ESET PROTECT

Guía de implementación del dispositivo virtual

Haga clic aquí para ver la versión de la Ayuda de este documento

ESET PROTECT está desarrollado por ESET, spol. s r.o.

Para obtener más información, visite https://www.eset.com.

Soporte técnico: https://support.eset.com

REV. 12/04/2024

1 Dispositivo virtual de ESET PROTECT 1
1.1 Acerca de la ayuda 1
1.2 Requisitos previos 2
1.2 Configuraciones recomendadas del sistema 3
2 Hipervisores compatibles 4
3 Fases de implementación y mantenimiento del dispositivo virtual de ESET PROTECT 4
4 Descargar dispositivo virtual de ESET PROTECT 5
5 Contraseñas del dispositivo virtual de ESET PROTECT 6
6 Proceso de implementación del dispositivo virtual de ESET PROTECT 6
6.1 vSphere 7
6.2 VMware Workstation/Player 9
6.3 Microsoft Hyper-V 11
6.4 Oracle VirtualBox 13
6.5 Citrix 15
7 Configuración del dispositivo virtual de ESET PROTECT 17
7.1 Dispositivo ESET PROTECT Server 18
7.2 ESET PROTECTDispositivo MDM 21
8 Consola de administración del dispositivo virtual de ESET PROTECT 26
8.1 Configurar la dirección IP estática 28
8.2 Activar o desactivar el acceso remoto 30
8.3 Copia de seguridad de la base de datos 31
8.4 Restaurar la base de datos 33
8.5 Restauración tras recuperación de instantánea 34
8.6 Recuperar la base de datos de otro servidor 35
8.7 Cambiar la contraseña de la máquina virtual 39
8.8 Cambiar la contraseña de la base de datos 40
8.9 Unirse de nuevo al dominio 41
8.10 Configurar el dominio 43
8.11 Restablecimiento a valores de fábrica 44
9 Interfaz de administración Webmin 46
9.1 Panel principal 47
9.2 Sistema 49
9.3 Servidores 50
9.3 ESET PROTECT 50
9.4 Herramientas 52
9.5 Red 53
10 Certificados de ESET PROTECT 54
11 Actualización o migración del dispositivo virtual de ESET PROTECT 55
12 Recuperación ante desastres del dispositivo virtual de ESET PROTECT 57
13 Resolución de problemas 58
14 Preguntas frecuentes sobre el dispositivo virtual de ESET PROTECT 59
14.1 Cómo saber qué componentes de ESET PROTECT hay instalados 60
14.2 Cómo activar el ping en el dispositivo virtual de ESET PROTECT 61
14.3 ¿Tengo que añadir otros componentes al dispositivo virtual de ESET PROTECT? 62
14.4 Cómo activar el proxy HTTP Apache en mi dispositivo virtual de ESET PROTECT después de la configuración inicial 62
14.5 Cómo configurar LDAP para que permita la sincronización del grupo estático en el dispositivo virtual de ESET PROTECT 63
14.6 Configurar la conexión LDAPS con un dominio 63
14.7 Cómo recuperar una contraseña olvidada del dispositivo virtual de ESET PROTECT 64

14.8 Cómo cambiar la cadena de conexión a la base de datos de ESET PROTECT 64
14.9 Cómo configurar Hyper-V Server para el Sensor RD 65
14.10 Cómo cambiar los números de puerto del dispositivo virtual de ESET PROTECT 65
14.11 Cómo aumentar el tamaño de la memoria para MySQL Server 66
14.12 Error con ESET PROTECT al ejecutarlo en Hyper-V Server 2012 R2 66
14.13 Cómo mejorar el rendimiento de Oracle VirtualBox 67
14.14 Cómo activar el comando YUM en el servidor proxy HTTP 67
14.15 Cómo actualizar el sistema operativo de un ordenador que ejecute el servidor del dispositivo virtual de ESET PROTECT 67
14.16 Cómo desactivar SELinux de forma permanente 68
14.17 Cómo reiniciar la consola de administración del dispositivo virtual 68
14.18 Cómo utilizar el proxy para las conexiones de los agentes 68
14.19 Cómo activar SSH 69
15 Acuerdo de licencia para el usuario final 69
16 Política de privacidad 76

Dispositivo virtual de ESET PROTECT

El dispositivo virtual de ESET PROTECT (ESET PROTECT VA) está disponible para aquellos usuarios que quieren ejecutar ESET PROTECT en un entorno virtualizado. Además, el dispositivo virtual de ESET PROTECT simplifica la implementación de ESET PROTECT y resulta más rápido que utilizar el instalador todo en uno o paquetes de instalación de componentes.

El dispositivo virtual de ESET PROTECT se puede implementar en la mayoría de entornos virtuales. Es compatible con hipervisores nativos o sin sistema operativo ((VMware vSphere/ESXi y Microsoft Hyper-V), así como en hipervisores alojados que normalmente se ejecutan en sistemas operativos de escritorio (VMware Workstation, VMware Player y Oracle VirtualBox); consulte Hipervisores compatibles para acceder a una lista completa.

En esta guía se describe de forma detallada cómo implementar y gestionar el dispositivo virtual de ESET PROTECT, incluidas sus nuevas funciones:

- Consola de administración del dispositivo virtual de ESET PROTECT: es una sencilla **Interfaz de usuario de texto** (TUI) basada en un menú principal. La interfaz le ayudará con los comandos de texto pidiéndole que especifique valores cuando sea necesario. Hasta los usuarios que no tienen mucha experiencia con CentOS 7 u otros sistemas operativos Linux podrán utilizar y gestionar el dispositivo virtual de ESET PROTECT con facilidad. Estas son algunas de las principales funciones:

    - Configurar la dirección IP estática: especifique manualmente la dirección IP estática si el dispositivo virtual de ESET PROTECT no recibe una dirección IP asignada por un servidor DHCP.

    - Recuperar la base de datos de otro servidor: si necesita actualizar o migrar el dispositivo virtual de ESET PROTECT.

    - Copia de seguridad y restauración de la base de datos de ESET PROTECT: estas funciones son importantes para su estrategia de recuperación ante desastres y están disponibles en caso de problemas con el dispositivo virtual de ESET PROTECT.

    - Restablecimiento a valores de fábrica: restaura los valores de fábrica del dispositivo. Puede resultar útil si tiene problemas con el dispositivo virtual de ESET PROTECT. Debe disponer de una copia de seguridad de la base de datos para no perder sus datos.

- Interfaz de administración de Webmin: es una interfaz web de terceros que simplifica la administración de un sistema Linux. Le ofrece la comodidad que supone poder administrar el dispositivo virtual de ESET PROTECT de forma remota, desde un navegador web y mediante una interfaz intuitiva. En este documento se describen los módulos más importantes de Webmin.

Acerca de la ayuda

Esta guía, la **Guía de implementación de VA**, contiene instrucciones sobre cómo implementar y configurar el dispositivo virtual de ESET PROTECT (ESET PROTECT VA). Está destinada a toda aquella persona que quiera implementar, gestionar y actualizar ESET PROTECT VA.

Por motivos de coherencia y para evitar confusiones, la terminología que se usa en esta guía está basada en los nombres de parámetro de ESET PROTECT. También usamos una serie de símbolos para destacar temas de especial interés o importancia.

Las notas pueden contener información valiosa, como funciones específicas o un vínculo a un tema relacionado.

Este contenido requiere su atención y no debe ignorarse. Normalmente ofrece información que no es vital, pero sí importante.

Se trata de información vital que debe tratar con mayor cautela. Las advertencias tienen como finalidad específica evitar que cometa errores que pueden tener consecuencias negativas. Lea y comprenda el texto situado en secciones de advertencia, ya que hace referencia a ajustes del sistema muy delicados o a cuestiones que pueden suponer un riesgo.

Se trata de una situación de ejemplo que describe un caso de uso pertinente para el tema en el que se incluye. Los ejemplos se usan para detallar temas más complicados.

Convención	Significado
Negrita	Nombres de elementos de la interfaz, como recuadros y botones de opciones.
Cursiva	Marcadores de posición de información que facilita. Por ejemplo, nombre de archivo o ruta de acceso significa que se debe escribir la ruta de acceso o el nombre de un archivo.
`Courier New`	Ejemplos de código o comandos.
Hipervínculo	Ofrece un acceso rápido y sencillo a temas como referencia cruzada o a sitios web externos. Los hipervínculos aparecen resaltados en azul y pueden estar subrayados.
%ProgramFiles%	El directorio del sistema operativo Windows en el que se almacenan los programas instalados de Windows y de otras empresas.

- La Ayuda en línea es la fuente principal de contenido de ayuda. Siempre que tenga una conexión a Internet disponible, se mostrará automáticamente la versión más reciente de la Ayuda en línea. Las páginas de la Ayuda en línea de ESET PROTECT presentan cuatro pestañas activas en el encabezado de navegación superior: Instalación/Actualización, Administración, Implementación del dispositivo virtual y Guía de SMB.
- Los temas de esta guía están divididos en diversos capítulos y subcapítulos. Puede buscar información pertinente desde el campo Buscar situado en la parte superior.

Cuando abra una guía del usuario desde la barra de navegación situada en la parte superior de la página, la búsqueda se limitará al contenido de dicha guía. Por ejemplo, si abre la guía Administración, no se incluirán en los resultados de la búsqueda los temas de las guías Instalación/Actualización e Implementación del dispositivo virtual.

- La Base de conocimiento ESET contiene respuestas a las preguntas más frecuentes, así como soluciones recomendadas para distintos problemas. Esta Base de conocimiento la actualizan periódicamente los especialistas técnicos de ESET, y es la herramienta más potente para resolver diversos tipos de problema.
- El Foro de ESET ofrece a los usuarios de ESET una forma sencilla de obtener ayuda y de ayudar a otras personas. Puede publicar cualquier problema o pregunta que tenga con respecto a sus productos ESET.

Requisitos previos

Antes de implementar el dispositivo virtual de ESET PROTECT se deben cumplir los siguientes requisitos:

- Debe usar un hipervisor compatible.

- Asegúrese de que el sistema operativo invitado (si se usa un hipervisor alojado, como VMware Workstation/Player u Oracle VirtualBox) sea compatible.

- Compruebe que la configuración del reloj del sistema esté sincronizada entre los sistemas operativos cliente e invitado.

- **VT debe estar habilitado** en la BIOS del sistema host. Esta función puede recibir el nombre VT, Tecnología Vanderpool, Tecnología de virtualización, VMX o Extensiones de máquina virtual. Este ajuste suele estar en la pantalla de seguridad de la BIOS. La ubicación de dicho ajuste varía en función del proveedor del sistema.

- Asegúrese de que la conexión del adaptador de red de su máquina virtual esté configurada como **Puente** (o como **NAT**). Durante la configuración del dispositivo virtual de ESET PROTECT puede especificar los ajustes de la red, incluidos los detalles del dominio, para que la tarea Sincronización del grupo estático se ejecute correctamente.

- Si está usando el modo **NAT**, en la máquina virtual debe estar configurado el reenvío de puertos para que pueda accederse a ESET PROTECT desde la red. Los puertos que requieren reenvío se muestran en la ventana de la consola del dispositivo virtual de ESET PROTECT después de implementarlo y configurarlo.

- El dispositivo virtual de ESET PROTECT solo es compatible con entornos IPv4. Aunque es posible configurar manualmente un entorno IPv6, no se admite el uso de IPv6.

Se recomienda crear una instantánea del dispositivo virtual de ESET PROTECT que acaba de implementar y configurar y sincronizarla con la instancia de Active Directory. También se recomienda crear una instantánea antes de implementar ESET Management Agent en los ordenadores cliente.

- Los certificados de ESET PROTECT son necesarios para implementar ESET PROTECT MDM. Debe tener una instancia de ESET PROTECT en ejecución para generar estos certificados, los cuales cifran la comunicación entre los componentes de ESET PROTECT.

Configuraciones recomendadas del sistema

En función de las dimensiones de la infraestructura, y más concretamente del número de máquinas cliente que el dispositivo virtual de ESET PROTECT gestionará, tenga en cuenta la configuración mínima y recomendada de la máquina virtual.

Las siguientes recomendaciones de dimensionamiento se aplican a ESET PROTECT Server y al dispositivo virtual de ESET PROTECT MDM:

Número de clientes	Número de núcleos	Tamaño de la RAM	Otros
Menos de 5.000 clientes	4	4 GB	Disco de aprovisionamiento pesado, cambie la configuración manualmente para aumentar el tamaño de la memoria para MySQL.
Más de 5.000 clientes	8	8 GB	Aumente proporcionalmente los recursos a disposición del dispositivo virtual de ESET PROTECT para evitar problemas de rendimiento.

Si tiene previsto tener más de 5.000 clientes administrados, se recomienda encarecidamente instalar ESET PROTECT Server/MDM en una máquina física en la que se ejecute Microsoft Windows Server con Microsoft SQL Server.

Hipervisores compatibles

El dispositivo virtual de ESET PROTECT (*protect_appliance.ova*) e un dispositivo de la familia de hardware virtual `vmx-07`.

El dispositivo virtual solo es compatible con los hipervisores indicados. Su ejecución en otros hipervisores será por cuenta y riesgo del usuario.

Hipervisor	Versión	Dispositivo ESET PROTECT Server	ESET PROTECTDispositivo MDM
VMware vSphere/ESXi	6.5 y más recientes	✔	✔
VMware Workstation	9 y más recientes	✔	✔
VMware Player	7 y más recientes	✔	✔
Microsoft Hyper-V	Server 2012, 2012 R2, 2016, 2019	✔	✔
Oracle VirtualBox	6.0 y más recientes	✔	✔
Citrix	7.0 y más recientes	✔	✔

Se recomienda utilizar un servidor DHCP en la red para asignar una dirección IP al dispositivo virtual de ESET PROTECT. Esta dirección IP es necesaria para acceder a la interfaz web de configuración del dispositivo virtual de ESET PROTECT. Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática.

Fases de implementación y mantenimiento del dispositivo virtual de ESET PROTECT

La implementación del dispositivo virtual de ESET PROTECT consta de las siguientes fases principales, necesarias para una implementación y configuración correctas:

1. Proceso de implementación del dispositivo de ESET PROTECT: implementación real del archivo ESET PROTECT del archivo *OVA* del dispositivo virtual de ERA en su hipervisor.

2. Configuración del dispositivo virtual de ESET PROTECT: configuración posterior a la implementación realizada mediante la interfaz web del dispositivo virtual de ESET PROTECT. Se trata de una página de configuración que le permite elegir el tipo de dispositivo y, a continuación, introducir los detalles concretos y las propiedades que resultan necesarios para que ese tipo de dispositivo virtual de ESET PROTECT concreto funcione correctamente.

El resto de la configuración y la administración se realizan desde la TUI (interfaz de usuario de texto) y Webmin:

1. Consola de administración del dispositivo virtual de ESET PROTECT: le permite realizar operaciones de mantenimiento como copia de seguridad y restauración, cambio de la contraseña, restablecimiento a valores de fábrica, etc.

2. Interfaz de administración de Webmin: facilita la administración del dispositivo virtual de ESET PROTECT.

Procedimientos de actualización, migración y recuperación ante desastres:

Actualización o migración del dispositivo virtual de ESET PROTECT: si quiere actualizar el dispositivo virtual de ESET PROTECT a la versión más reciente, consulte este apartado para acceder a información detallada y conocer el procedimiento paso a paso. Si desea migrar el dispositivo virtual de ESET PROTECT, se aplica el mismo procedimiento.

Recuperación ante desastres del dispositivo virtual de ESET PROTECT: siga este procedimiento si el dispositivo virtual de ESET PROTECT deja de funcionar y no se puede solucionar el problema o no puede recuperar una instancia dañada del dispositivo virtual de ESET PROTECT.

Descargar dispositivo virtual de ESET PROTECT

El dispositivo virtual de ESET PROTECT se proporciona en forma de archivo OVA (siglas en inglés de dispositivo de virtualización abierta). Está disponible en la sección de descargas. El dispositivo está disponible como protect_appliance.ova.

Si está implementando su dispositivo virtual en Microsoft Hyper-V, utilice `protect_appliance.vhd.zip` en lugar del archivo *OVA*.

- *protect_appliance.ova*: contiene varios tipos de dispositivo de ESET PROTECT. Implemente este archivo y elija qué tipo de dispositivo desea ejecutar. Puede elegir entre los siguientes tipos de dispositivo:
  - **ESET PROTECT Server**: ESET PROTECT Server que se ejecutará en una máquina virtual dedicada. También incluye Rogue Detection Sensor.
  - **ESET PROTECT MDM**: solo el componente de administración de dispositivos móviles. Si no desea exponer su instancia de ESET PROTECT Server, puede hacer que la máquina virtual ESET PROTECT MDM sea accesible desde Internet para poder administrar los dispositivos móviles.

El archivo *OVA* es una plantilla que contiene un sistema operativo CentOS 7 funcional. Para implementar el archivo *OVA* del dispositivo virtual de ESET PROTECT, siga las instrucciones correspondientes a su hipervisor. Cuando usa `protect_appliance.ova`, puede elegir qué tipo de dispositivo ESET PROTECT quiere que ejecute la máquina virtual tras la implementación. Una vez que haya seleccionado el tipo podrá empezar a configurar su dispositivo virtual de ESET PROTECT. Tras implementar el archivo *OVA*, seleccione el tipo de dispositivo y configure los ajustes de su dispositivo virtual. El dispositivo virtual es un entorno completo con ESET PROTECT (o uno de sus componentes).

Antes de iniciar el proceso de implementación, asegúrese de que se cumplan todos los requisitos previos.

Cuando termine el proceso de implementación y configuración, podrá conectarse a ESET PROTECT utilizando ESET PROTECT y empezar a usar ESET PROTECT.

ESET proporciona los dispositivos virtuales de ESET PROTECT, pero no es responsable de las tareas de soporte y mantenimiento de su sistema operativo ni de los componentes del mismo. Los dispositivos virtuales de ESET PROTECT están diseñados para simplificar el uso y la implementación, y están disponibles con un sistema operativo disponible al público que incluye componentes que no son de ESET. La administración y la actualización de estos componentes es responsabilidad exclusiva del usuario del dispositivo virtual de ESET PROTECT. Se recomienda actualizar el sistema operativo de forma regular para evitar problemas de seguridad.

Contraseñas del dispositivo virtual de ESET PROTECT

El dispositivo virtual de ESET PROTECT utiliza distintas cuentas de usuario. En la siguiente tabla se explican los distintos tipos de cuenta:

Tipo de cuenta	Contraseña predeterminada	Descripción y uso
Root del sistema operativo (CentOS)	`eraadmin`	Esta cuenta se puede utilizar para iniciar sesión en el dispositivo virtual de ESET PROTECT. Le permite acceder a la Consola de administración del dispositivo virtual de ESET PROTECT y a la Interfaz de administración de Webmin, le permite realizar un Restablecimiento a valores de fábrica o, si lo necesita, Recuperar la base de datos de otro servidor. Lo normal es que se le pida que introduzca la **contraseña de la máquina virtual**.
Root de la base de datos (MySQL)	`eraadmin`	Esta es una cuenta root para el servidor de bases de datos MySQL. Le permite realizar operaciones con la base de datos, como Copia de seguridad o Restauración de la base de datos. Lo normal es que se le pida que introduzca la **contraseña del usuario root de la base de datos**.
Administrador de ESET PROTECT Web Console	Se especifica durante la configuración del dispositivo virtual de ESET PROTECT	Esta contraseña resulta importante, ya que le permite acceder a ESET PROTECT Web Console.

La contraseña predeterminada se cambia durante la configuración del dispositivo virtual de ESET PROTECT. Todas las cuentas anteriores tendrán la misma contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT. Sin embargo, cada cuenta puede tener una contraseña distinta. Es más seguro utilizar contraseñas distintas, aunque el uso de varias contraseñas puede resultar más complejo. Se recomienda trazar un plan eficaz de gestión de las diversas contraseñas del dispositivo virtual de ESET PROTECT, con el fin de evitar la confusión.

> **i** Cuando implementa un dispositivo virtual de ESET PROTECT que aún no está configurado, utiliza la misma contraseña `eraadmin` para todas las para todas las cuentas anteriores, hasta que la contraseña se modifica durante la configuración del dispositivo virtual de ESET PROTECT.

En caso de olvidar la contraseña de alguna de las cuentas anteriores, consulte el capítulo Cómo recuperar una contraseña del dispositivo virtual de ESET PROTECT olvidada.

Proceso de implementación del dispositivo virtual de ESET PROTECT

Haga clic en el hipervisor que utilizará para ver las instrucciones de implementación correspondientes:

- vSphere
- VMware Workstation/Player
- Microsoft Hyper-V

- Oracle VirtualBox
- Citrix

vSphere

Implementación de ESET PROTECT VA en vSphere Client

1. Conéctese a su instancia de vCenter Server con vSphere Client o directamente al servidor ESXi.

2. Si utiliza vSphere Client para escritorio, haga clic en **Archivo** > **Implementar plantilla OVF**. Si utiliza vSphere Web Client, haga clic en **Acciones** > **Implementar plantilla OVF**.

3. Haga clic en **Examinar**, diríjase al archivo *protect_appliance.ova* que ha descargado de ESET.com y, a continuación, haga clic en **Abrir**.

Las versiones no compatibles de VMware ESXi no aceptan certificados de SHA-256. Si ve un error de certificado al importar el paquete de *.ova* del dispositivo virtual de ESET PROTECT 9.0, tiene que eliminar el archivo de *.cert* de *.ova* y después continuar con la implementación.

4. Haga clic en **Siguiente** en la ventana Detalles de la plantilla OVF.

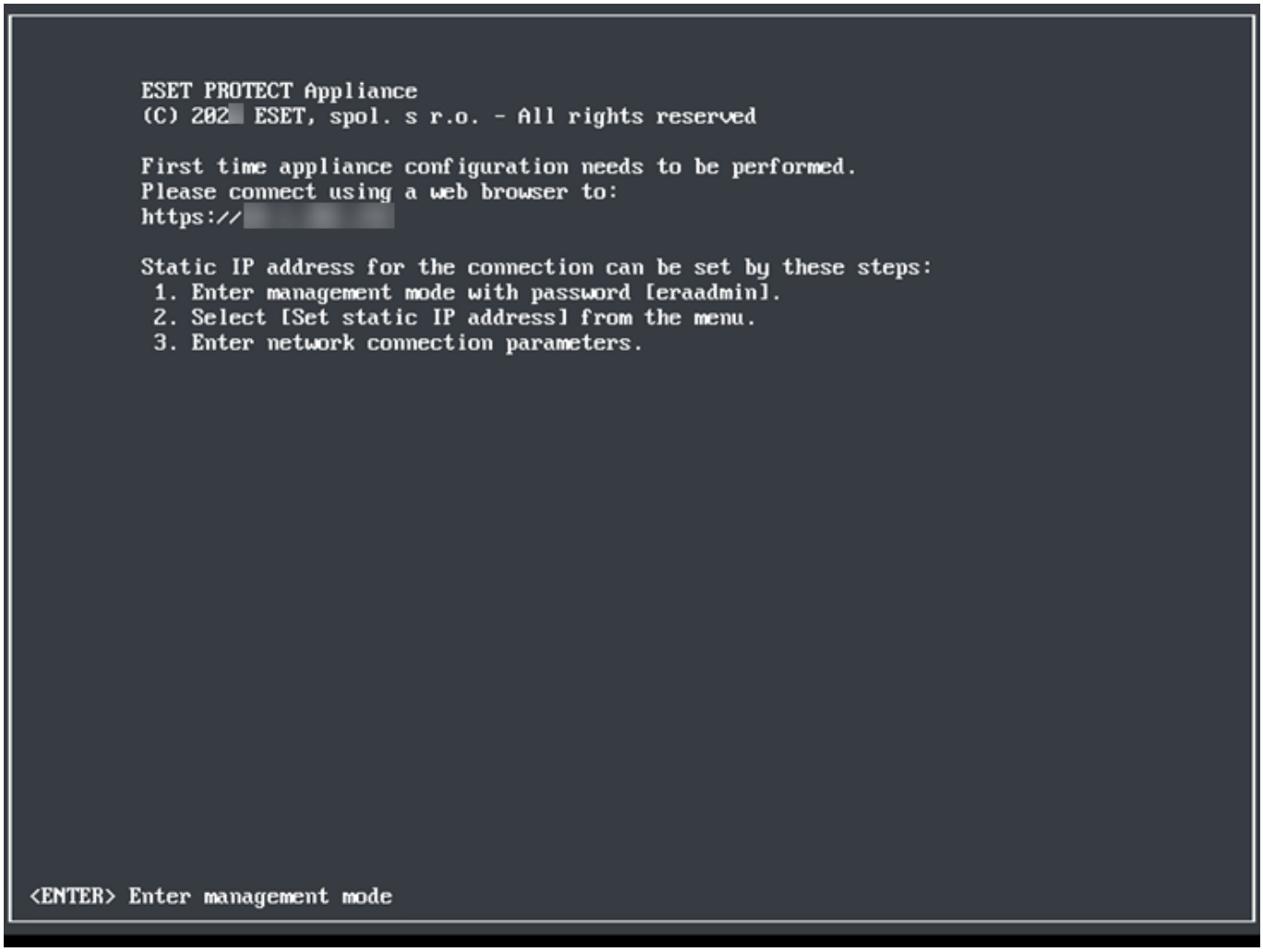
5. Lea y acepte el Acuerdo de licencia de usuario final (EULA).

