : domain is "(none)"
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Server Communication Manager" 1.
 Id={CAA1A89F-AF21-4C1E-9407-1E185FFEEB5C} in 69 ms
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Auditing and Reporting Service"
.0 Id={0E969074-3164-467F-BF3D-D9E695F48240} in <1 ms
2018.02.18 10:51:37.069 [01077] (00005) I AdvATP  : Advanced Threat Prevention Cylance component lo
ging initialized
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded plugin "Advanced Threat Prevention" 1.0
d={96BBD97F-9BF0-4D61-94F8-A9884F8DC287} in 8 ms
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded 3 plugins
2018.02.18 10:51:37.090 [01077] (00010) I Comm    : AgentID 00397403-c05f-4cbf-b6b4-e15dd577186a
2018.02.18 10:51:37.102 [01077] (00011) I AdvATP  : AdvancedAtpManager Starting
2018.02.18 10:51:37.125 [01077] (00011) I AdvATP  : management is active
2018.02.18 10:51:37.129 [01077] (00011) I AdvATP  : processing new policies - Policy list count=1
```

`atp -s` - Incluye lo siguiente:

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

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp -s
Registration Status: Registered
Serial Number: 0088ab40-ce18-43fa-a959-85f44e5ff251
Policy:  (Online)
```

El siguiente comando detalla las variables de la línea de comandos para Endpoint Security Suite Enterprise para Linux:

```
/opt/cylance/desktop/atp --help
```

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp --help
usage: atp <options>
options:
    -r, --register=token    : register with Dell Data Security servers with the
provided token
    -s, --status            : get status of Advanced Threat Prevention
    -u, --checkupdates      : check for updates
    -b, --start-bg-scan     : start background scan
    -B, --stop-bg-scan      : stop background scan
    -d, --scan-dir=dir      : scan directory
    -l, --getloglevel       : get current log level
    -L, --setloglevel=level : set log level
    -P, --getpolicytime     : get the policy update time
    -p, --checkpolicy       : check for policy updates
    -t, --threats           : list threats
    -q, --quarantine=id     : quarantine a file by id (hash)
    -w, --waive=id          : waive a file by id (hash)
    -v, --version           : print this tools version
    -h, --help              : atp help
```

El comando Advanced Threat Prevention *atp* se agrega al directorio */usr/sbin*, que se incluirá normalmente en una variable de RUTA de shell, de modo que se puede utilizar en la mayoría de los casos sin una ruta explícita.

Solución de problemas

Desactivar el certificado SSL de confianza

Si el certificado del servidor de una computadora se perdió o se autofirmó, debe deshabilitar el certificado SSL de confianza en el lado del cliente solamente.

Si utiliza un certificado poco común, importe el certificado raíz al almacén de certificados Linux, a continuación, reinicie los servicios de Endpoint Security Suite para Linux con el siguiente comando: `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Acceda a una ventana terminal.

2 Ingrese la ruta de acceso de la aplicación CsfConfig:
```
/usr/lib/dell/esse/CsfConfig
```

3 Ejecute CsfConfig.app:
```
sudo ./CsfConfig
```

Aparecerán los siguientes valores predeterminados:

Configuración actual:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = Falso

DumpXmlInventory = Falso

DumpPolicies = Falso

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

5 Para desactivar el certificado SSL de confianza en la computadora de destino, ingrese el siguiente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

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 la *aplicación CsfConfig* como se describió más arriba.

2 Para cambiar *DumpXmlInventory* a *Verdadero*, ingrese el siguiente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 Para cambiar *DumpPolicies* a *Verdadero*, ingrese el siguiente comando:
```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

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

4 Para ver los archivos de registro inventory.xml y policies.xml, vaya a */var/log/Dell/Dell Data Protection*.

NOTA: Es posible que los cambios de CsfConfig no se apliquen de manera inmediata.

Recopilar archivos de registro

Los registros de Endpoint Security Suite Enterprise for Linux se encuentran en la siguiente ubicación: */var/log/Dell/ESSE*. Para generar registros, utilice el siguiente comando: **. /getlogs.sh**

Para obtener información sobre cómo recopilar los registros, consulte SLN303924.