6. Siga las instrucciones en pantalla para completar la instalación y especifique la siguiente información acerca del cliente virtual:

- **Nombre y ubicación**: especifique el nombre de la plantilla implementada y la ubicación en la que están almacenados los archivos de la máquina virtual.
- **Host/Clúster**: seleccione el host o clúster en el que quiere ejecutar la plantilla.
- **Grupo de recursos**: seleccione el grupo de recursos en el que quiere implementar la plantilla.
- **Almacenamiento**: seleccione una ubicación en la que almacenar los archivos de la máquina virtual.
- **Formato de disco**: seleccione el formato que emplearán los discos virtuales.
- **Asignación de red**: seleccione la red que desea que utilice la máquina virtual. Asegúrese de seleccionar la red de la máquina virtual asociada al grupo de IP que ha creado.

7. Haga clic en **Siguiente**, revise el resumen de implementación y haga clic en **Finalizar**. El proceso creará automáticamente una máquina virtual con la configuración que ha especificado.

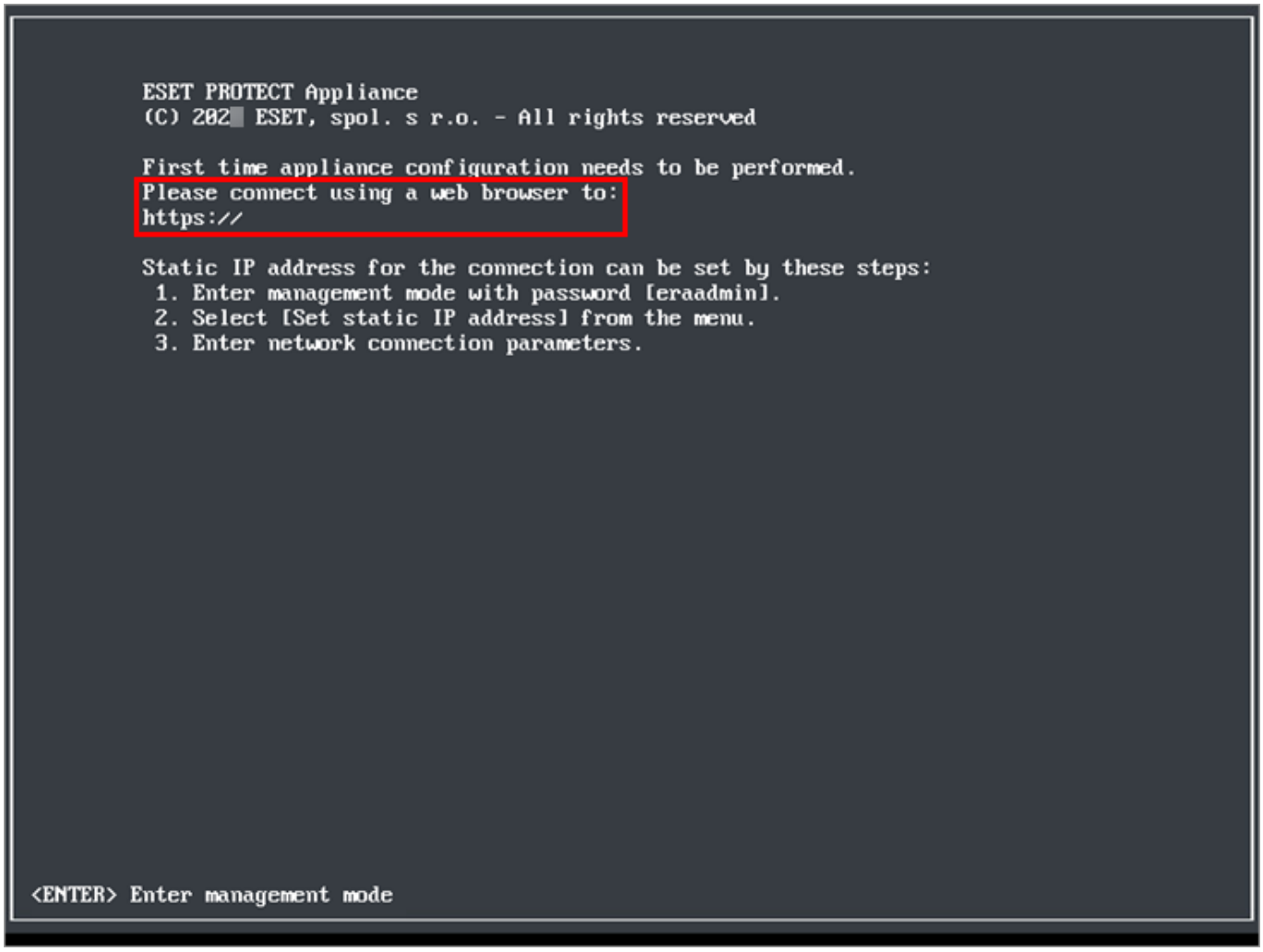
8. Cuando el dispositivo virtual de ESET PROTECT esté correctamente implementado, enciéndalo. Se mostrará la siguiente información:



Abra su navegador web y especifique en la barra de direcciones la dirección IP del dispositivo de ESET PROTECT que acaba de implementar. Podrá ver que la dirección IP aparece en la ventana de la consola (como se muestra anteriormente). Dirá "**Se debe realizar la primera configuración del dispositivo. Utilice un navegador web para visitar:***https://[IP address]*".

El próximo paso es configurar su dispositivo a través de la interfaz web.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT desde la Consola de administración. Si no hay ninguna dirección IP asignada, se mostrará la siguiente información y la URL no contendrá una dirección IP.
Si no hay ninguna dirección IP asignada, puede que el servidor DHCP no pueda asignar una. Asegúrese de que haya direcciones IP disponibles en la subred en la que se encuentra el dispositivo virtual.



Le recomendamos encarecidamente que configure las funciones y permisos de vCenter de forma que los usuarios de VMware no tengan acceso a la máquina virtual de ESET PROTECT. De esta forma se evitará que los usuarios manipulen la máquina virtual de ESET PROTECT. No es necesario que los usuarios de ESET PROTECT accedan a la máquina virtual. Para administrar el acceso a ESET PROTECT, utilice Derechos de acceso en ESET PROTECT Web Console.

VMware Workstation/Player

Implementación de ESET PROTECT VA en VMware Workstation/Player

Se recomienda usar la versión más reciente de VMware Player. Configure la conexión del adaptador de red de la máquina virtual en **Puente** o **NAT**.

Para que pueda accederse a ESET PROTECT desde la red, en la máquina virtual debe estar configurado el reenvío de puertos.

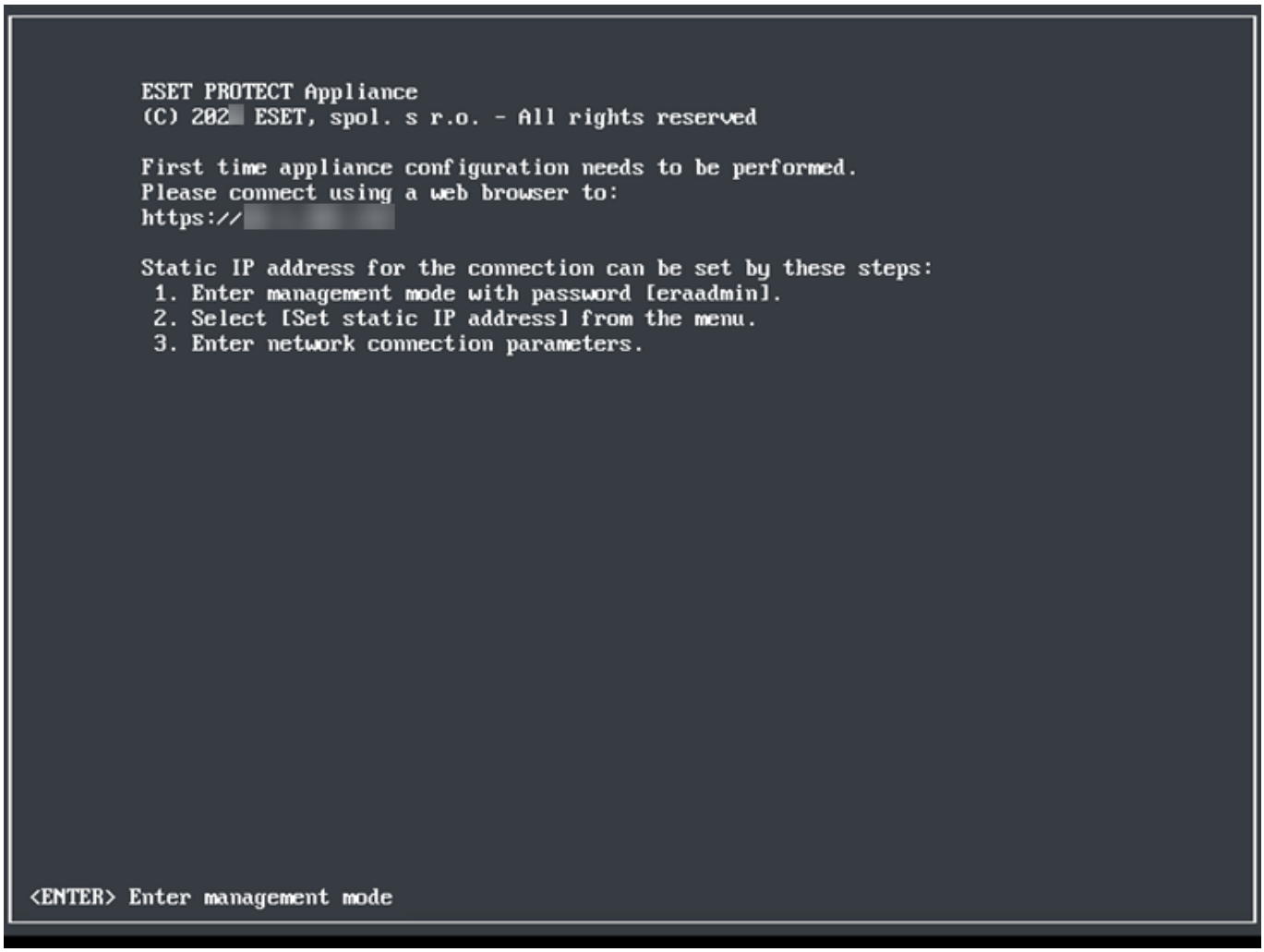
1. Seleccione **Archivo** > **Implementar plantilla OVF**.

2. Diríjase al archivo *protect_appliance.ova* que ha descargado del sitio web de ESET y haga clic en **Abrir**.

3. Indique el nombre y la ruta de acceso de almacenamiento local de la nueva máquina virtual, y haga clic en **Importar**.

4. Lea y acepte el Acuerdo de licencia de usuario final (EULA), si está de acuerdo con él.

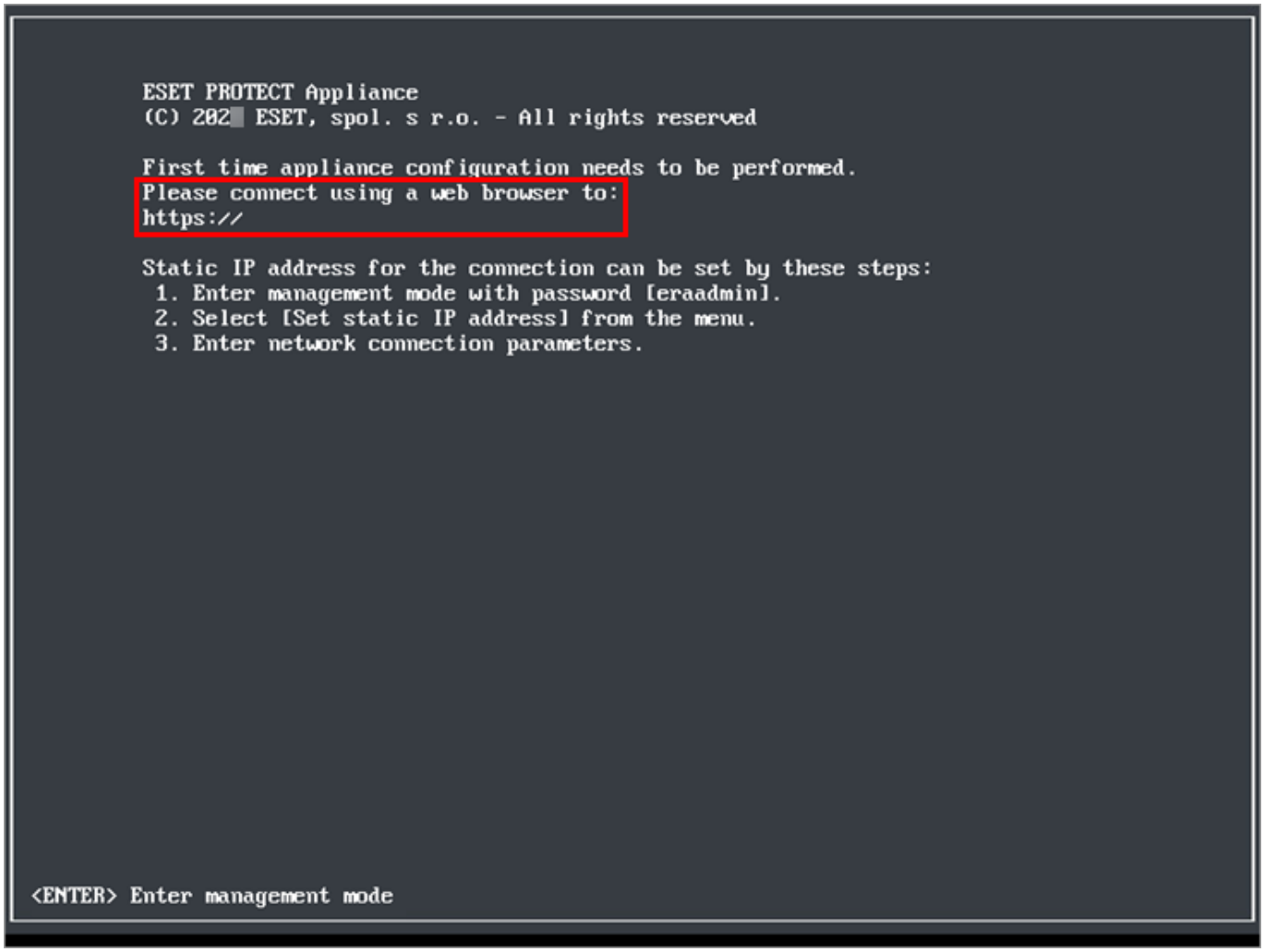
5. Cuando el dispositivo esté implementado, enciéndalo. Se mostrará la siguiente información:



Abra su navegador web y especifique en la barra de direcciones la dirección IP del dispositivo de ESET PROTECT que acaba de implementar. Podrá ver que la dirección IP aparece en la ventana de la consola (como se muestra anteriormente). Dirá "**Se debe realizar la primera configuración del dispositivo. Utilice un navegador web para visitar:***https://[IP address]*".

El próximo paso es configurar su dispositivo a través de la interfaz web.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT desde la Consola de administración. Si no hay ninguna dirección IP asignada, se mostrará la siguiente información y la URL no contendrá una dirección IP.
Si no hay ninguna dirección IP asignada, puede que el servidor DHCP no pueda asignar una. Asegúrese de que haya direcciones IP disponibles en la subred en la que se encuentra el dispositivo virtual.



Microsoft Hyper-V

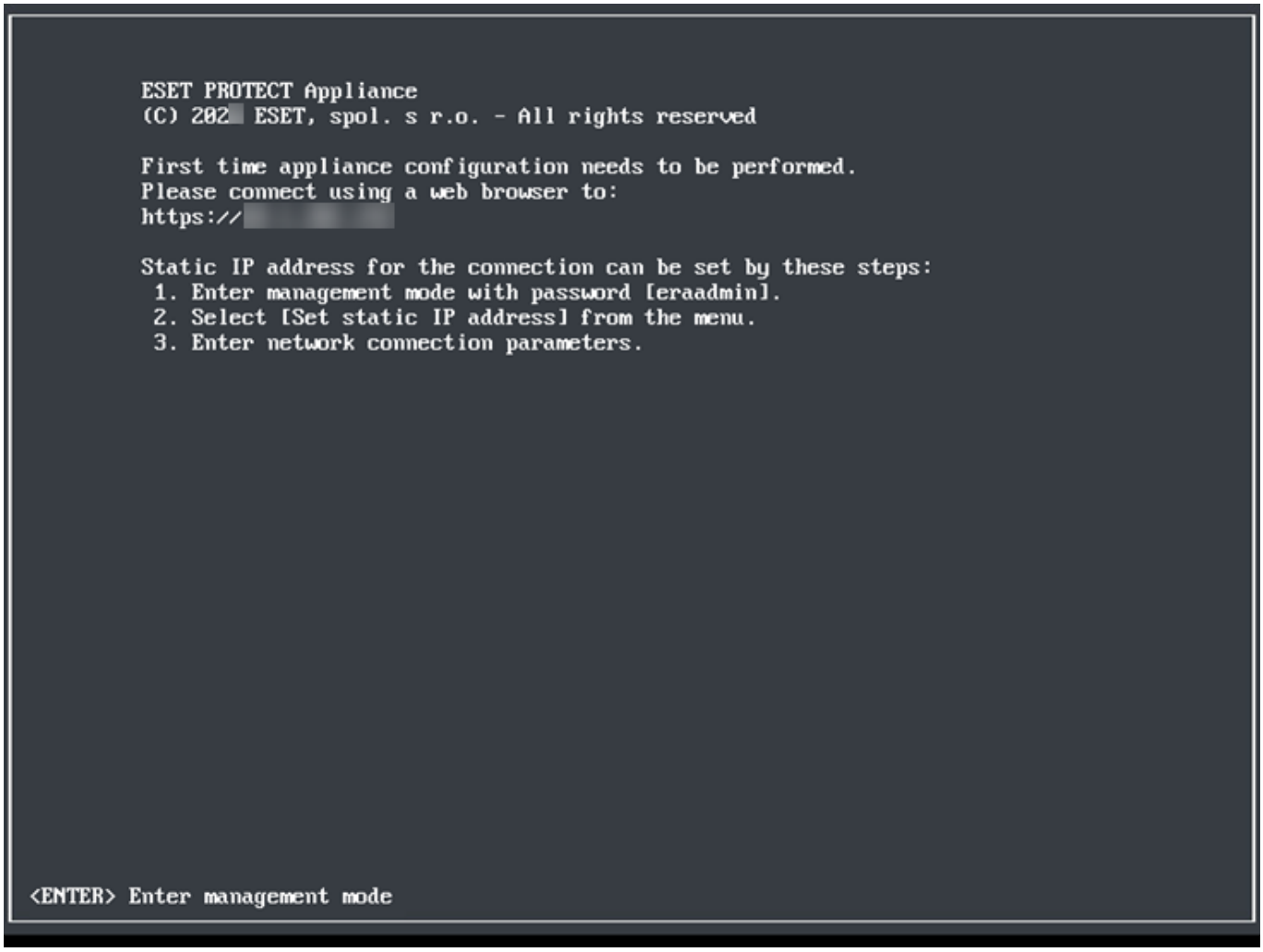
Implementación del dispositivo virtual de ESET PROTECT en Microsoft Hyper-V

1. Extraiga el archivo `protect_appliance.vhd.zip` (descargado de ESET.com) con una utilidad como, por ejemplo, Tar o 7-Zip.

2. Abra el Administrador de Hyper-V y conéctese al Hyper-V correspondiente.

3. Cree una **nueva** máquina virtual (Generación 1) con un mínimo de 4 núcleos y 4 GB de RAM.

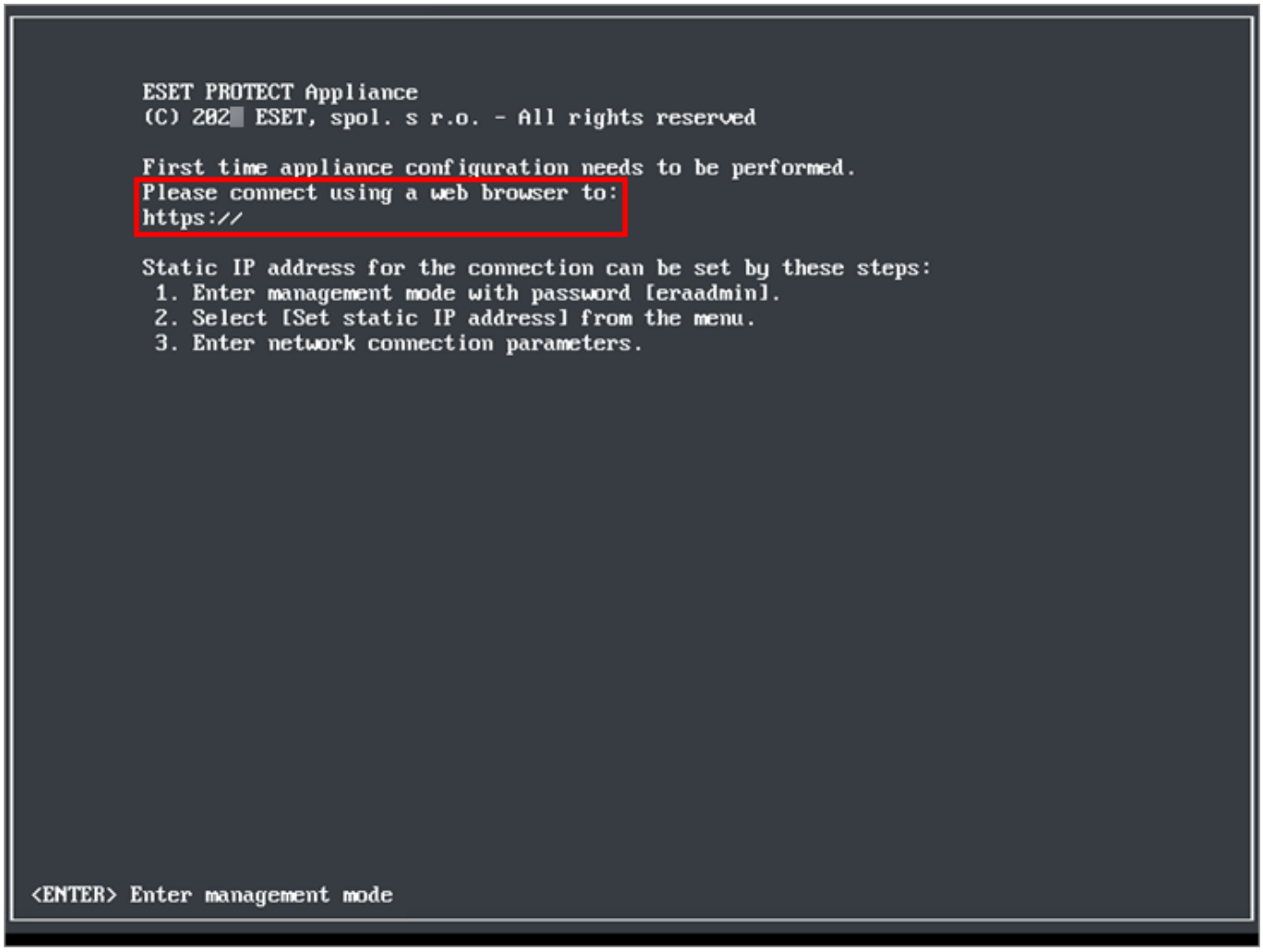
4. Cuando se haya creado correctamente la máquina virtual, enciéndala. Se mostrará la siguiente información:



Abra su navegador web y especifique en la barra de direcciones la dirección IP del dispositivo de ESET PROTECT que acaba de implementar. Podrá ver que la dirección IP aparece en la ventana de la consola (como se muestra anteriormente). Dirá "**Se debe realizar la primera configuración del dispositivo. Utilice un navegador web para visitar:***https://[IP address]*".

El próximo paso es configurar su dispositivo a través de la interfaz web.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT desde la Consola de administración. Si no hay ninguna dirección IP asignada, se mostrará la siguiente información y la URL no contendrá una dirección IP.
Si no hay ninguna dirección IP asignada, puede que el servidor DHCP no pueda asignar una. Asegúrese de que haya direcciones IP disponibles en la subred en la que se encuentra el dispositivo virtual.



Oracle VirtualBox

Implementación del dispositivo virtual de ESET PROTECT en VirtualBox

Se recomienda usar la versión más reciente de VirtualBox. Configure la conexión del adaptador de red de la máquina virtual en **Bridged** o **NAT**.

> Para que pueda accederse a ESET PROTECT desde Internet, en la máquina virtual debe estar configurado el reenvío de puertos (en caso de ser necesario).

1. Haga clic en **File** y seleccione **Import Appliance**.

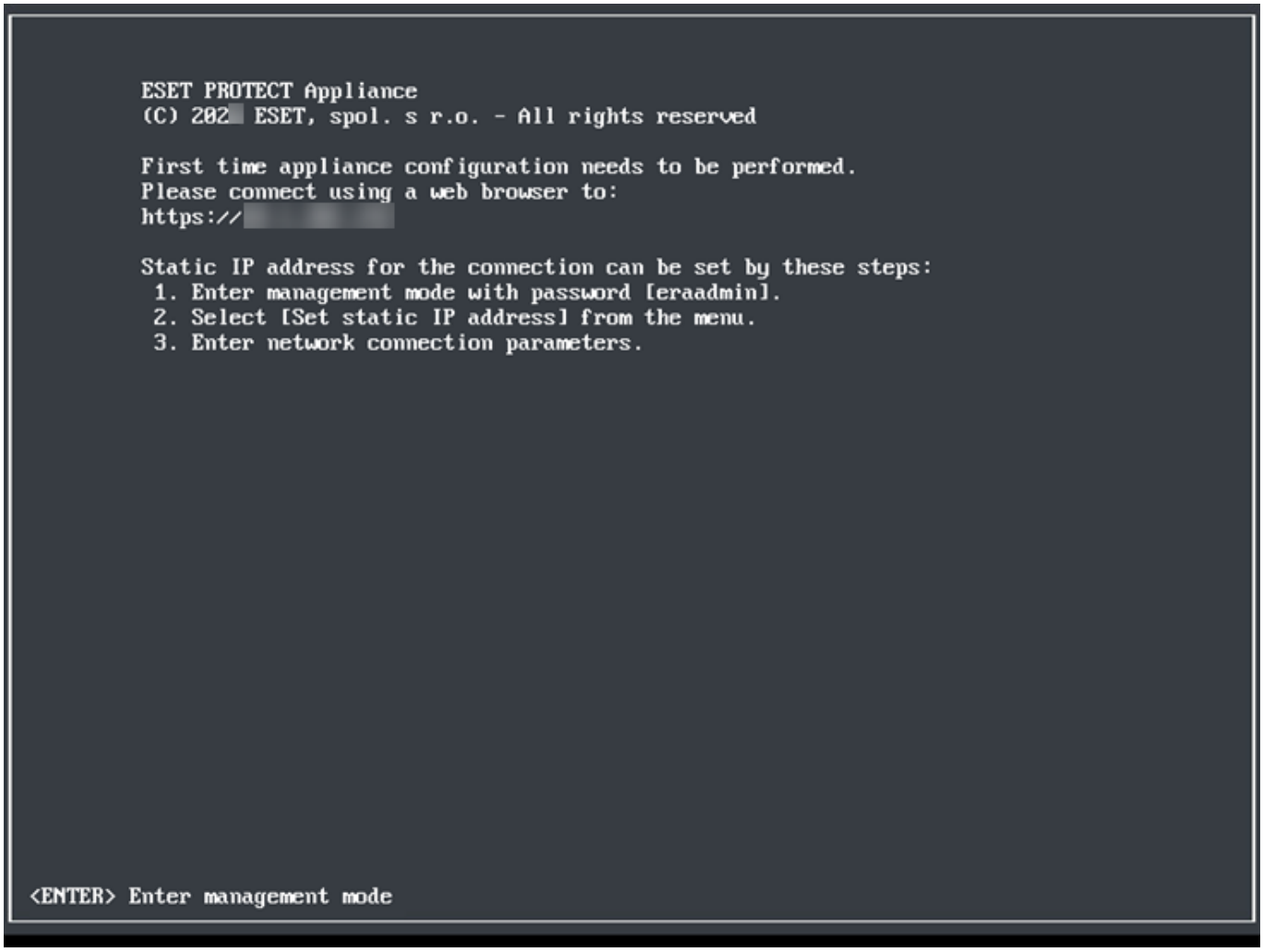
2. Haga clic en **Browse**, diríjase al archivo *protect_appliance.ova* que descargó de ESET.com y haga clic en **Open**.

3. Haga clic en **Next**

4. Revise la configuración de su dispositivo y haga clic en **Import**.

5. Lea y acepte el Acuerdo de licencia de usuario final (EULA), si está de acuerdo con él.

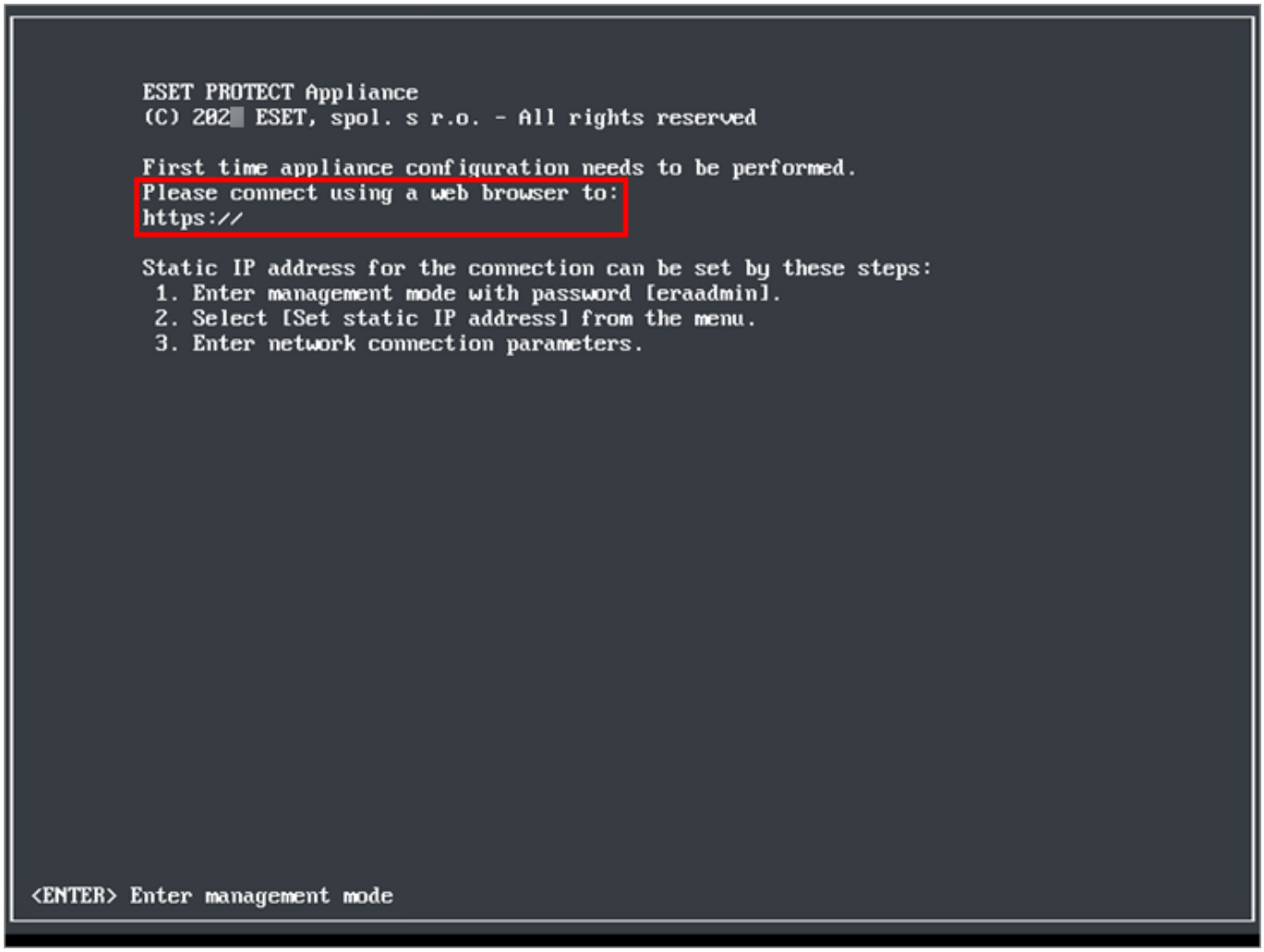
6. Cuando el dispositivo virtual de ESET PROTECT esté correctamente implementado, enciéndalo. Se mostrará la siguiente información:



Abra su navegador web y especifique en la barra de direcciones la dirección IP del dispositivo de ESET PROTECT que acaba de implementar. Podrá ver que la dirección IP aparece en la ventana de la consola (como se muestra anteriormente). Dirá "**Se debe realizar la primera configuración del dispositivo. Utilice un navegador web para visitar:***https://[IP address]*".

El próximo paso es configurar su dispositivo a través de la interfaz web.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT desde la Consola de administración. Si no hay ninguna dirección IP asignada, se mostrará la siguiente información y la URL no contendrá una dirección IP.
Si no hay ninguna dirección IP asignada, puede que el servidor DHCP no pueda asignar una. Asegúrese de que haya direcciones IP disponibles en la subred en la que se encuentra el dispositivo virtual.



Citrix

Implementación del dispositivo virtual de ESET PROTECT en Citrix:

Requisitos previos

- Su red IPv4 está disponible en el entorno Citrix. IPv6 no es compatible con el dispositivo virtual de ESET PROTECT.
- El archivo *.ovf* del dispositivo está disponible en la máquina en la que va a implementar el dispositivo virtual de ESET PROTECT.
- Se necesitan permisos de administración del grupo para importar el paquete *OVF/OVA*.
- Debe haber suficiente espacio de almacenamiento disponible para el usuario que va a realizar la implementación, 100 GB como mínimo.

Proceso de implementación

1.Seleccione **File** > **Import**.

2.Haga clic en **Browse**, diríjase al archivo *protect_appliance.ova* que descargó del sitio web de ESET y haga clic en **Next**.

3.Seleccione la casilla de verificación **I accept the End User License Agreements** y haga clic en **Next**.

4.Seleccione el servidor de grupo o independiente en el que desee colocar el dispositivo virtual de ESET PROTECT y haga clic en **Next**.

5.Coloque el disco virtual importado en un repositorio de almacenamiento y haga clic en **Next**.

6.Asigne las interfaces de red virtuales seleccionando la **Target Network** y haga clic en **Next**.

7.Seleccione verificar la firma digital (opcional) y haga clic en **Next**.

8.Seleccione **Don't use Operating System Fixup** y haga clic en **Next**.

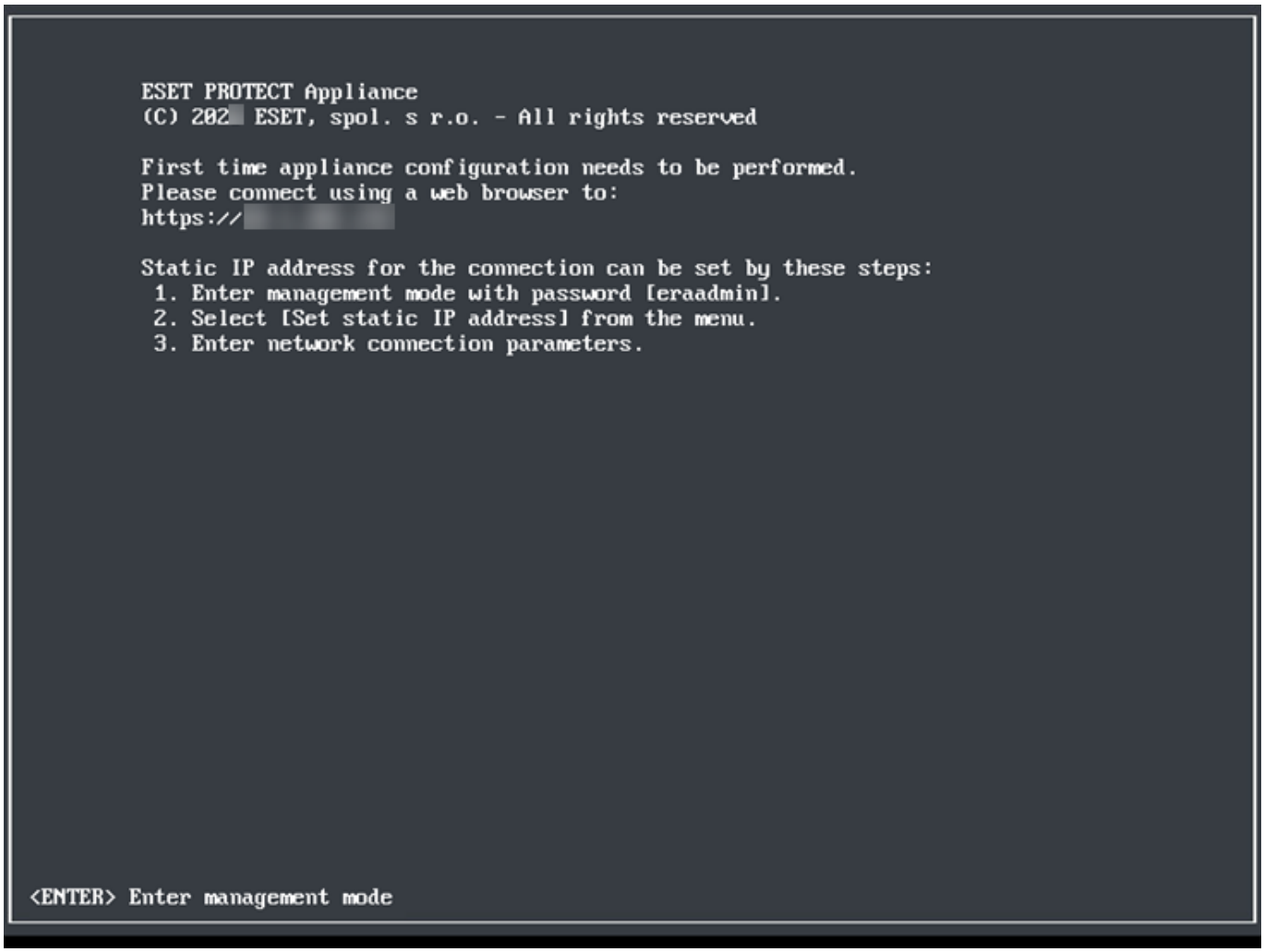
9.Seleccione la red (la misma que seleccionó en el paso 6) en la que vaya a instalar el dispositivo virtual de ESET PROTECT temporal utilizado para realizar la operación de importación y haga clic en **Next**.

10. Revise la configuración y haga clic en **Finish**.

El proceso de implementación puede llevar algún tiempo, durante el que el servidor Citrix estará inactivo. No interrumpa el proceso.

Consulte la documentación del proveedor sobre implementación de *OVF/OVA*.

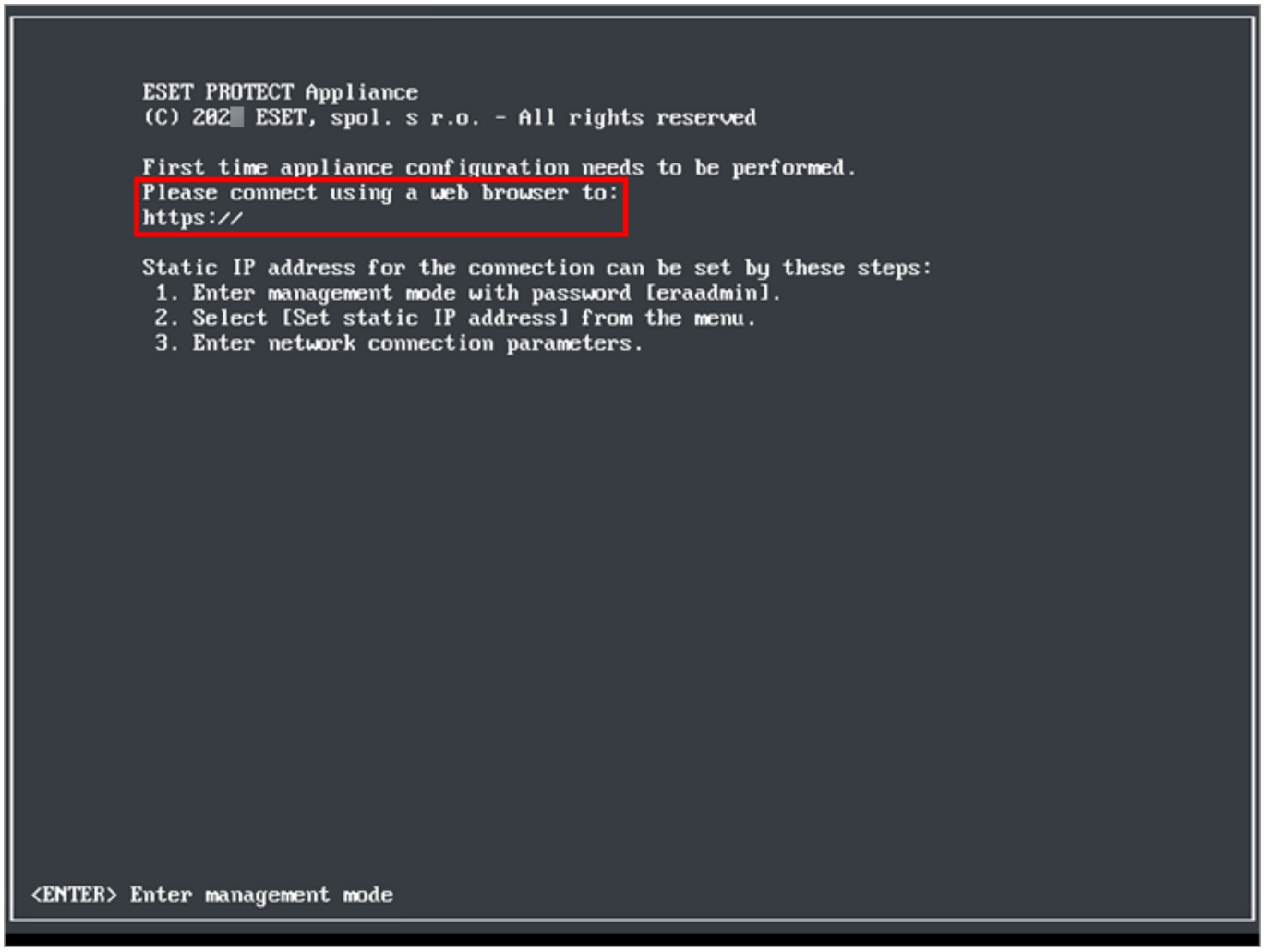
Cuando se haya creado correctamente la máquina virtual, enciéndala. Se mostrará la siguiente información:



Abra su navegador web y especifique en la barra de direcciones la dirección IP del dispositivo de ESET PROTECT que acaba de implementar. Podrá ver que la dirección IP aparece en la ventana de la consola (como se muestra anteriormente). Dirá "**Se debe realizar la primera configuración del dispositivo. Utilice un navegador web para visitar:***https://[IP address]*".

El próximo paso es configurar su dispositivo a través de la interfaz web.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT desde la Consola de administración. Si no hay ninguna dirección IP asignada, se mostrará la siguiente información y la URL no contendrá una dirección IP.
Si no hay ninguna dirección IP asignada, puede que el servidor DHCP no pueda asignar una. Asegúrese de que haya direcciones IP disponibles en la subred en la que se encuentra el dispositivo virtual.



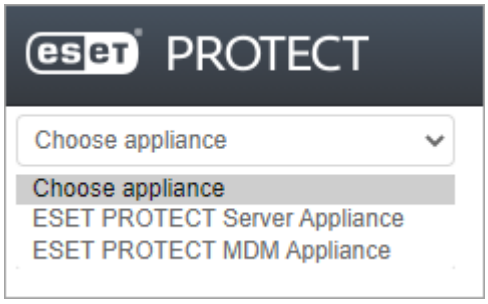
Configuración del dispositivo virtual de ESET PROTECT

El dispositivo virtual de ESET PROTECT (ESET PROTECT VA) puede configurarse fácilmente a través de su interfaz web. Tendrá que contar con un servidor DHCP en su red, para que el dispositivo virtual de ESET PROTECT reciba automáticamente una dirección IP que, a su vez, le permitirá acceder a la interfaz web de configuración del dispositivo virtual de ESET PROTECT.

Si no dispone de un servidor DHCP en su red, tendrá que Configurar la dirección IP estática del dispositivo virtual de ESET PROTECT.