Aprovisionamiento de un inquilino

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

Requisitos previos

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

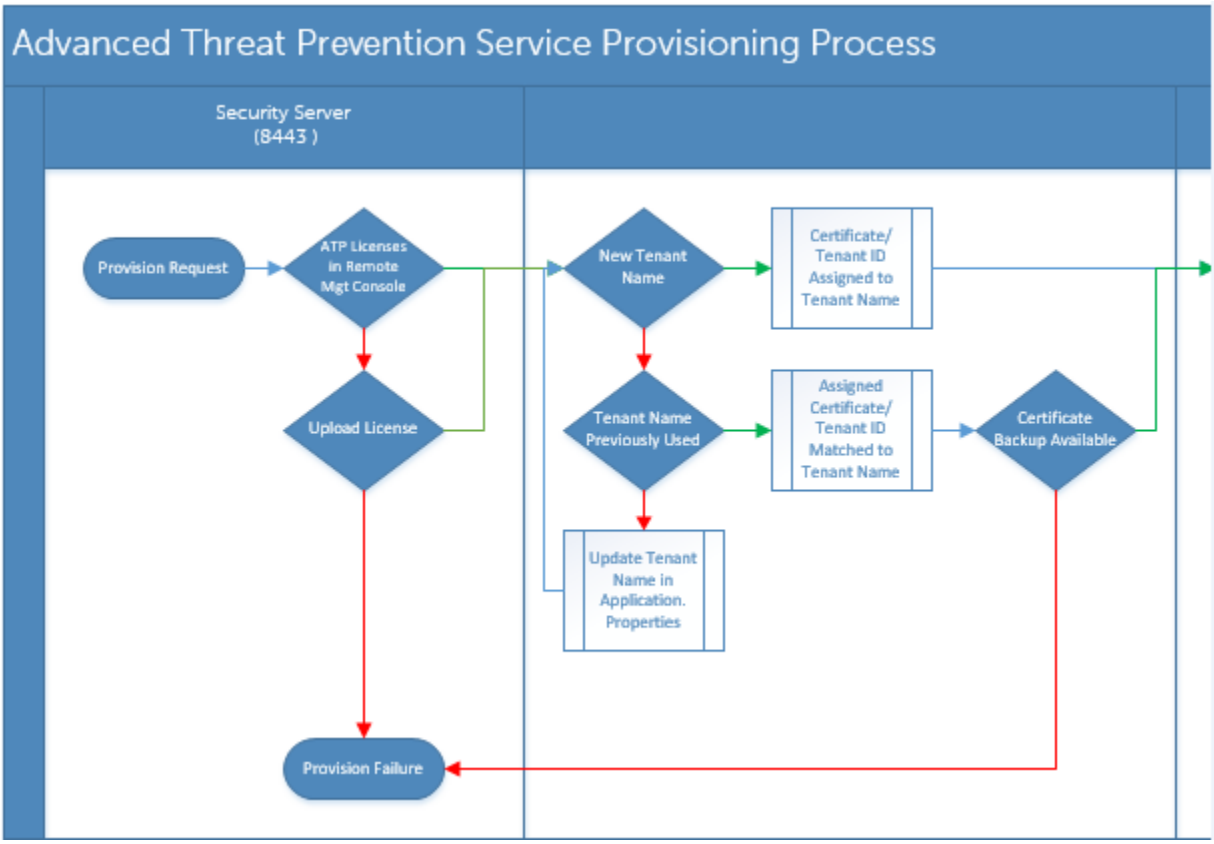
Aprovisionamiento de un inquilino

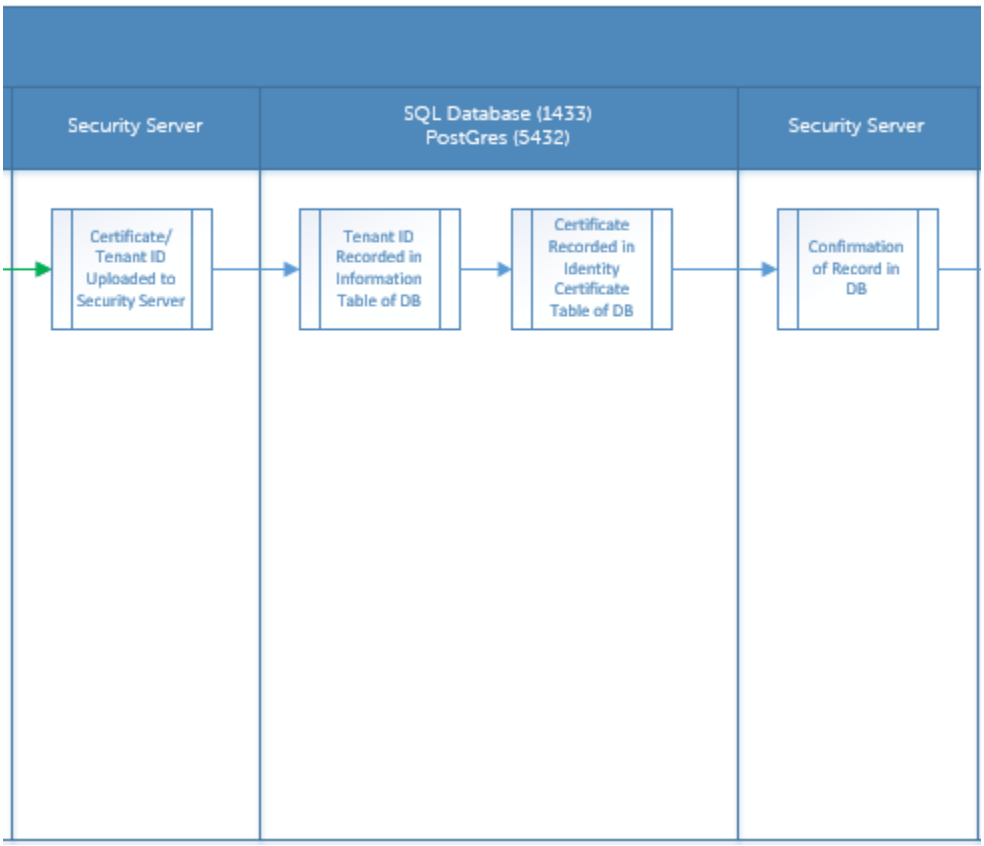
1. Como administrador de Dell, inicie sesión en la Remote Management Console.
2. En el panel izquierdo de la consola de administración, haga clic en **Administración > Administración de servicios**.
3. Haga clic en **Configurar servicio Advanced Threat Protection**. Importe sus licencias Advanced Threat Prevention si se produce un error en este punto.
4. La configuración guiada inicia una vez que se han importado las licencias. Haga clic en **Siguiente** para empezar.
5. Lea y acepte el EULA y haga clic en **Siguiente**.
6. Proporcione las credenciales de identificación a Dell Server para aprovisionar el inquilino. Haga clic en **Siguiente**. *No se permite aprovisionar un inquilino existente con marca Cylance.*