Una vez que haya implementado su máquina virtual de dispositivo virtual de ESET PROTECT, elija qué **tipo de dispositivo de ESET PROTECT** desea ejecutar. En el navegador web, elija en el menú desplegable el tipo de dispositivo de ESET PROTECT desde el que desea ejecutar su máquina virtual y configúrelo. Haga clic a continuación en el enlace correspondiente para acceder a las instrucciones de configuración de los distintos tipos de dispositivo:

- Dispositivo ESET PROTECT Server
- Dispositivo ESET PROTECT MDM



Dispositivo ESET PROTECT Server

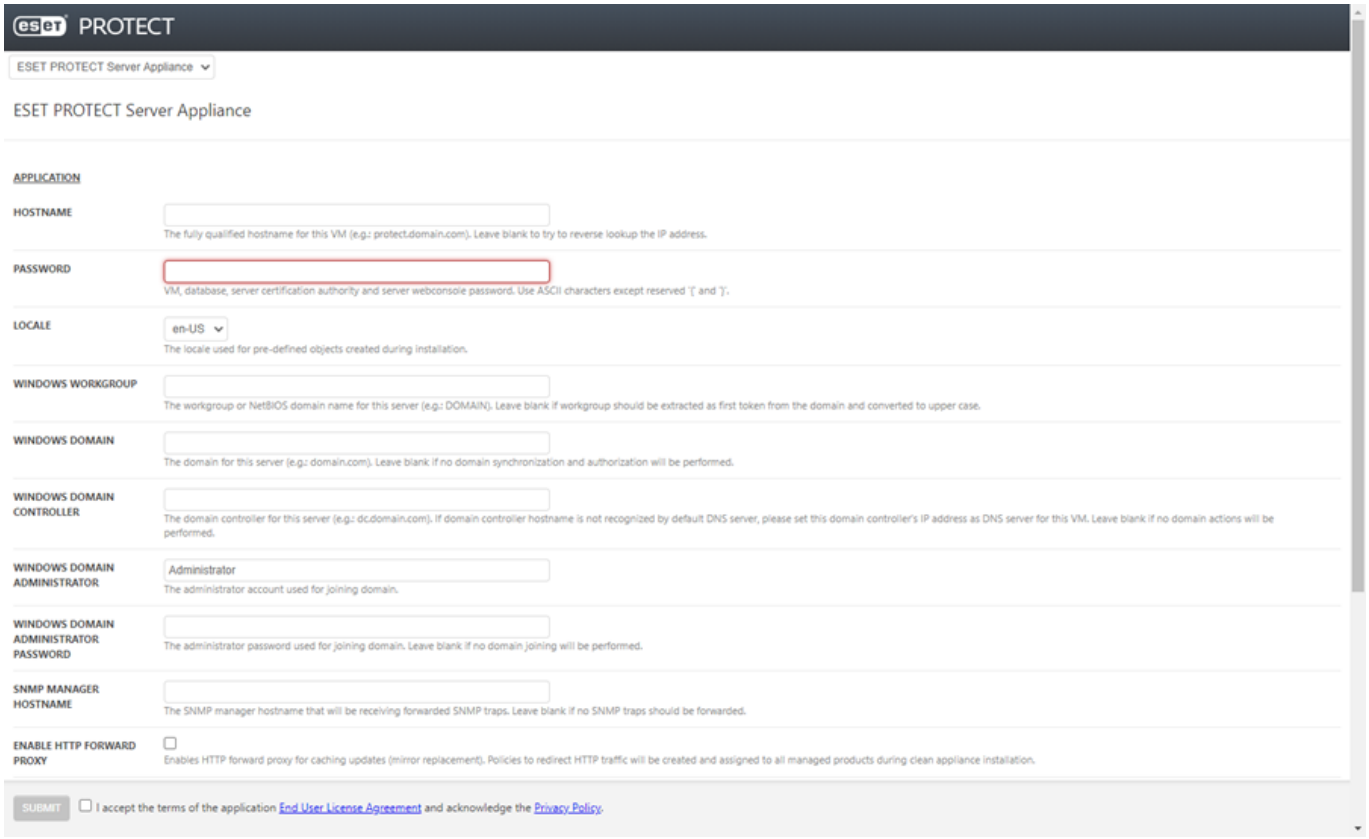
Esta es la página de configuración del dispositivo ESET PROTECT Server. Está dividida en dos secciones, **Aplicación** y **Propiedades de la red**. Cumplimente todos los campos obligatorios (marcados en color rojo). En caso de ser necesario, puede especificar parámetros de configuración opcionales.

Este tipo de dispositivo virtual de ESET PROTECT ejecuta ESET PROTECT Server en una máquina virtual dedicada. Esta configuración está recomendada para redes de pequeñas y grandes empresas.

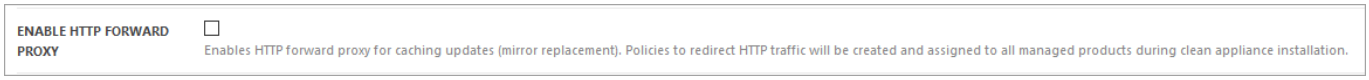
Campos de configuración obligatorios del dispositivo ESET PROTECT Server:

- **Password**: esta contraseña es importante porque se utilizará en la máquina virtual, en la base de datos de ESET PROTECT, en la autoridad certificadora de ESET PROTECT Server y en ESET PROTECT Web Console.

El usuario predeterminado de Web Console es **Administrator**.



A pesar de no ser obligatorio, se recomienda que especifique parámetros opcionales, Como por ejemplo Detalles de dominio, Detalles de DC, credenciales de la cuenta del Administrador del dominio, etc. Esta opción resulta útil para acciones relacionadas con dominios, como es el caso de la sincronización.



Ver la imagen más grande

También puede habilitar el proxy HTTP Apache para almacenar las actualizaciones en la caché. Seleccione la casilla situada junto a **Enable HTTP forward proxy** para instalar el proxy HTTP Apache y cree y aplique políticas (con el nombre **Uso de proxy HTTP**, aplicadas al grupo **Todos**) para los siguientes productos:

- ESET Endpoint para Windows
- ESET Endpoint para macOS (OS X) y Linux
- ESET Management Agent
- ESET File Security para Windows Server (6+)
- ESET Server Security para Windows (8 o posterior)
- Caché local compartida de ESET

- La política activa el proxy HTTP para los productos aplicables. Con la configuración predeterminada, el host del proxy se configura en la dirección IP local del servidor de ESET PROTECT en el puerto 3128. La autenticación se desactiva. Puede copiar esta configuración en otras políticas para configurar otros productos.

- El uso del proxy HTTP puede ahorrar gran cantidad de ancho de banda en los datos descargados de Internet

y mejorar las velocidades de descarga de las actualizaciones del producto. Le recomendamos que marque la casilla de verificación situada junto a **Proxy HTTP Apache** si va a administrar más de 37 ordenadores desde ESET PROTECT.

- Puede instalar el proxy HTTP Apache más tarde si lo desea. Para obtener más información, consulte las Preguntas más frecuentes sobre el dispositivo virtual de ESET PROTECT.

Propiedades de red

Desplácese hacia abajo para configurar las siguientes propiedades de red: **Dirección IP de la red**, **Máscara de red**, **Puerta de enlace predeterminada**, **DNS1**, **DNS2**. Todos los campos son opcionales.

Unir el dispositivo virtual de ESET PROTECT al dominio

Puede configurar el dispositivo virtual de ESET PROTECT para que se ejecute en un dominio durante la configuración inicial. Para poder usar ESET PROTECT VA en un dominio son obligatorios los siguientes ajustes:

Windows workgroup: un nombre de dominio de NETBIOS o grupo de trabajo para este servidor, por ejemplo, DOMAIN.

Windows domain: un dominio para este servidor, por ejemplo, *domain.com*.

Windows domain controller: un controlador de dominio para este servidor. Introduzca el nombre de dominio completo (FQDN) del controlador de dominio.

Windows domain administrator: una cuenta utilizada para unirse al dominio.

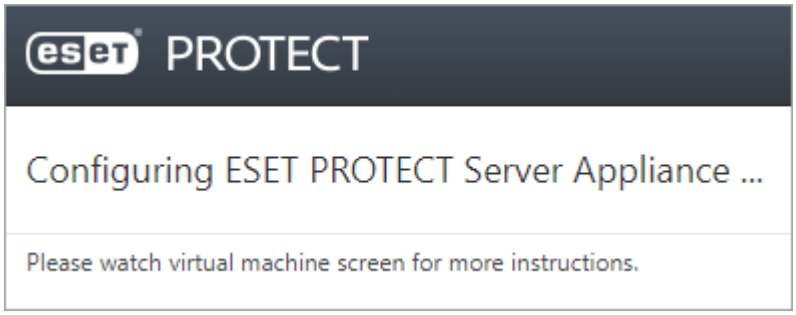
Windows domain administrator password: una contraseña de administrador utilizada para unirse al dominio.

DNS1: un servidor de nombres de dominio para esta máquina virtual. Escriba la dirección IP del controlador de dominio.

Revise los parámetros de configuración especificados. Asegúrese de que la configuración sea correcta, ya que no es posible realizar cambios de configuración adicionales.

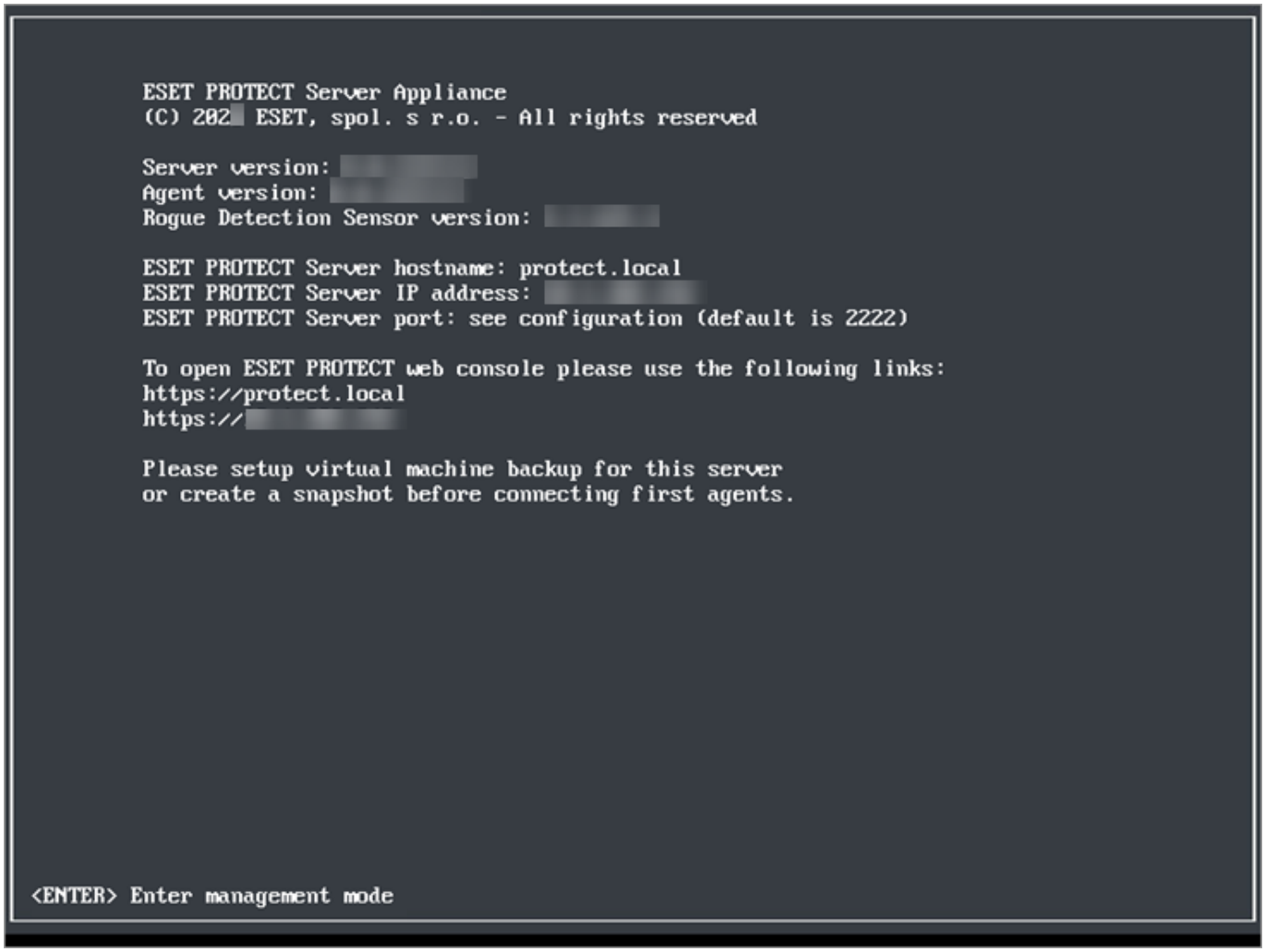
Marque la casilla **Acepto los términos del Contrato de licencia para el usuario final y la Política de privacidad de la aplicación**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET para obtener más información.

Cuando haga clic en **Submit** se mostrará la siguiente información:



No actualice esta página en el navegador web, cierre la pestaña y acceda a la ventana de la consola del dispositivo virtual de ESET PROTECT.

En la ventana de la consola del dispositivo virtual de ESET PROTECT se mostrará su información de estado. Se mostrarán las versiones del componente de ESET PROTECT, así como el nombre de host, la dirección IP y el número de puerto de ESET PROTECT Server. La dirección de la Consola web de ESET PROTECT también se mostrará en el siguiente formato: *https:///[hostname] and https:///[IP address]*.



Se recomienda crear una instantánea o hacer una copia de seguridad de la máquina virtual antes de implementar y conectar los primeros agentes de ESET Management.

Introduzca en su navegador la dirección de ESET PROTECT Web Console (como se muestra anteriormente) e inicie sesión en ESET PROTECT Web Console. Lo más probable es que su nombre de host y dirección IP sean distintos, los mostrados anteriormente se incluyen a título únicamente ilustrativo. Una vez que haya iniciado sesión podrá empezar a usar ESET PROTECT.

Tras el primer inicio de sesión en la Consola web de ESET PROTECT, recomendamos ejecutar la tarea del cliente Actualización del sistema operativo en el ordenador en el que está instalado ESET PROTECT.

ESET PROTECTDispositivo MDM

Esta es la página de configuración del dispositivo ESET PROTECT MDM. La configuración está dividida en dos secciones, **Aplicación** y **Propiedades de la red**. Rellene todos los campos obligatorios (marcados en color rojo). En caso de ser necesario, puede especificar otros parámetros de configuración opcionales.

Este tipo de dispositivo virtual de ESET PROTECT ejecuta el dispositivo ESET PROTECT MDM en una máquina virtual dedicada. Adecuado para redes de grandes empresas, pero también puede utilizarse para pequeñas empresas.

Antes de empezar a configurar el dispositivo ESET PROTECT MDM, cree un certificado de Mobile Device Connector en la Consola web del servidor de ESET PROTECT que se conectará a su dispositivo ESET PROTECT MDM.

Puede configurar ESET PROTECT MDM de dos formas:

1.**Configuración con credenciales de Consola web**

Campos de configuración obligatorios del dispositivo ESET PROTECT MDM:

- **Password**: esta contraseña es importante, ya que se utilizará en la base de datos de ESET PROTECT y en la máquina virtual.
- **ESET PROTECT Server Hostname**: escriba el nombre de host o la dirección IP de ESET PROTECT Server para que ESET PROTECT MDM pueda conectarse a ESET PROTECT Server.
- **ESET PROTECT Server Port**: el puerto predeterminado de ESET PROTECT Server es el 2222, si utiliza un puerto diferente, cambie el puerto predeterminado por su número de puerto personalizado.
- **Web Console Port**: el puerto predeterminado de Web Console es el 2223; si utiliza un puerto diferente, cambie el puerto predeterminado por su número de puerto personalizado.
- **Contraseña de Consola web**: esta contraseña es importante porque la necesita para acceder a la Consola web de ESET PROTECT.
- Opcionalmente, puede introducir el **Nombre de host** de la **Consola web**. La Consola web utiliza este nombre de host para conectarse al servidor. Si deja vacío el campo, el valor se copiará automáticamente del **Nombre de host del servidor de ESET PROTECT**.
- **Nombre de host MDM**: escriba el FQDN o la dirección IP de MDM (como se especifica en el certificado de MDC que creó en ESET PROTECT Web Console).

2.**Configuración con uso de certificados**

Campos de configuración obligatorios del dispositivo ESET PROTECT MDM:

- **Password**: esta contraseña es importante, ya que se utilizará en la base de datos de ESET PROTECT y en la máquina virtual.
- **ESET PROTECT Server Hostname**: escriba el nombre de host o la dirección IP de ESET PROTECT Server para que ESET PROTECT MDM pueda conectarse a ESET PROTECT Server.
- **ESET PROTECT Server Port**: el puerto predeterminado de ESET PROTECT Server es el 2222, si utiliza un puerto diferente, cambie el puerto predeterminado por su número de puerto personalizado.
- **Web Console Port**: el puerto predeterminado de Web Console es el 2223; si utiliza un puerto diferente, cambie el puerto predeterminado por su número de puerto personalizado.
- **Autoridad de certificación Base64**: pegue el certificado de la autoridad de certificación en formato Base64

(consulte Certificados de ESET PROTECT para obtener información detallada sobre cómo obtener el certificado).

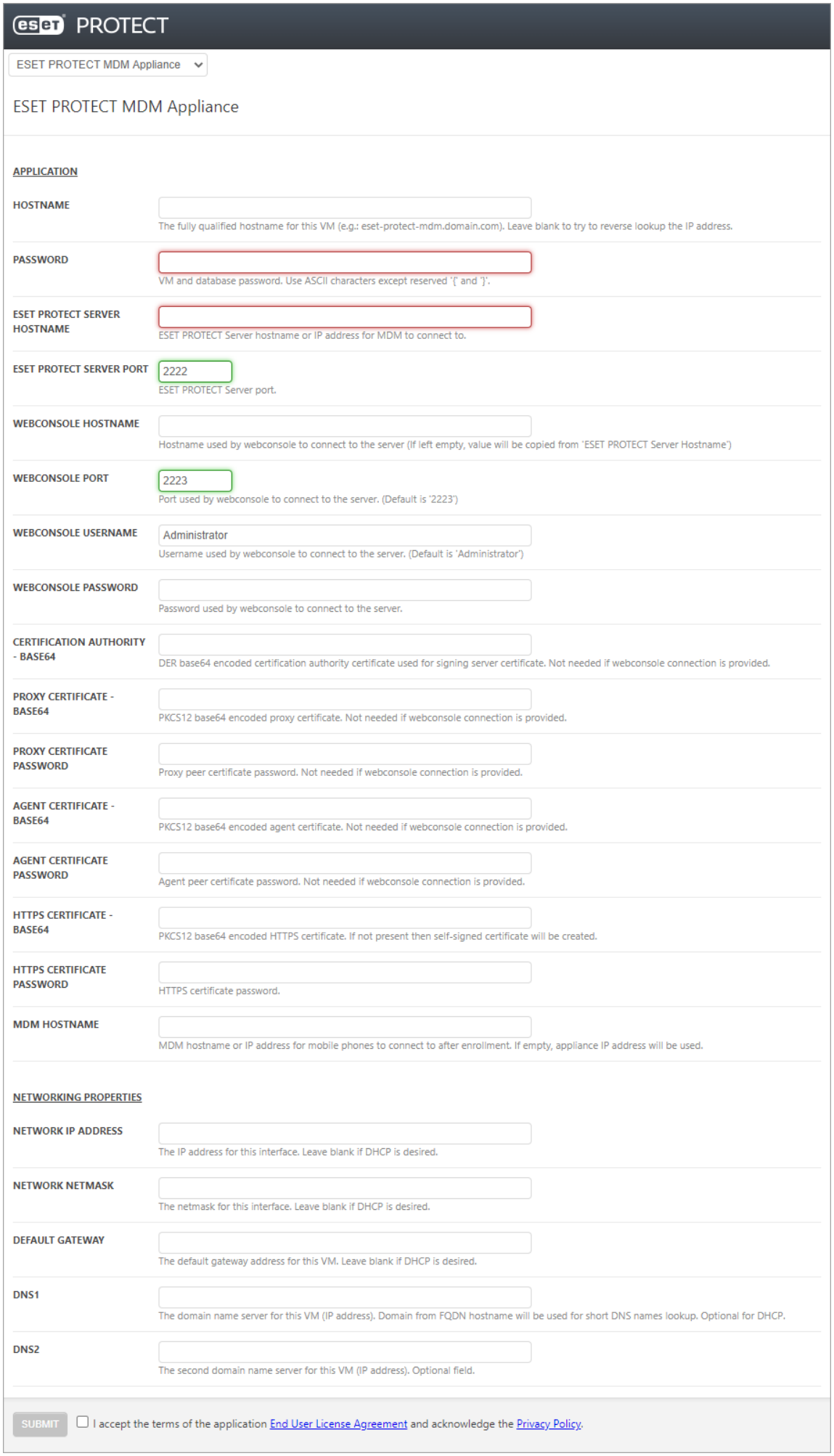
- **Certificado de proxy Base64**: pegue el certificado del proxy en formato Base64 (consulte Certificados de ESET PROTECT para obtener información detallada sobre cómo obtener el certificado). Para autenticar la comunicación entre ESET PROTECT Server y MDM, se utiliza un certificado de proxy.

- **Certificado de agente Base64**: pegue el certificado del agente en formato Base64 (consulte Certificados de ESET PROTECT para obtener información detallada sobre cómo obtener el certificado).

- **Nombre de host MDM**: escriba el FQDN o la dirección IP de MDM (como se especifica en el certificado de MDC que creó en ESET PROTECT Web Console).

Propiedades de red

Desplácese hacia abajo para configurar las siguientes propiedades de red: **Dirección IP de la red**, **Máscara de red**, **Puerta de enlace predeterminada**, **DNS1**, **DNS2**. Todos los campos son opcionales.


PROTECT
ESET PROTECT MDM Appliance
ESET PROTECT MDM Appliance
APPLICATION
HOSTNAME
The fully qualified hostname for this VM (e.g.: eset-protect-mdm.domain.com). Leave blank to try to reverse lookup the IP address.
PASSWORD
VM and database password. Use ASCII characters except reserved '{' and '}'.
ESET PROTECT SERVER HOSTNAME
ESET PROTECT Server hostname or IP address for MDM to connect to.
ESET PROTECT SERVER PORT
2222
ESET PROTECT Server port.
WEBCONSOLE HOSTNAME
Hostname used by webconsole to connect to the server (If left empty, value will be copied from 'ESET PROTECT Server Hostname')
WEBCONSOLE PORT
2223
Port used by webconsole to connect to the server. (Default is '2223')
WEBCONSOLE USERNAME
Administrator
Username used by webconsole to connect to the server. (Default is 'Administrator')
WEBCONSOLE PASSWORD
Password used by webconsole to connect to the server.
CERTIFICATION AUTHORITY - BASE64
DER base64 encoded certification authority certificate used for signing server certificate. Not needed if webconsole connection is provided.
PROXY CERTIFICATE - BASE64
PKCS12 base64 encoded proxy certificate. Not needed if webconsole connection is provided.
PROXY CERTIFICATE PASSWORD
Proxy peer certificate password. Not needed if webconsole connection is provided.
AGENT CERTIFICATE - BASE64
PKCS12 base64 encoded agent certificate. Not needed if webconsole connection is provided.
AGENT CERTIFICATE PASSWORD
Agent peer certificate password. Not needed if webconsole connection is provided.
HTTPS CERTIFICATE - BASE64
PKCS12 base64 encoded HTTPS certificate. If not present then self-signed certificate will be created.
HTTPS CERTIFICATE PASSWORD
HTTPS certificate password.
MDM HOSTNAME
MDM hostname or IP address for mobile phones to connect to after enrollment. If empty, appliance IP address will be used.
NETWORKING PROPERTIES
NETWORK IP ADDRESS
The IP address for this interface. Leave blank if DHCP is desired.
NETWORK NETMASK
The netmask for this interface. Leave blank if DHCP is desired.
DEFAULT GATEWAY
The default gateway address for this VM. Leave blank if DHCP is desired.
DNS1
The domain name server for this VM (IP address). Domain from FQDN hostname will be used for short DNS names lookup. Optional for DHCP.
DNS2
The second domain name server for this VM (IP address). Optional field.
SUBMIT
I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy.

Revise los parámetros de configuración. Asegúrese de que la configuración sea correcta, ya que no es posible realizar cambios de configuración adicionales.