7. Descargue el certificado. Esto es necesario para poder llevar a cabo una recuperación si se produce algún problema con Dell Server. No se realiza automáticamente una copia de seguridad de este certificado. Realice una copia de seguridad del certificado en una ubicación segura de otro equipo. Seleccione la casilla de verificación para confirmar que se realizó una copia de seguridad del certificado y haga clic en **Siguiente**.
8. La configuración ha terminado. Haga clic en **Aceptar**.

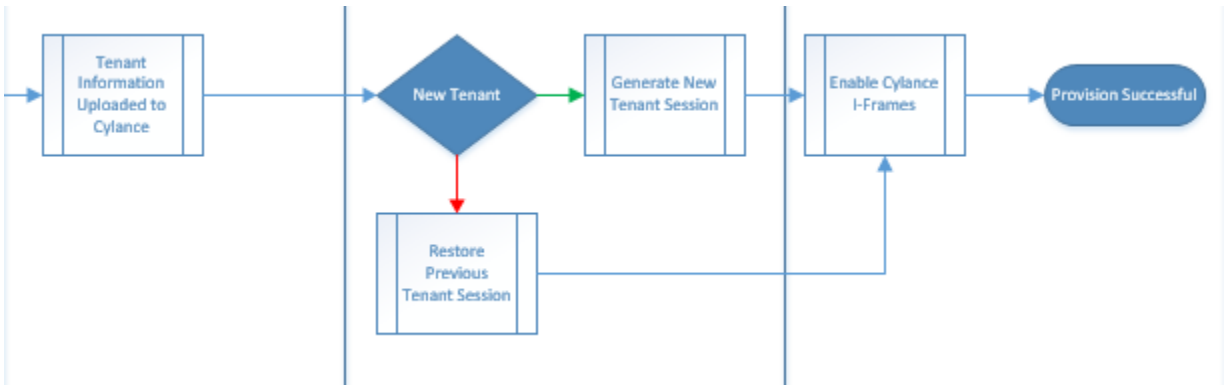
Solución de problemas de aprovisionamiento

Comunicación de agentes y aprovisionamiento

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


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
Provision Failure
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


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.