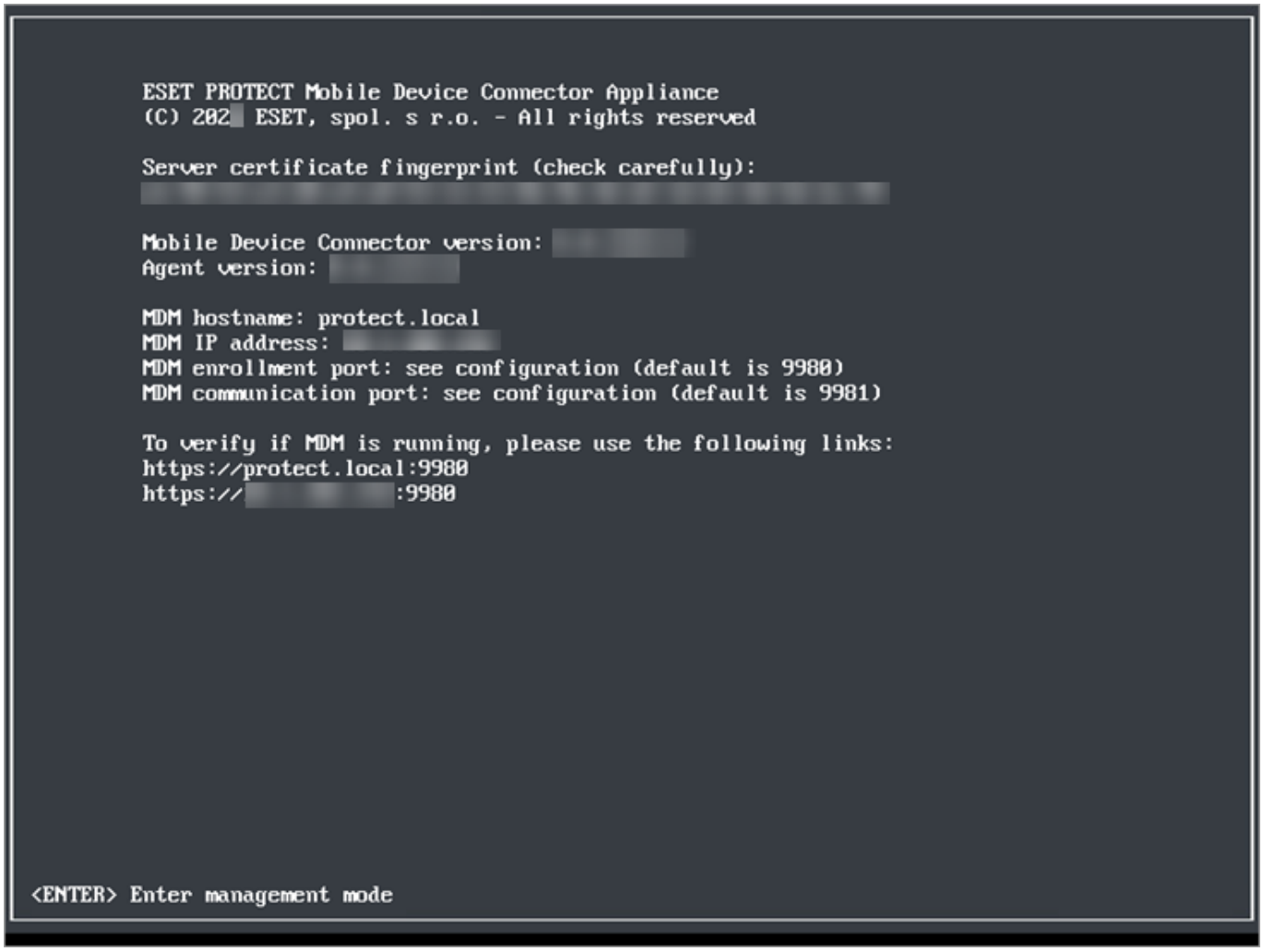
Marque la casilla **Acepto los términos del Contrato de licencia para el usuario final y la Política de privacidad de la aplicación**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET para obtener más información.

Haga clic en **Enviar** cuando haya terminado de hacer cambios.

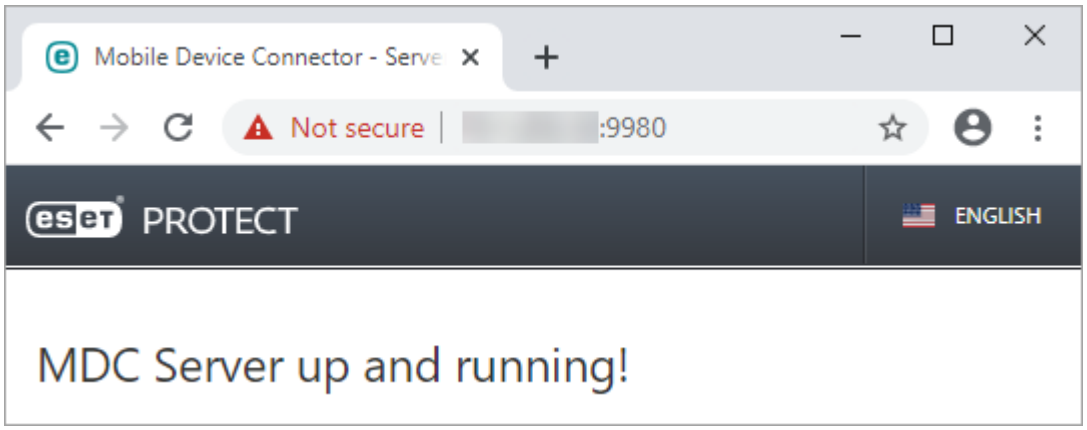
Cuando haga clic en **Enviar**, se mostrará la siguiente notificación:

> No actualice esta página en el navegador web, cierre la pestaña y acceda a la ventana de la consola del dispositivo virtual de ESET PROTECT.

En la ventana de la consola del dispositivo virtual de ESET PROTECT se mostrará su información de estado. Se mostrarán las versiones del componente de ESET PROTECT, así como el nombre de host, la dirección IP y el número de puerto de ESET PROTECT MDM. También encontrará la dirección de inscripción del dispositivo MDM con el siguiente formato: *https://[nombre de host]:9980 y https://[dirección IP]:9980*.



Introduzca la dirección de inscripción del dispositivo MDM mostrada (como se indica anteriormente) en su navegador para confirmar que el Conector de dispositivo móvil se ejecuta de forma correcta. Lo más probable es que su nombre de host y dirección IP sean distintos, los mostrados anteriormente se incluyen a título únicamente ilustrativo. Si la implementación se completó correctamente, se mostrará el siguiente mensaje:



Consola de administración del dispositivo virtual de ESET PROTECT

Una vez que haya implementado correctamente el dispositivo virtual de ESET PROTECT, abra la ventana de terminal de la máquina virtual. Verá una pantalla con información básica sobre el dispositivo virtual de ESET

PROTECT y su estado. Esta es la pantalla principal del dispositivo virtual de ESET PROTECT. Desde aquí puede iniciar sesión en la **Consola de administración del dispositivo virtual de ESET PROTECT** (también conocido como el **modo de administración**) pulsando la tecla **Entrar** en su teclado. Para acceder al modo de administración, escriba la contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT y pulse **Entrar** dos veces. Si no ha configurado el dispositivo virtual de ESET PROTECT todavía, puede usar la contraseña predeterminada`eraadmin` para acceder al modo de administración.

Cuando inicie sesión en la Consola de administración del dispositivo virtual de ESET PROTECT se mostrarán las siguientes opciones de configuración o administración:

- Configurar la dirección IP estática
- Activar o desactivar el acceso remoto
- Copia de seguridad de la base de datos
- Restaurar la base de datos
- Restauración tras recuperación de instantánea
- Recuperar la base de datos de otro servidor
- Cambiar la contraseña de la máquina virtual
- Cambiar la contraseña de la base de datos
- Unirse de nuevo al dominio
- Configurar el dominio
- Restablecimiento a valores de fábrica

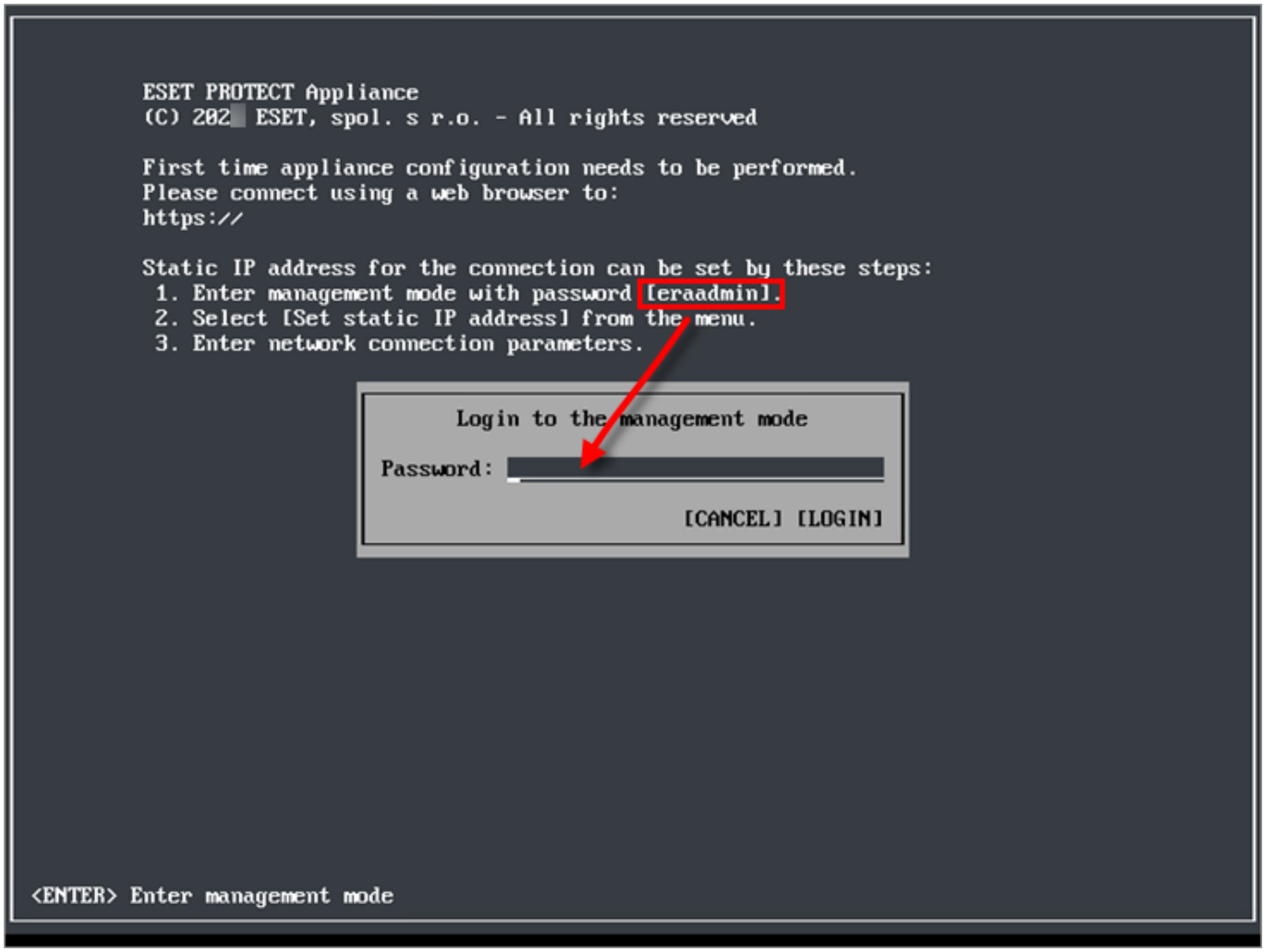
La presencia de los elementos anteriores puede variar según la fase de implementación del dispositivo virtual de ESET PROTECT y el tipo de dispositivo configurado.

- **Reiniciar el sistema**: si desea reiniciar el dispositivo virtual de ERAESET PROTECT.
- **Apagar el sistema**: si desea apagar el dispositivo virtual de ESET PROTECT.
- **Bloquear pantalla**: debe bloquear la pantalla para evitar que otras personas utilicen el dispositivo virtual de ESET PROTECT y accedan a sus archivos. También puede utilizar la tecla **Esc** para bloquear la pantalla, lo que resulta todavía más rápido. El modo de administración se cerrará y verá la pantalla principal del dispositivo virtual de ESET PROTECT.
- **Salir a terminal**: utilice esta opción si desea acceder al terminal del sistema operativo. Se cerrará la Consola de administración del dispositivo virtual de ESET PROTECT y se mostrará la ventana de terminal. Para volver a la pantalla principal del dispositivo virtual de ESET PROTECT desde la ventana del terminal, escriba `exit` y pulse la tecla **Entrar** (también puede usar el comando `logout`, que tiene el mismo efecto).

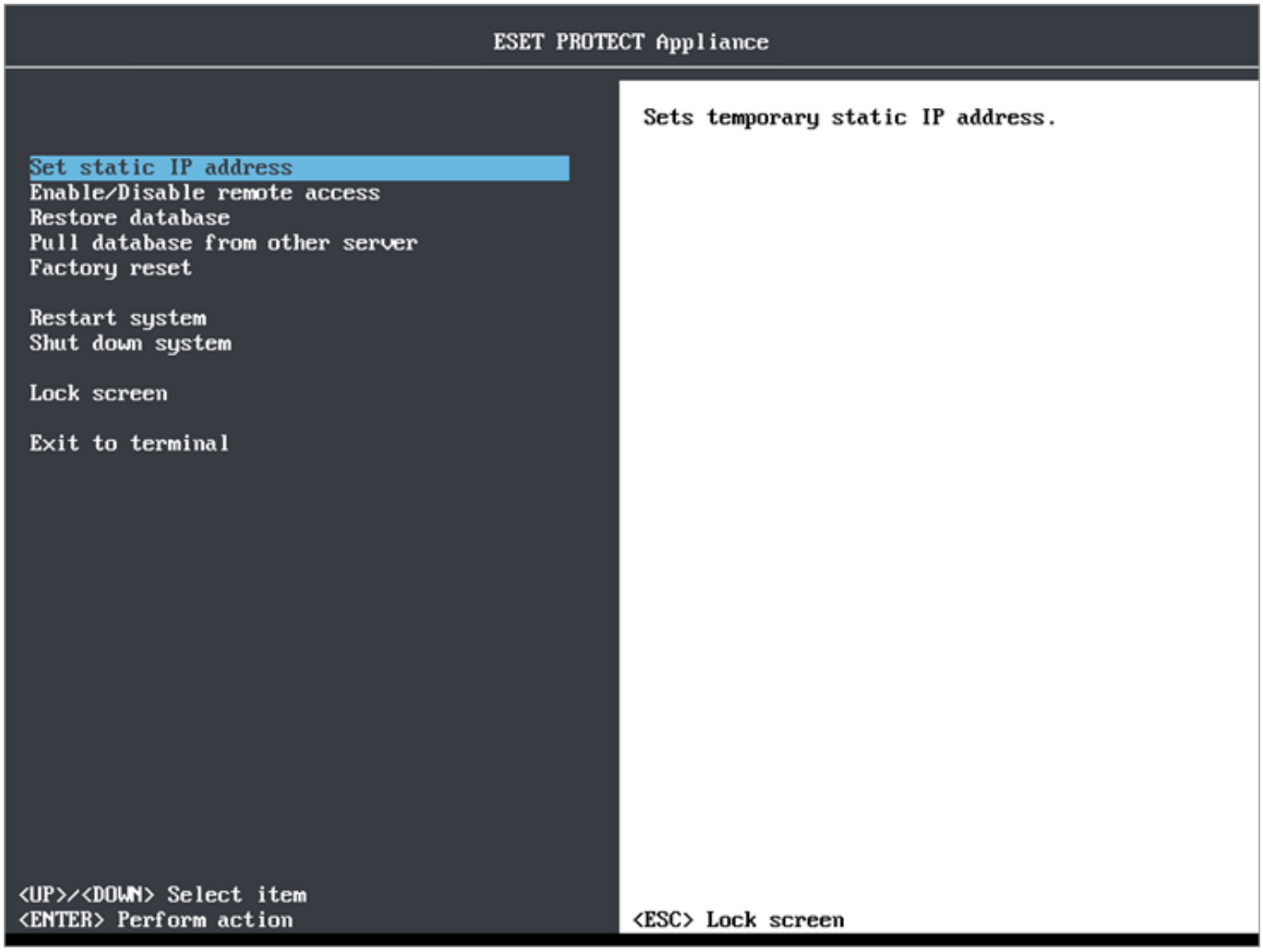
Configurar la dirección IP estática

Es necesario establecer la configuración de forma manual si el dispositivo virtual de ESET PROTECT no recibe una dirección IP asignada por un servidor DHCP. Para configurar una dirección IP estática manualmente, siga las instrucciones indicadas a continuación:

1. Desde la pantalla principal de la consola de la máquina virtual, pulse **Entrar** en el teclado para **Acceder al modo de administración**. Escriba `eraadmin` y pulse **Entrar** dos veces para **iniciar sesión**.



2. Seleccione **Configurar la dirección IP estática** con las teclas de flecha y pulse **Entrar**.



3. Se iniciará un asistente de configuración de red interactivo que le pedirá que configure los siguientes datos:
   - Dirección IP estática
   - Máscara de red
   - Dirección de la puerta de enlace
   - Dirección del servidor DNS

> Los parámetros de red se deben introducir en la notación IPv4 de puntos decimales, por ejemplo `192.168.1.10` (dirección IP) o `255.255.255.0` (máscara de red).
> Hasta si la red está correctamente configurada, **no** es posible hacer ping al equipo que contiene el dispositivo virtual de ESET PROTECT.

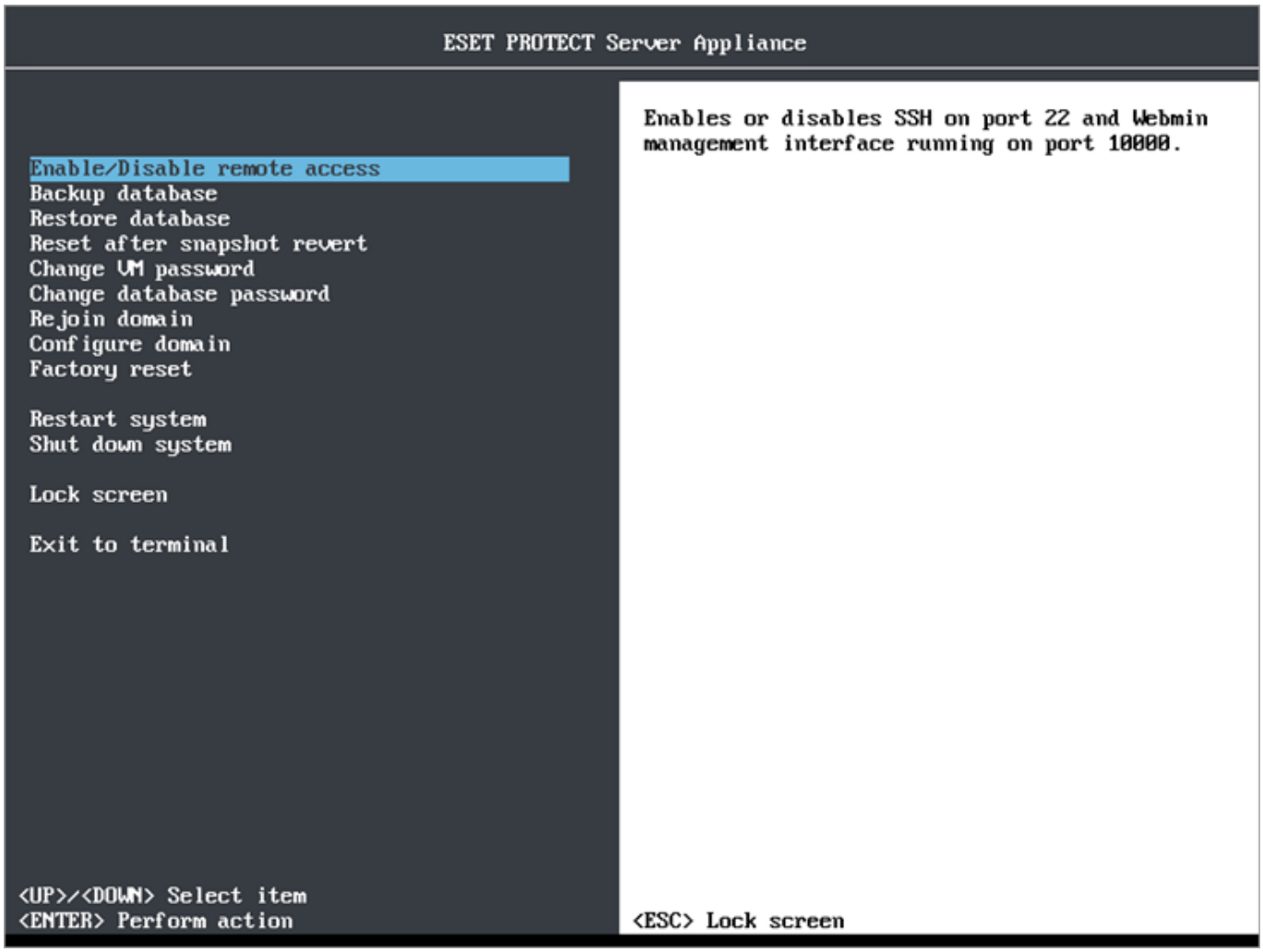
4. Pulse **Entrar** para continuar o **Ctrl+C** para **permanecer** en la ventana de terminal.

El dispositivo virtual de ESET PROTECT tiene, de forma predeterminada, un adaptador de red. Esto resulta suficiente, pero si agrega varios adaptadores de red por otros motivos, **Configurar la dirección IP estática** solo se aplicará al adaptador `eth0`

Activar o desactivar el acceso remoto

Para poder utilizar el acceso remoto (la interfaz de administración de Webmin y SSH), primero tiene que activarlo.

Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Enable/Disable remote access** con las teclas de flecha y pulse **Entrar**.

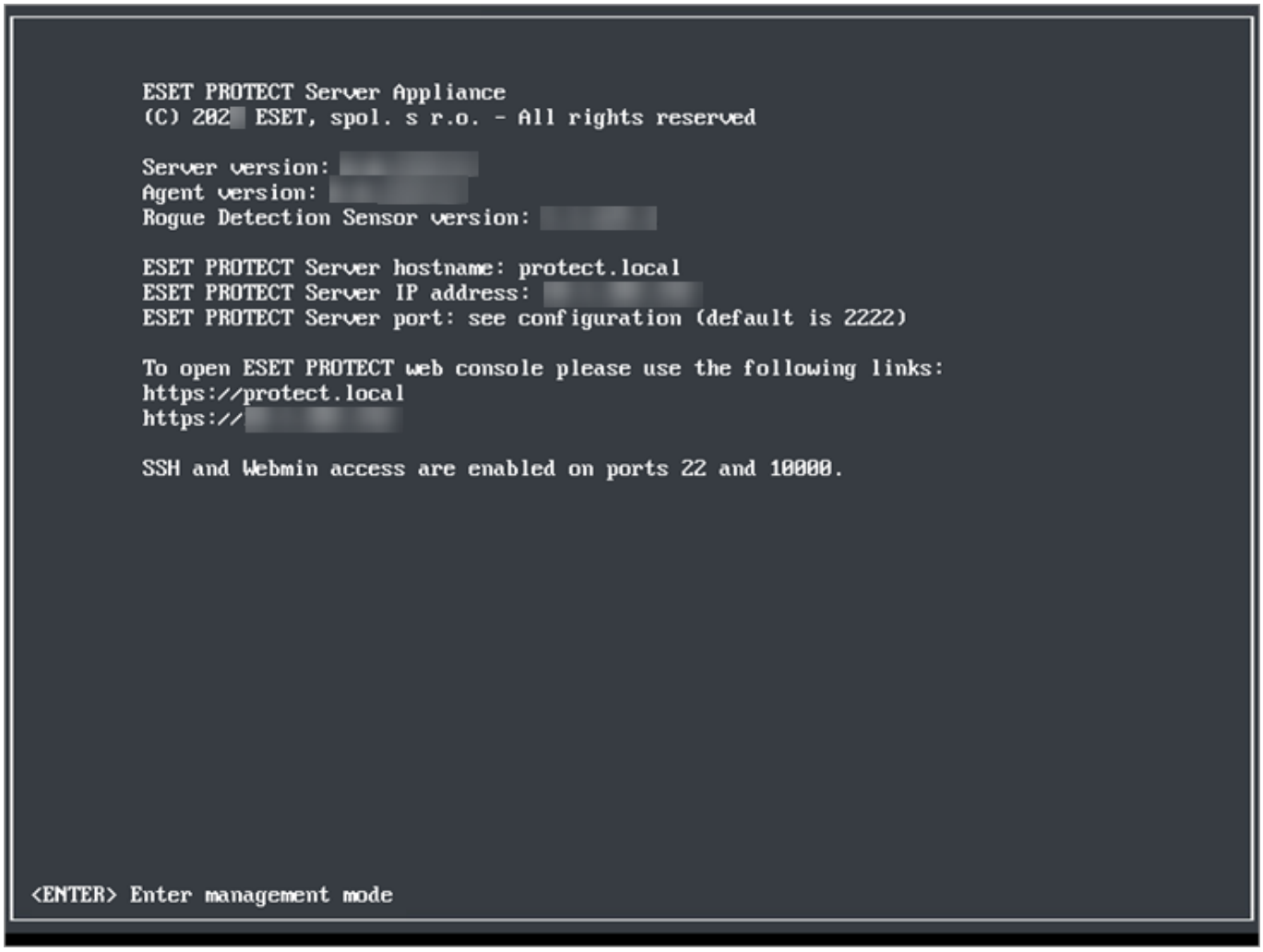


Ahora puede utilizar:

- Webminconsulte Interfaz de administración Webmin para obtener información detallada. Webmin utiliza HTTPS y se ejecuta en el puerto 10000. Para acceder a la interfaz de Webmin, utilice la dirección IP indicada con el número de puerto 10000 (*https://<host name or IP address>:10000*, por ejemplo, *https://10.10.11.16:10000* o *https://protect.local:10000*).

- Acceso remoto mediante SSH en el puerto 22 (es necesario para activar la recuperación de la base de datos).

En la pantalla principal de la Consola de administración del dispositivo virtual de ESET PROTECT se mostrará la siguiente información:



Consulte también Resolución de problemas de SSH.

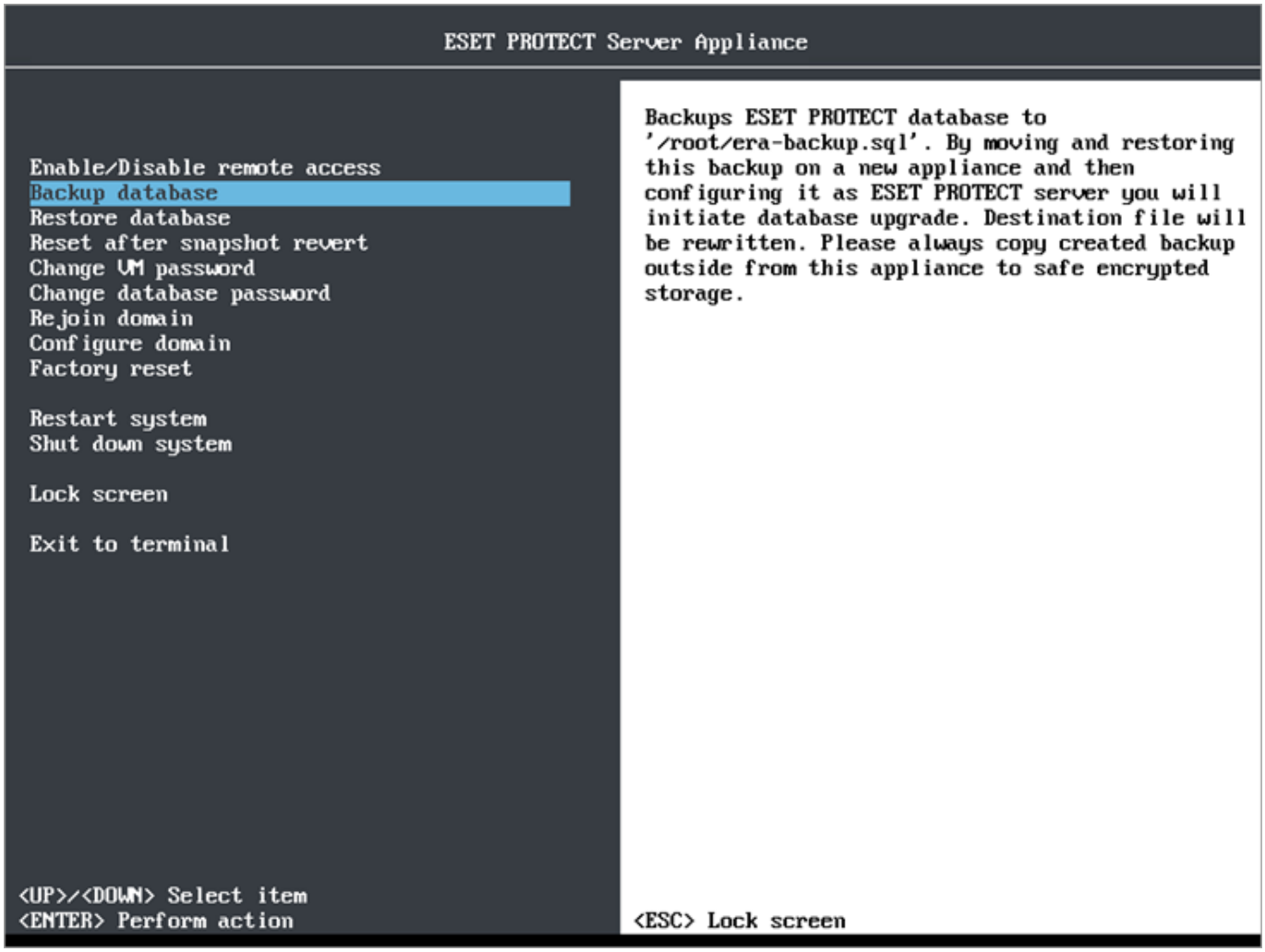
Copia de seguridad de la base de datos

La copia de seguridad es un elemento completamente vital dentro de una estrategia de recuperación de desastres sólida. Con la función **Copia de seguridad de la base de datos** se realizará una copia de seguridad de su **base de datos de ESET PROTECT** que se guardará en el archivo de copia de seguridad de MySQL *era-backup.sql* en la carpeta *root*.

Una alternativa a la copia de seguridad de la base de datos es crear instantáneas de la máquina virtual. De esta forma se conservará todo el dispositivo virtual de ESET PROTECT, todos los ajustes y la base de datos de ESET PROTECT. Sin embargo, si restaura una instantánea de su máquina virtual, tendrá que ejecutar la Restauración tras recuperación de instantánea.

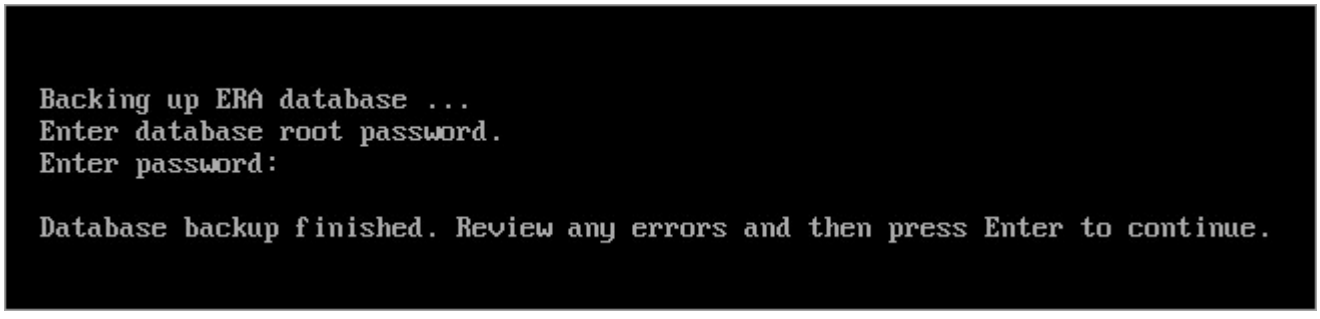
Le recomendamos que realice una copia de seguridad de la base de datos de ESET PROTECT con frecuencia, y que guarde el archivo de copia de seguridad en un dispositivo de almacenamiento externo. Esto es importante, ya que así tendrá una copia de toda la base de datos de ESET PROTECT almacenada en otra ubicación física (fuera de su dispositivo virtual de ESET PROTECT), en caso de que se produzca una situación de desastre. Por ejemplo, si el dispositivo virtual de ESET PROTECT se rompe, elimina o destruye por cualquier otro motivo. Al contar con una copia de seguridad reciente de la base de datos de ESET PROTECT podrá restaurar el dispositivo virtual de ESET PROTECT al mismo estado que presentaba antes de producirse el desastre. Para conocer el procedimiento detallado, consulte Recuperación de desastres del dispositivo virtual de ESET PROTECT.

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Copia de seguridad de la base de datos** con las teclas de flecha y pulse **Entrar**.



2. Se le pedirá que escriba la contraseña del usuario root de la base de datos para que pueda realizarse la copia de seguridad de la base de datos.

> Si no recuerda la contraseña del usuario root de la base de datos, puede modificarla y ejecutar de nuevo la copia de seguridad de la base de datos.



Este proceso puede tardar de unos segundos a varias horas, en función del tamaño de la base de datos.

> Compruebe siempre la pantalla en busca de errores. Si aparecen mensajes de error, no se podrá considerar que la copia de seguridad de la base de datos ha finalizado correctamente. Pruebe a ejecutar de nuevo la **Copia de seguridad de la base de datos**.

La copia de seguridad de la base de datos se almacena en la siguiente ruta de acceso: */root/era-backup.sql*

Descargue el archivo de copia de seguridad en un lugar seguro utilizando el gestor de archivos Webmin.

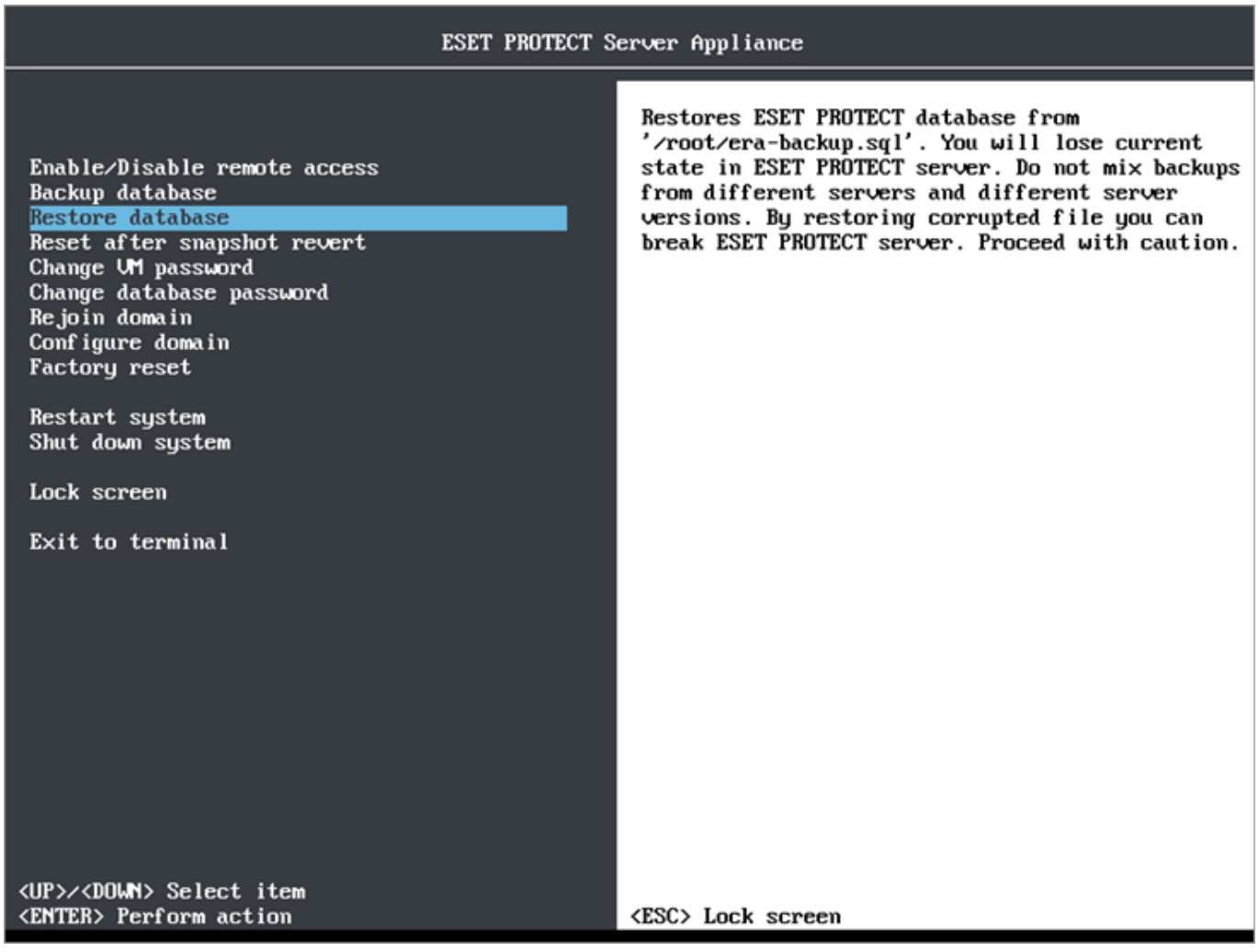
Restaurar la base de datos

Esta función sustituirá la base de datos actual con una base de datos de la copia de seguridad.

Se recomienda disponer de una instantánea de la máquina virtual o de una copia de seguridad de la base de datos actual. Se trata de una alternativa de restauración por si tiene problemas durante la restauración.

Siga estas instrucciones para **restaurar la base de datos**:

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Restaurar la base de datos** con las teclas de flecha y pulse **Entrar**.



Cargue el archivo de copia de seguridad *era-backup.sql* que quiera restaurar en el directorio *root* con el gestor de archivos de Webmin. El archivo *era-backup.sql* de destino se sobrescribirá. Omita este paso si desea restaurar el archivo *era-backup.sql* que ya se encuentra en el directorio *root*.

No mezcle copias de seguridad de servidores y versiones de servidor distintos. Utilice únicamente el archivo *era-backup.sql* del que realizó la copia de seguridad en este mismo dispositivo virtual de ESET PROTECT. Sin embargo, hay un caso en el que puede restaurar la base de datos en un dispositivo virtual de ESET PROTECT distinto, y es aquel en el que se acaba de implementar y aún no se ha realizado su configuración.

2. Puede que se le pida que **Introduzca la contraseña del usuario root de la base de datos** al principio del proceso de restauración de la base de datos. Sin embargo, si restaura la base de datos en un dispositivo virtual de ESET PROTECT recién implementado que aún no se ha configurado, no se le pedirá que introduzca la contraseña.

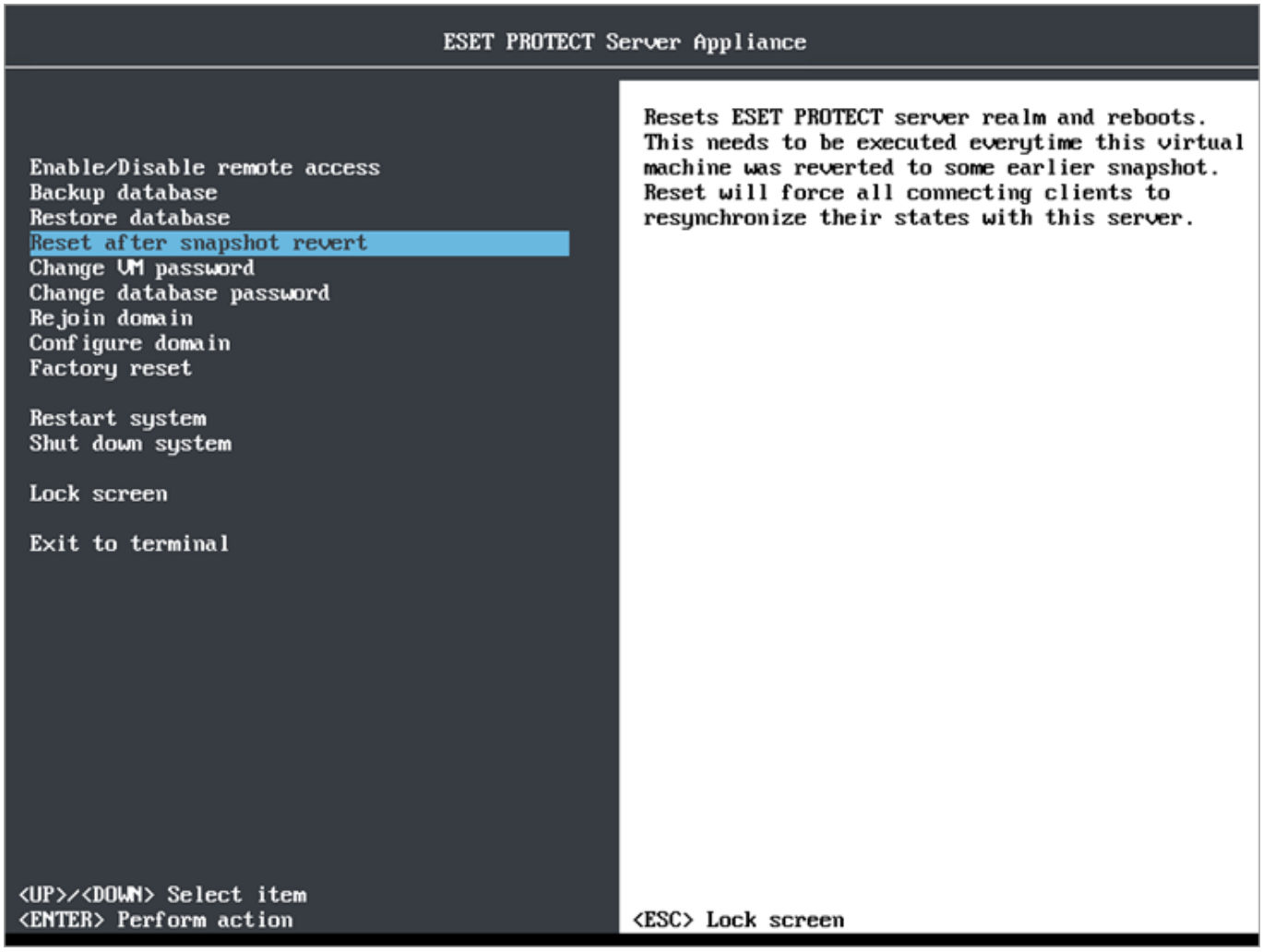
Este proceso puede tardar de unos segundos a varias horas, en función del tamaño de la base de datos.

Compruebe siempre la pantalla en busca de errores. Si aparecen mensajes de error, no se podrá considerar que la restauración de la base de datos ha finalizado correctamente. Pruebe a ejecutar de nuevo la **Restauración de la base de datos**.

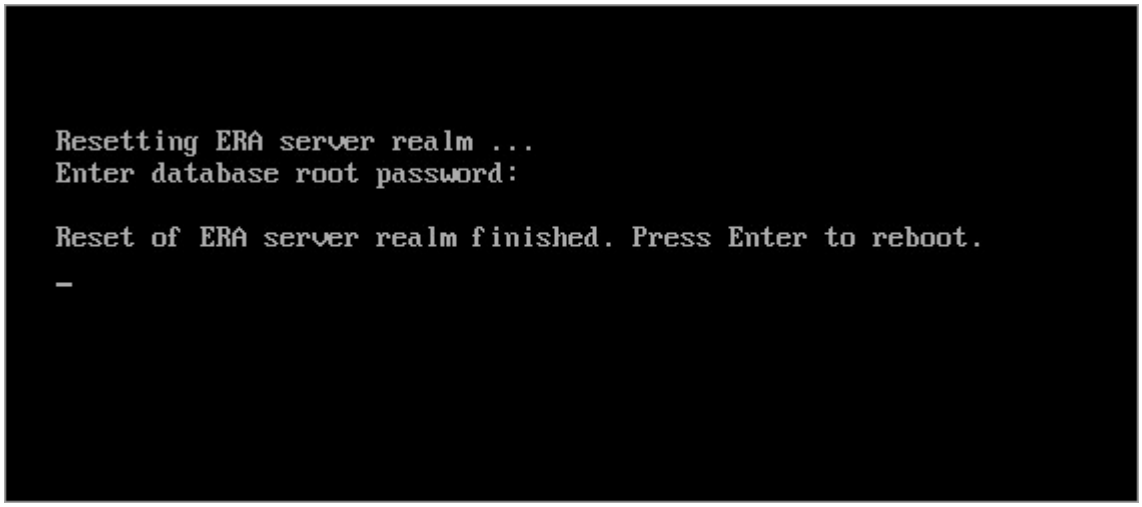
Restauración tras recuperación de instantánea

Siempre que restaure una instantánea de la máquina virtual a un estado anterior, tendrá que ejecutar la función **Reset after snapshot revert** para obligar a todos los clientes conectados a sincronizar su estado con este servidor.

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Reset after snapshot revert** con las teclas de flecha y pulse **Entrar**.



2. Se le pedirá que escriba la contraseña del usuario root de la base de datos para que se pueda restablecer el **ESET PROTECT Server realm**.



Recuperar la base de datos de otro servidor

Esta función le permite recuperar la base de datos de ESET PROTECT de un dispositivo virtual de ESET PROTECT que se encuentra en ejecución en su infraestructura. Solo es compatible con el servidor de ESET PROTECT, no en los demás componentes (MDM). Es una opción muy práctica al actualizar el dispositivo virtual de ESMC o un dispositivo virtual de ESET PROTECT antiguo al dispositivo virtual de ESET PROTECT más reciente, o si quiere

migrar el dispositivo virtual de ESET PROTECT.

Si realiza una migración, debe poder accederse al dispositivo virtual de ESET PROTECT antiguo para que la política de cambio del nombre de host o la dirección IP se aplique a todos los ordenadores cliente. De lo contrario, los clientes no se conectarán al nuevo dispositivo virtual de ESET PROTECT, e intentarán conectarse al antiguo.

Asegúrese de activar SSH en su dispositivo virtual de ESET PROTECT.

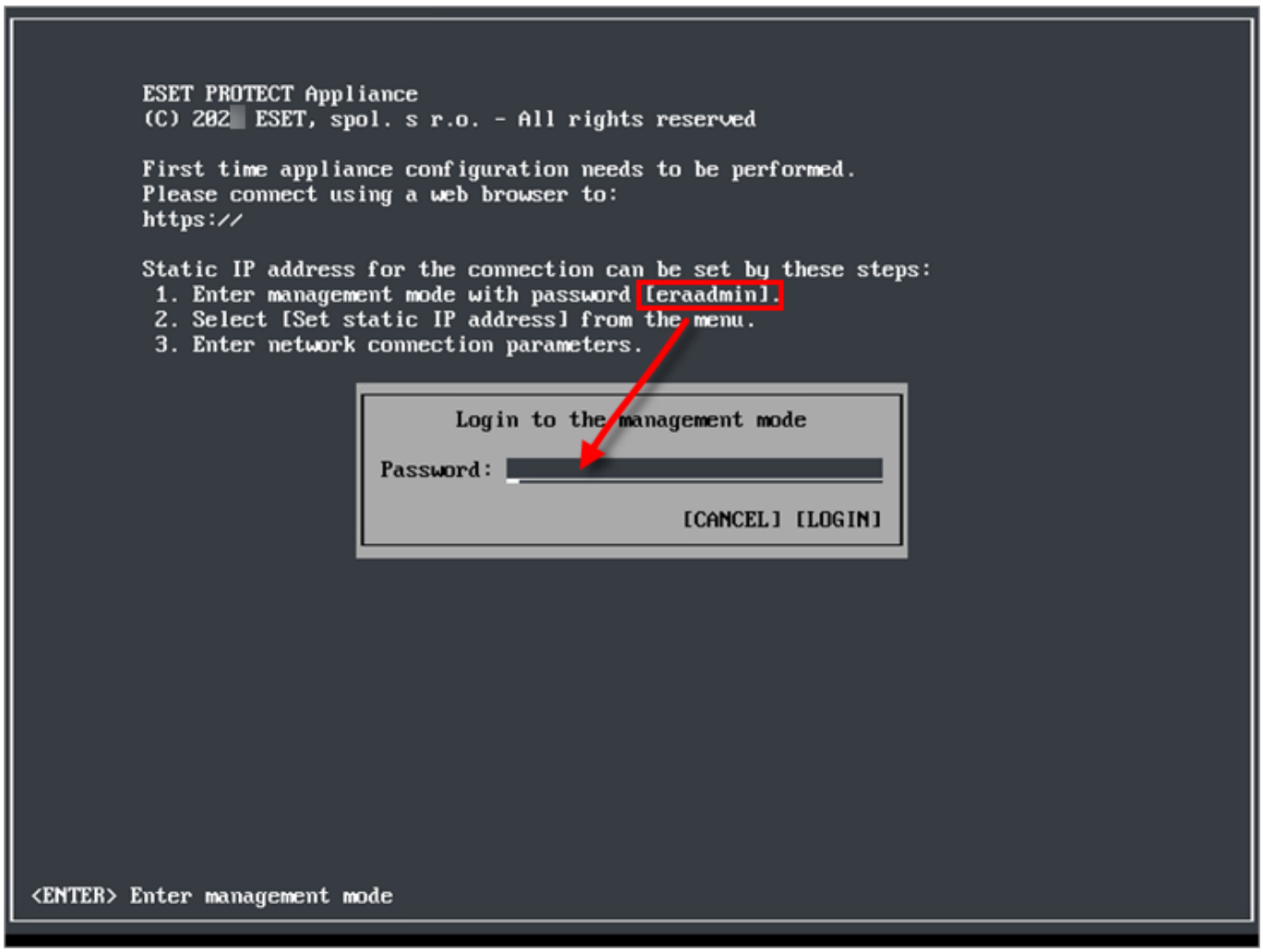
Realice una recuperación de la base de datos solo al migrar a una versión más reciente o a la misma versión de ESET PROTECT Server. Durante el procedimiento de recuperación, se actualiza la estructura de la base de datos, pero este proceso fallará si se recupera en un servidor más antiguo. La recuperación de la base de datos es una de las dos formas de actualizar el dispositivo virtual.

Siga estos pasos para recuperar una base de datos:

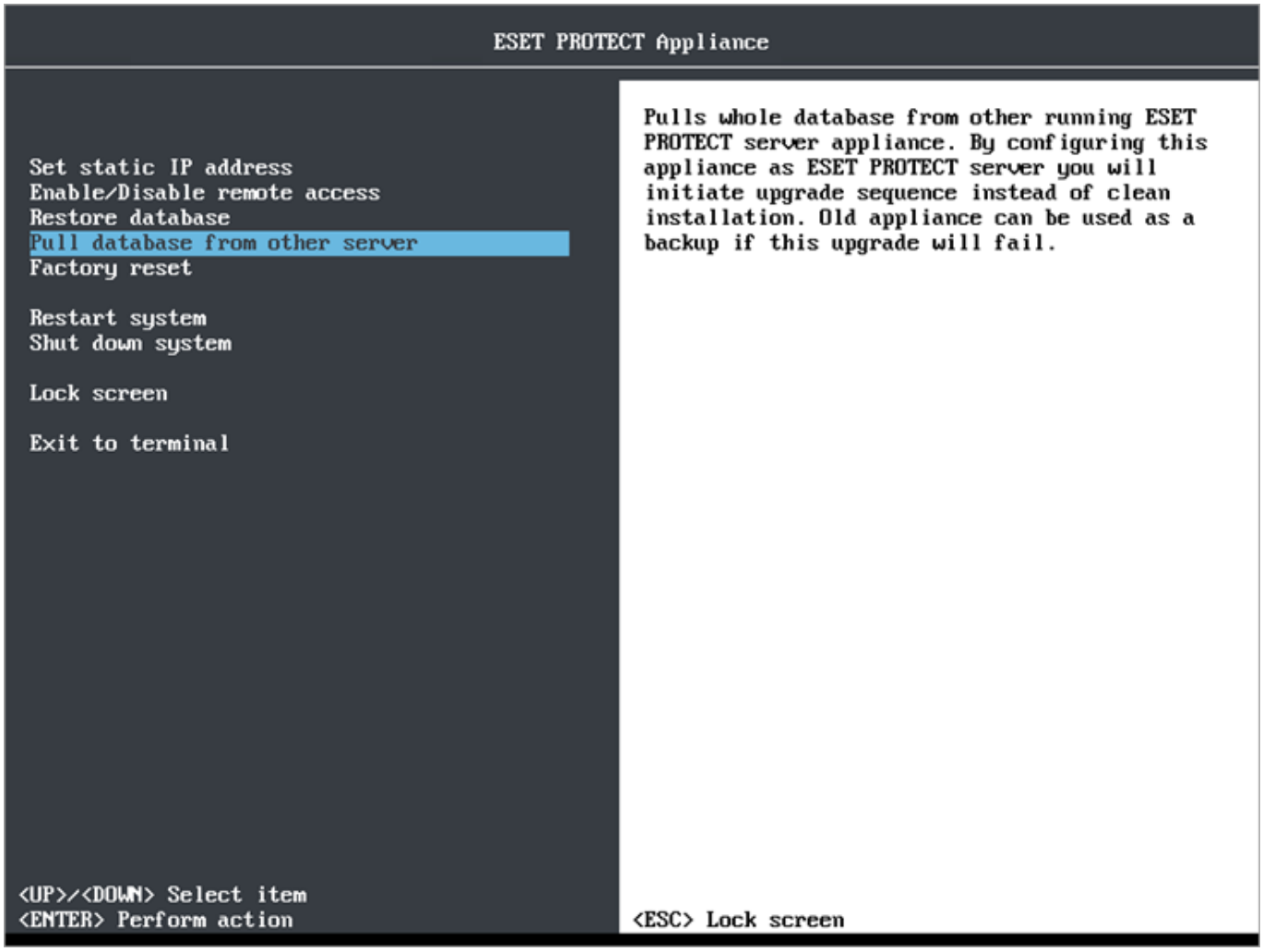
1. Implemente un dispositivo virtual de ESET PROTECT nuevo, pero no lo configure todavía.

2. Abra la consola de la máquina virtual y, en la pantalla principal, pulse **Entrar** en el teclado para **Acceder al modo de administración** del dispositivo virtual de ESET PROTECT que acaba de implementar.

3. Escriba `eraadmin` y pulse **Entrar** dos veces para **iniciar sesión**.



4. Seleccione **Recuperar la base de datos de otro servidor** con las teclas de flecha y pulse **Entrar**.



5. **Introduzca la contraseña del usuario root de la base de datos** en el dispositivo virtual de ESET PROTECT remoto desde el que quiere recuperar la base de datos de ESET PROTECT (el dispositivo virtual de ESET PROTECT antiguo). Si solo utiliza una contraseña en el dispositivo virtual de ESET PROTECT antiguo, escríbala aquí.

6. **Introduzca la conexión con el dispositivo virtual de ESET PROTECT remoto (SSH)**: escriba el nombre de usuario (`root`) y el nombre de cliente o la dirección IP de su antiguo dispositivo virtual de ESET PROTECT con el siguiente formato: `root@direcciónIP` o `root@nombrehost`.

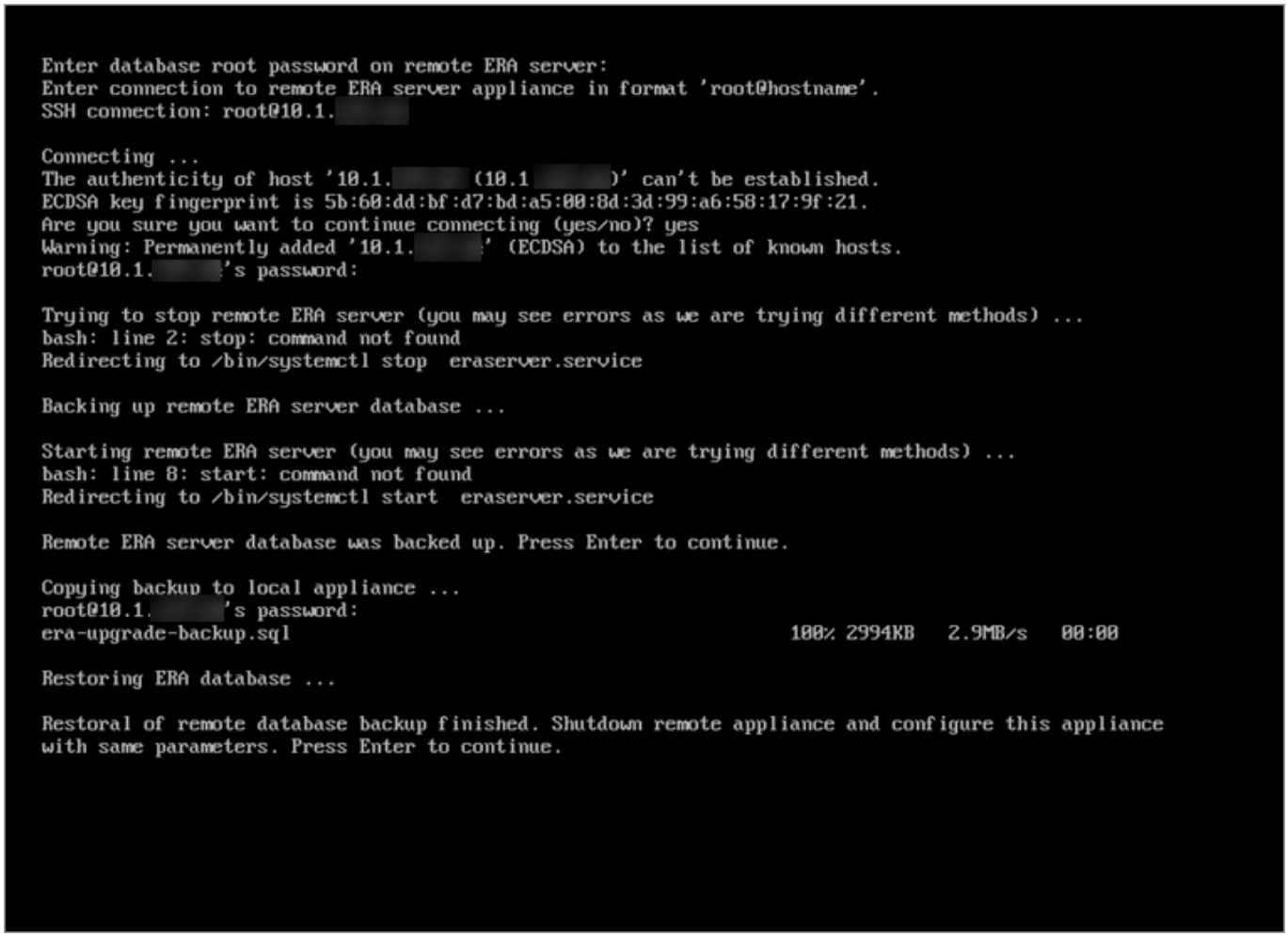
7. Si se le pregunta acerca de **La autenticidad del host**, escriba `yes`. De lo contrario, ignore este paso.

8. Escriba la **Contraseña de la máquina virtual** del dispositivo virtual de ESET PROTECT antiguo, y pulse **Entrar**. Se mostrará el mensaje **Se realizó una copia de seguridad de la base de datos del ERA Server remoto** cuando la operación de copia de seguridad haya finalizado.

> El tiempo necesario para finalizar las operaciones de copia de seguridad y restauración variará en función del tamaño de la base de datos.

9. Escriba la **Contraseña de la máquina virtual** del dispositivo virtual de ESET PROTECT antiguo de nuevo. Puede que se le pida que introduzca la contraseña varias veces durante el proceso de copia, en función del tiempo que tarde la copia de la base de datos.

10. Espere hasta que se restaure la base de datos.



11. Si está realizando una actualización: Tras recuperar la base de datos de ESET PROTECT correctamente, apague el dispositivo virtual de ESET PROTECT antiguo para retirarlo.

- Se recomienda que conserve el dispositivo virtual de ESET PROTECT durante tiempo suficiente para asegurarse de que la nueva instancia está funcionando correctamente.
- Le recomendamos encarecidamente que no desinstale el antiguo dispositivo virtual de ESET PROTECT Server mediante un script de desinstalación. Este procedimiento de desinstalación disociará (quitará) todas las licencias de la nueva base de datos del dispositivo virtual de ESET PROTECT Server. Para evitar este comportamiento, elimine la base de datos del antiguo dispositivo virtual de ESET PROTECT Server (DROP DATABASE) antes de desinstalar.

12. Configure el nuevo dispositivo:

- **Actualización**: configure el nuevo dispositivo virtual exactamente igual que el dispositivo virtual de ESET PROTECT anterior.

- **Migración**: cambie la configuración para adaptarla a las propiedades de un nuevo dominio (configurar o unirse de nuevo al dominio) o una nueva red, por ejemplo, si ha trasladado el dispositivo virtual de ESET PROTECT a una red distinta.

Asegúrese de que se conservan todos los datos, de que todos los clientes se conectan al servidor nuevo y de que el dispositivo virtual de ESET PROTECT nuevo se comporta exactamente igual que el antiguo.

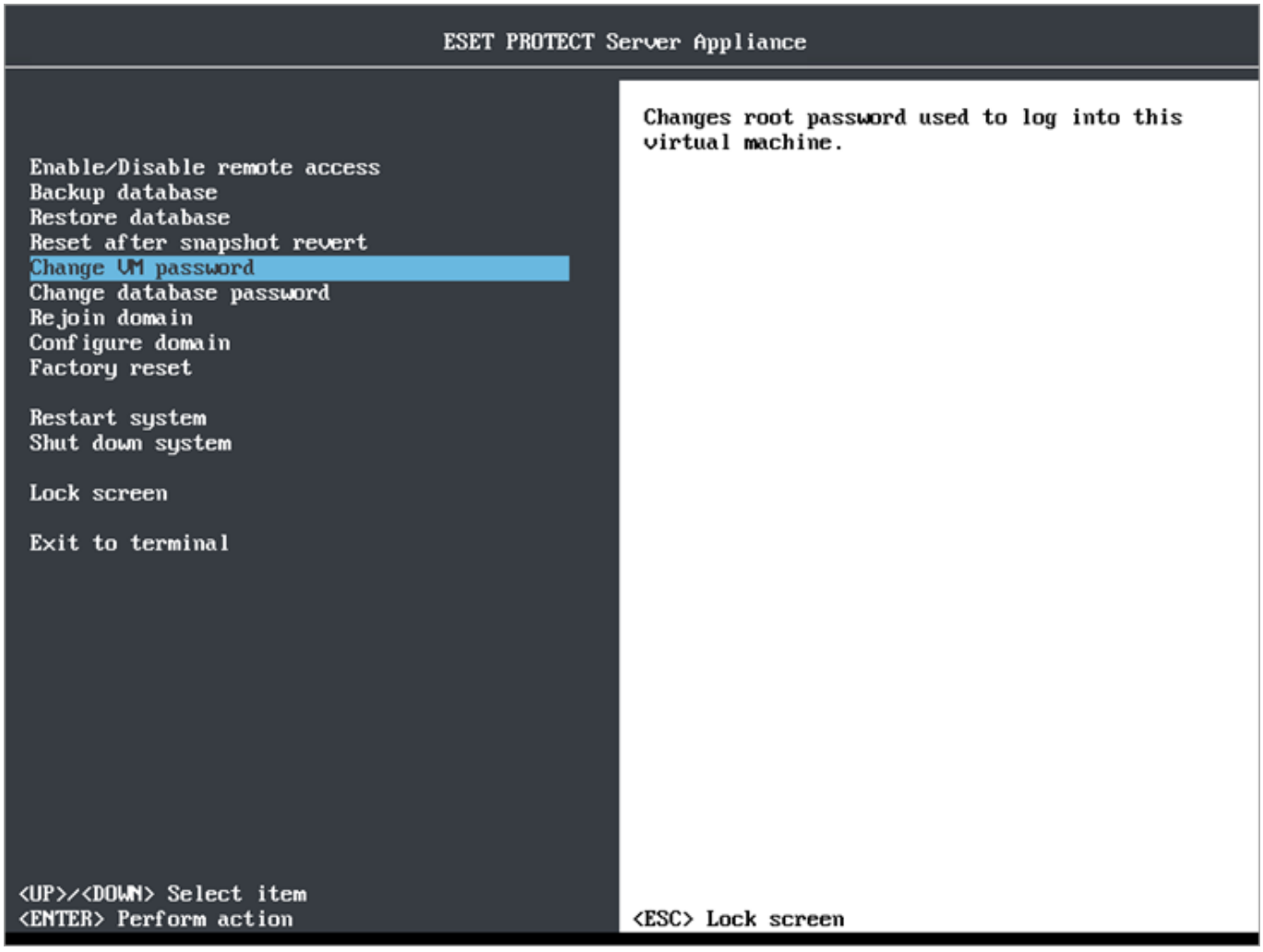
Cambiar la contraseña de la máquina virtual

La contraseña de la máquina virtual se utiliza para iniciar sesión en el dispositivo virtual de ESET PROTECT implementado. Si desea cambiar la contraseña de la máquina virtual o mejorar la seguridad de la misma, le recomendamos que utilice contraseñas seguras y las cambie regularmente.

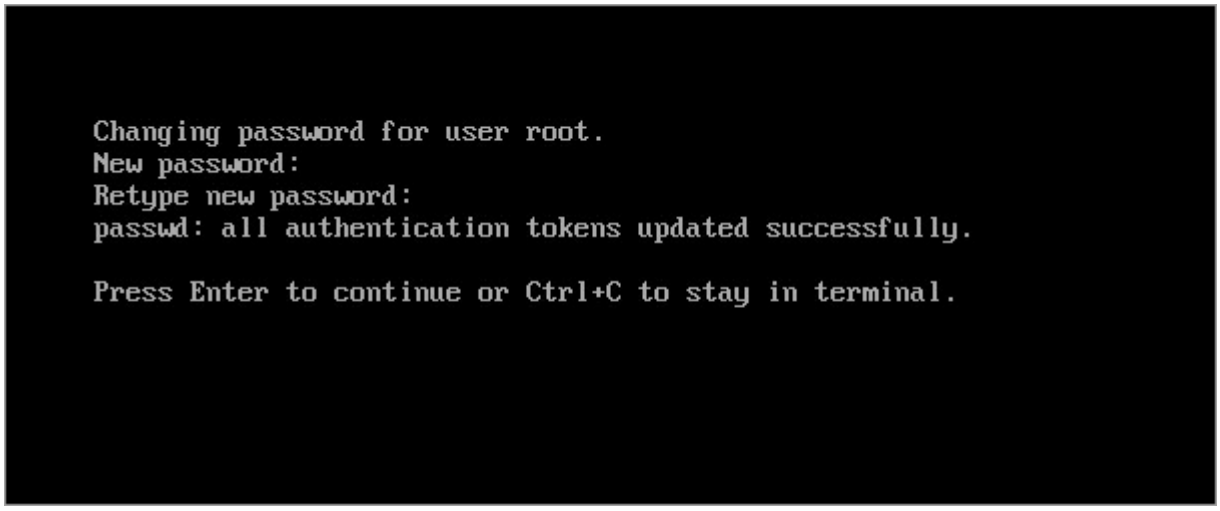
Este procedimiento solo cambiará la contraseña de la máquina virtual. La contraseña de ESET PROTECT Web Console y del usuario root de la base de datos no se modificarán. Para obtener más información, consulte los tipos de contraseña del dispositivo virtual de ESET PROTECT.

Si ha olvidado la contraseña, consulte Cómo recuperar una contraseña del dispositivo virtual de ESET PROTECT olvidada.

1. Acceda al **modo de administración** escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione**Cambiar la contraseña de la máquina virtual** con las teclas de flecha y pulse **Entrar**.



2. Escriba la **Nueva contraseña** en el campo vacío, pulse **Entrar** y, a continuación, **Vuelva a escribirla** para confirmarla.

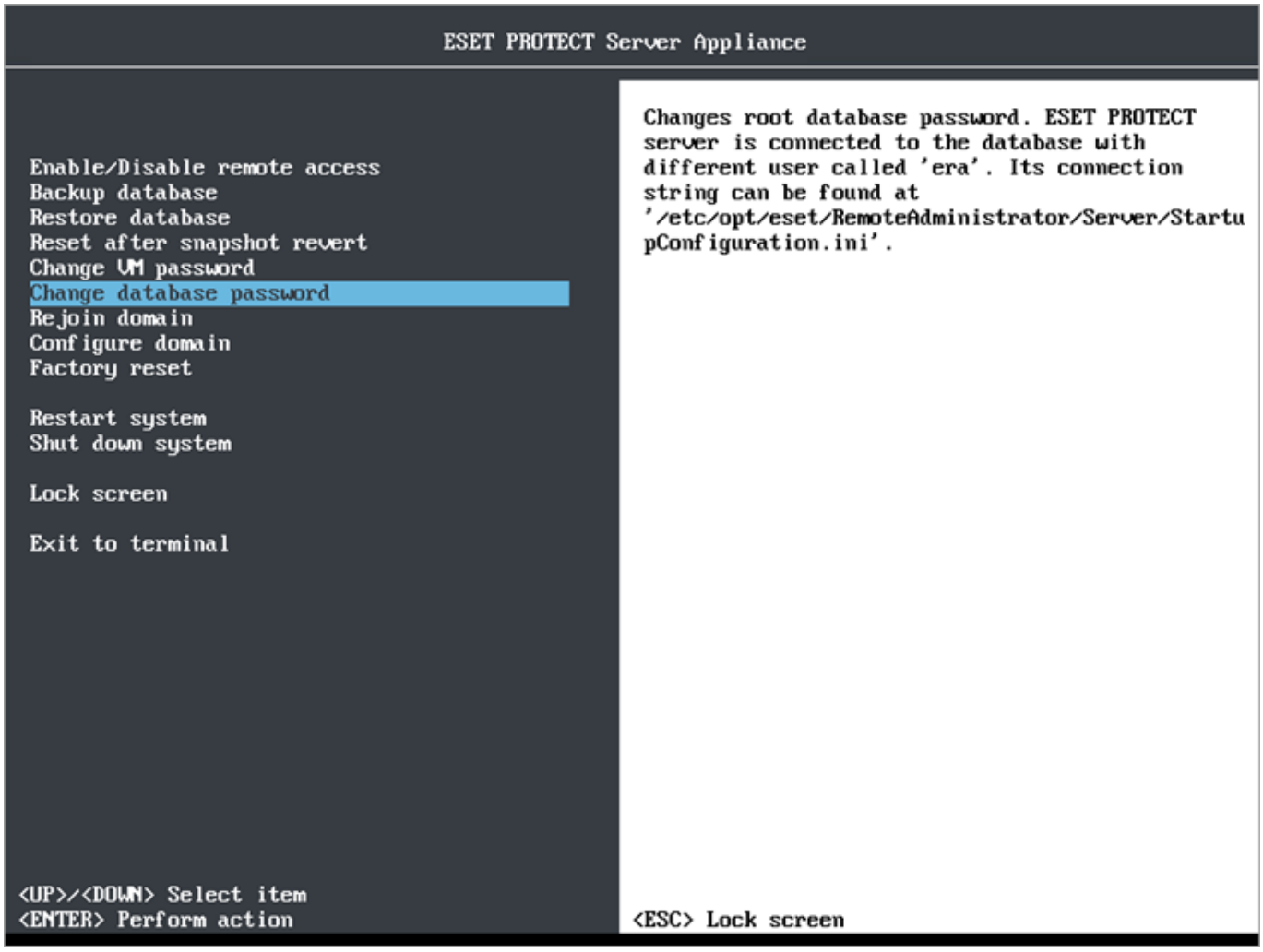


Se mostrará el mensaje Todos los tokens de autenticación se han actualizado correctamente cuando termine, y se le solicitará la **Nueva contraseña** para iniciar sesión.

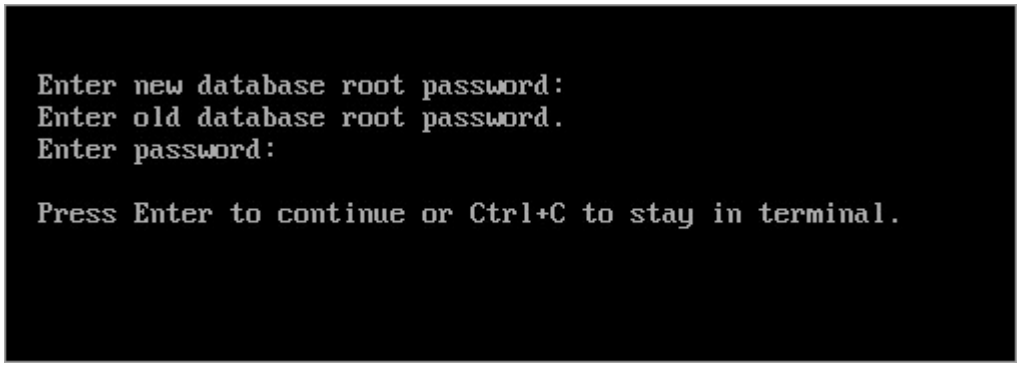
Cambiar la contraseña de la base de datos

La contraseña del usuario `root` de la base de datos concede acceso total al servidor de bases de datos MySQL. El usuario `root` de MySQL tiene control total únicamente del servidor MySQL.

1. Acceda al **modo de administración** escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Change database password** con las teclas de flecha y pulse **Entrar**.



2. Cuando se le pida que **Introduzca la antigua contraseña del usuario root de la base de datos**, introduzca la contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT. Esta contraseña puede ser distinta de la **Contraseña de la máquina virtual**, si la ha modificado por separado.



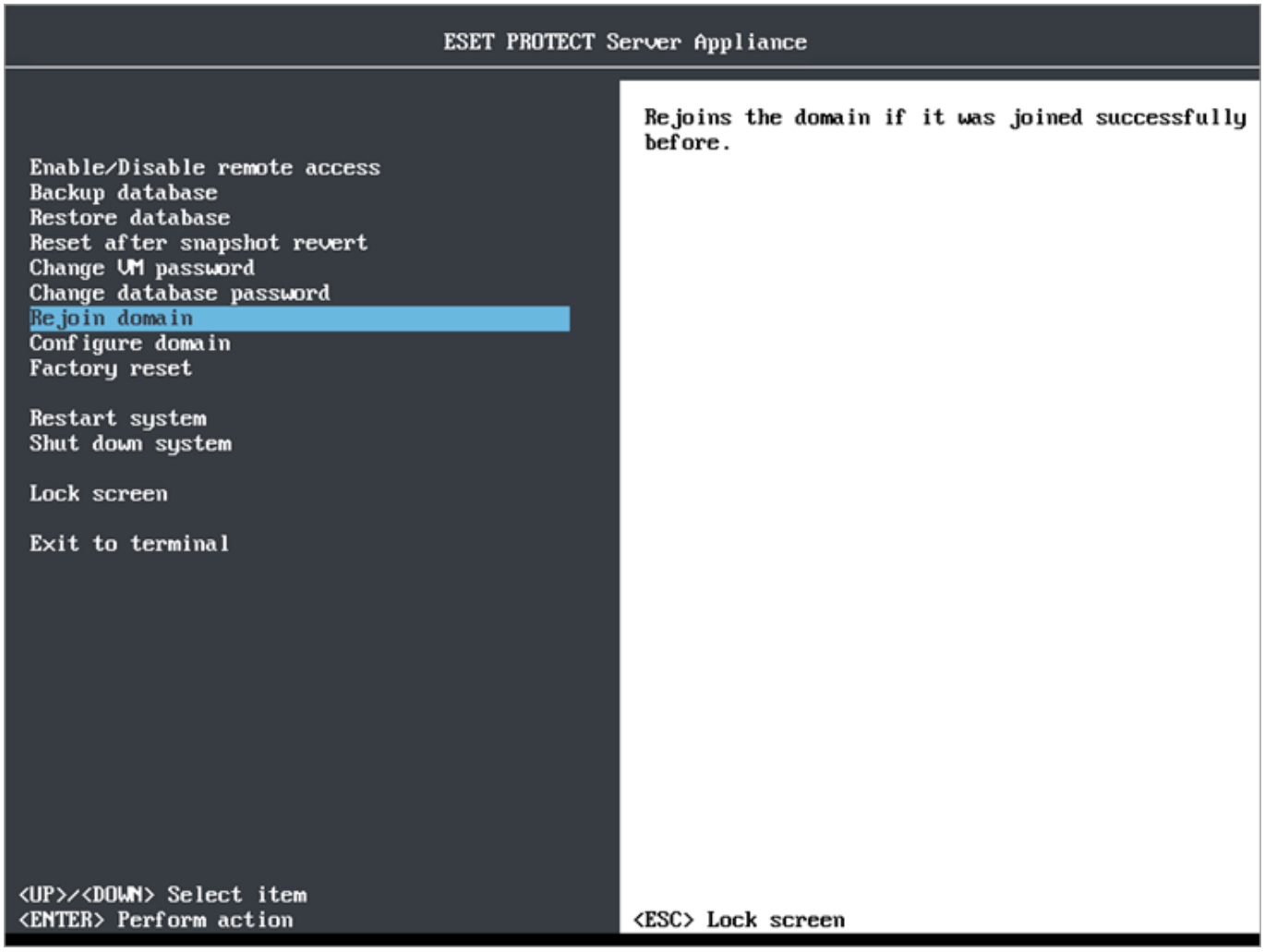
La contraseña del usuario `root` de la base de datos se ha modificado.

Unirse de nuevo al dominio

Utilice esta función si tiene problemas con Active Directory o con las relaciones de confianza con el dominio.

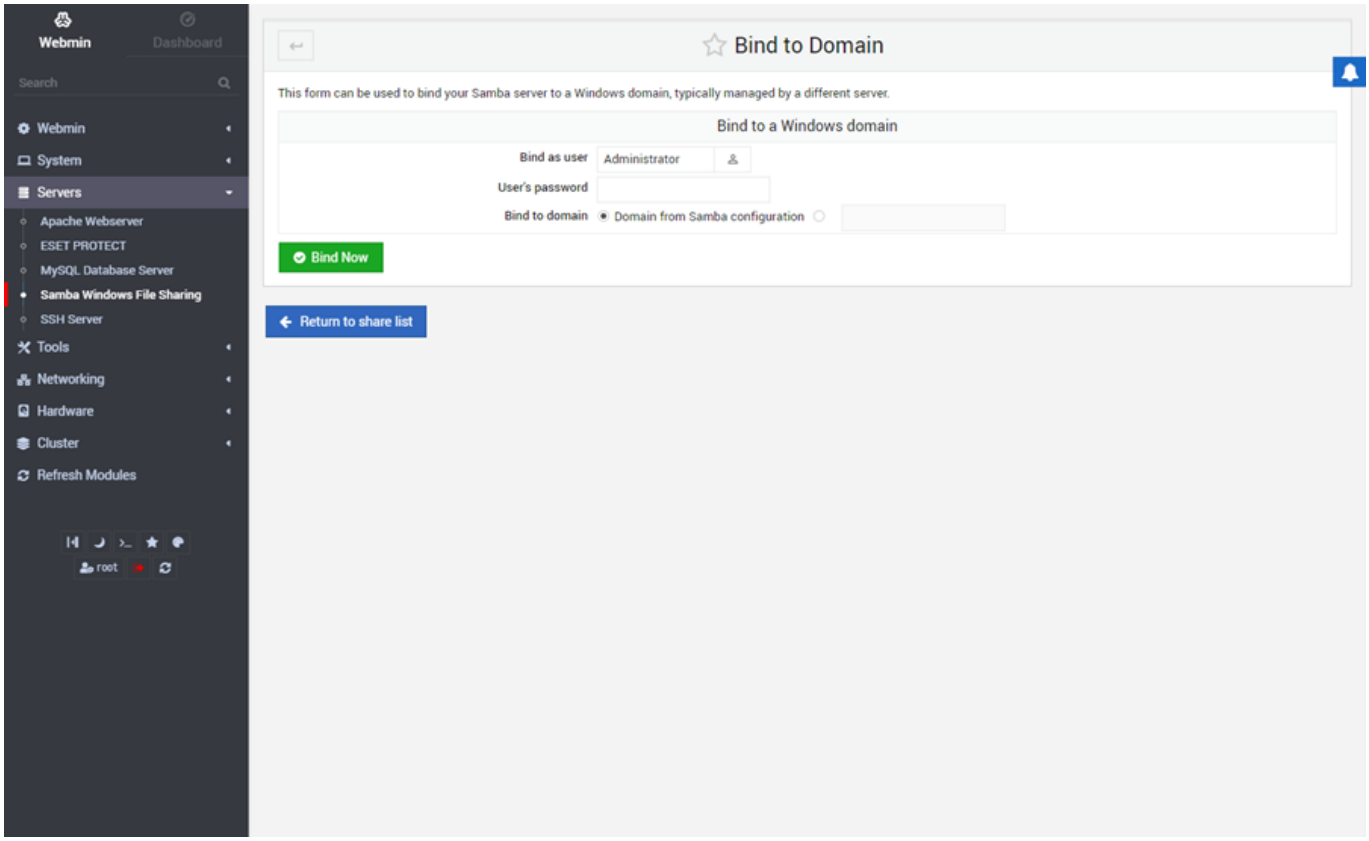
Es necesario tener el dominio configurado correctamente, o la función Unirse de nuevo al dominio podría no ejecutarse.

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Rejoin domain** con las teclas de flecha y pulse **Entrar**.



2. Escriba el nombre de usuario de dominio que se utilizará para unirse al dominio.

Si no está familiarizado con Linux y la ventana de terminal, puede acceder a Webmin y utilizar la función **Bind to Domain** de Compartir archivos en Windows con Samba.



Configurar el dominio

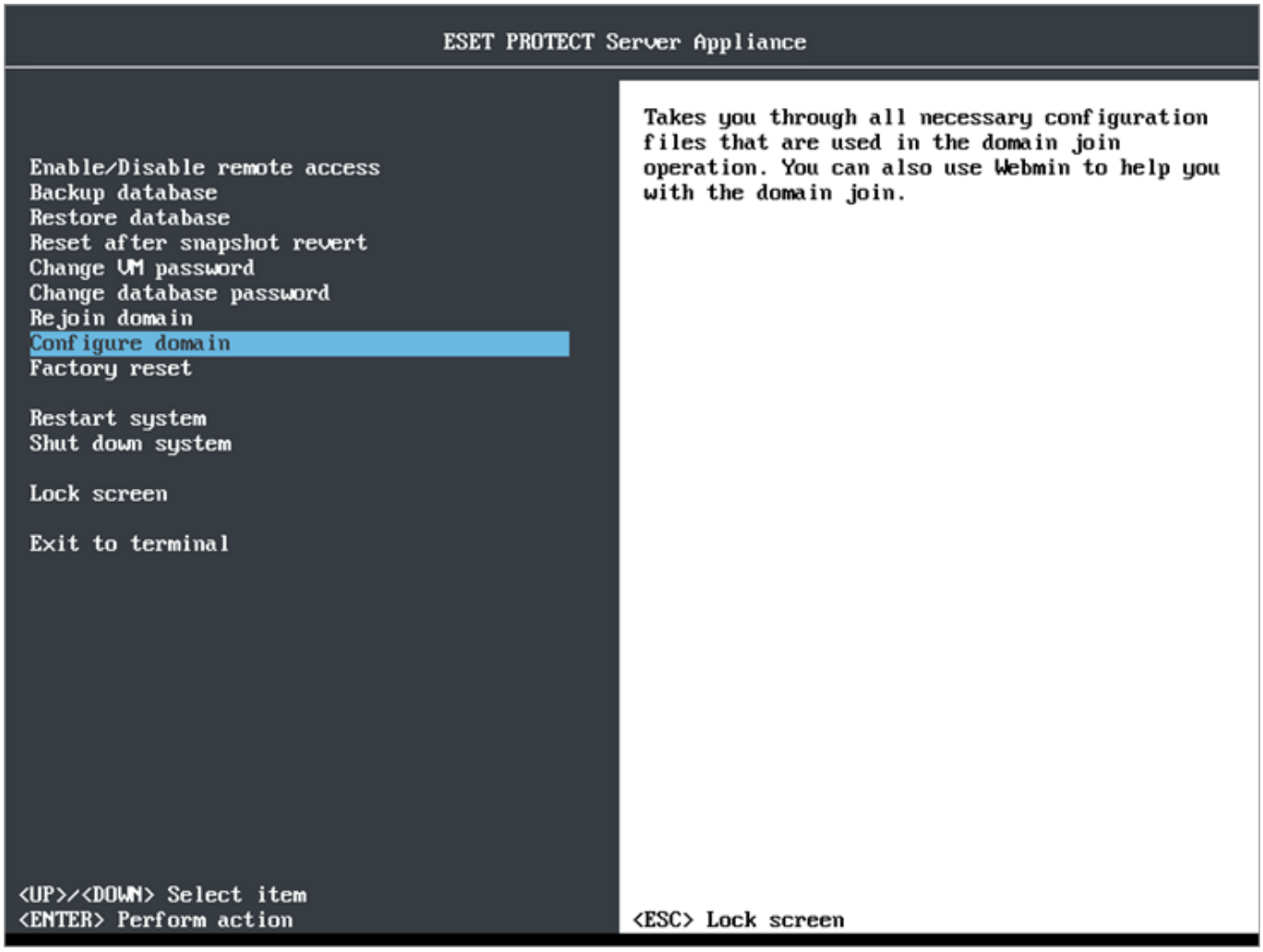
Si la operación de unión al dominio falla, el motivo suele ser una configuración incorrecta de los archivos del dispositivo virtual de ESET PROTECT. **Configure Domain** le permite modificar los archivos de configuración para incluir ajustes específicos de su entorno. Están disponibles los siguientes archivos de configuración:

Nombre del archivo	Descripción
/etc/hosts	El archivo Hosts debe estar correctamente asignado al nombre de su controlador de dominio y a su dirección IP.
/etc/krb5.conf	El archivo de configuración de Kerberos debe generarse correctamente. Asegúrese de que `kinit <user-from-domain>` funciona.
/etc/ntp.conf	El archivo de configuración de NTP debe contener un registro para actualizaciones de tiempo periódicas según la información del controlador de dominio.
/etc/samba/smb.conf	El archivo de configuración de Samba debe generarse correctamente.

Estos archivos están preconfigurados y requieren cambios mínimos al especificar un nombre de dominio, por ejemplo, o un nombre de controlador de dominio, un nombre de servidor de DNS, etc.

1. Acceda al **modo de administración** escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Configure domain** con las teclas de flecha y pulse **Entrar**.

> este es un procedimiento avanzado que recomendamos exclusivamente a administradores expertos.



2. Pulse **Entrar** para modificar el primer archivo de configuración.

3. Pulse **Ctrl+X** para cerrar el editor de texto. Se le pedirá que guarde los cambios, pulse **Y** para guardarlos o **N** para descartarlos. Si no ha efectuado ningún cambio, el editor de texto simplemente se cerrará. Si desea realizar más cambios, no utilice **Ctrl+X**, pulse **Ctrl+C** para cancelar y volver al editor de texto. Visite este artículo de la base de conocimiento para ver ejemplos de cómo cambiar los archivos de configuración.

Consulte */root/help-with-domain.txt* en su dispositivo virtual de ESET PROTECT; la forma más sencilla es buscar *help-with-domain.txt* con el gestor de archivos Webmin. También puede utilizar el comando `nano help-with-domain.txt` para consultar el archivo de ayuda.
Si no está familiarizado con Linux y la ventana de terminal, puede configurar la conexión a dominio (configuración de Kerberos, NTP o red mediante Compartir archivos en Windows con Samba) desde Webmin.

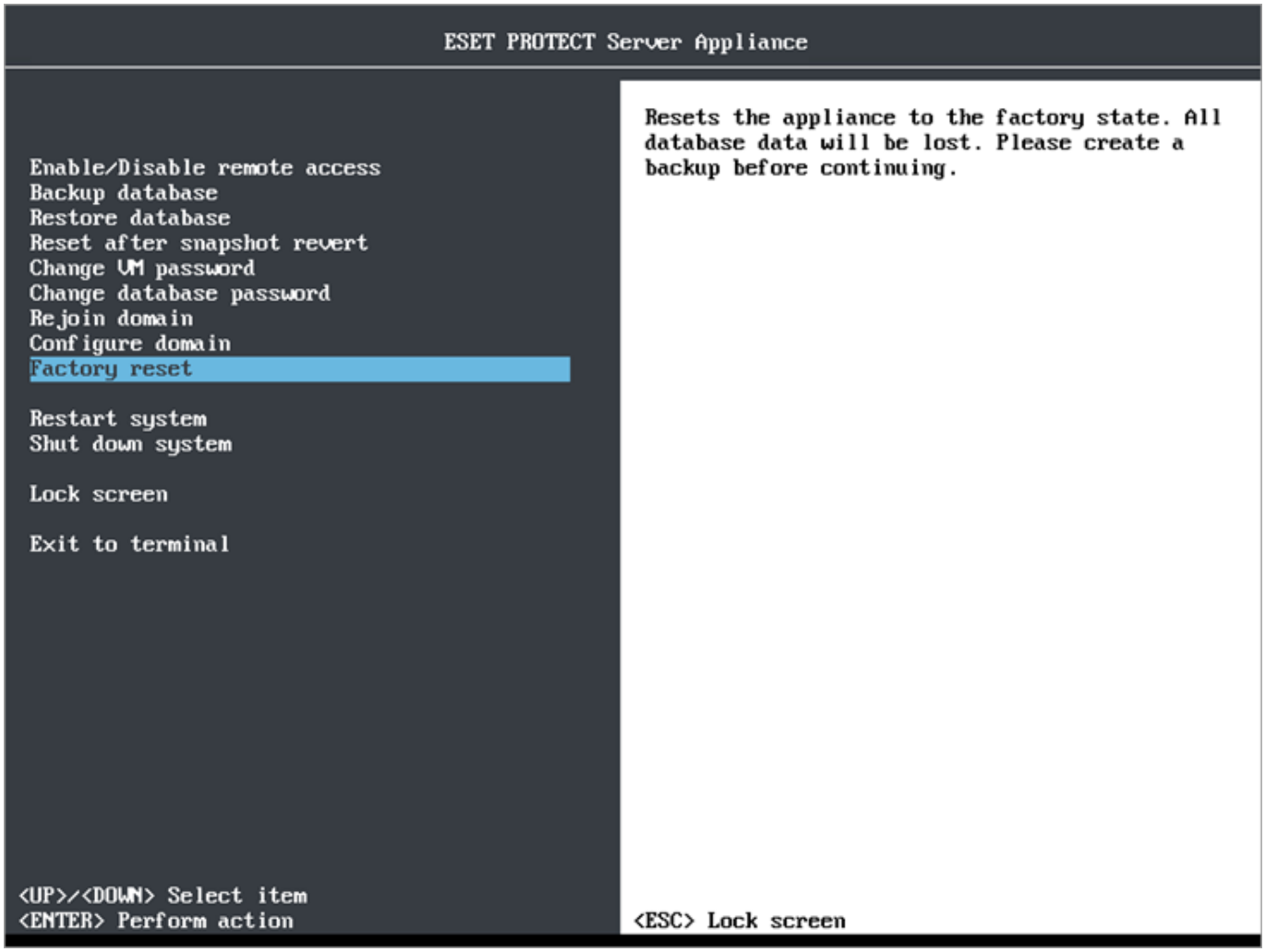
4. Una vez configurado el dominio, seleccione **Unirse de nuevo al dominio** y escriba el nombre y la contraseña del administrador para la conexión al dominio.

Restablecimiento a valores de fábrica

Puede utilizar el **Restablecimiento a valores de fábrica** para restaurar el estado original del dispositivo virtual de ESET PROTECT que presentaba cuando se implementó por primera vez. Se restablecerán la configuración y los ajustes, y se eliminará la base de datos de ESET PROTECT al completo.

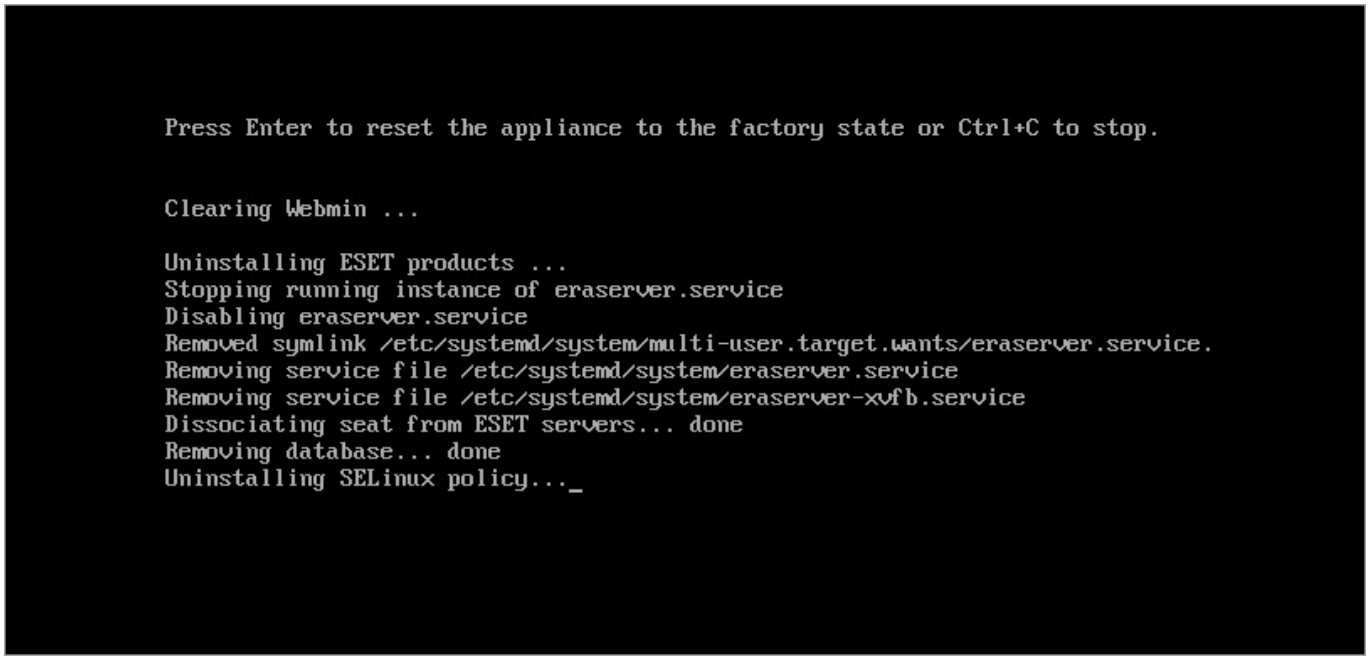
Se recomienda encarecidamente realizar una copia de seguridad de la base de datos de ESET PROTECT antes de ejecutar un **restablecimiento a valores de fábrica**. Tras realizarlo, la base de datos estará vacía. El **restablecimiento a valores de fábrica** únicamente restaurará los ajustes modificados durante la configuración del dispositivo virtual de ESET PROTECT, el resto de cambios y ajustes se conservarán. En casos extraños, el **restablecimiento a valores de fábrica** no restaurará por completo el estado original de su dispositivo virtual. Si tiene problemas con el dispositivo virtual de ESET PROTECT, se recomienda que implemente una máquina nueva. Siga los pasos necesarios para realizar una actualización o migración, o ejecute un procedimiento de recuperación ante desastres.

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Factory reset** con las teclas de flecha y pulse **Entrar**.



2. Pulse **Entrar** para ejecutar el **restablecimiento a valores de fábrica** del dispositivo virtual de ESET PROTECT o puede salir al menú pulsando **Ctrl+C** en este punto.

Mientras el **restablecimiento a valores de fábrica** esté en ejecución, no pulse **Ctrl+C**, ya que hacerlo puede dañar el dispositivo virtual.



Si ve algún mensaje de error en la pantalla durante el **restablecimiento a valores de fábrica**, pruebe a ejecutar el restablecimiento de nuevo. Si ejecutar el **restablecimiento a valores de fábrica** de nuevo no sirve de ayuda o no está seguro, se recomienda realizar una implementación nueva. Puede seguir los mismos pasos que se describen en actualización o migración, o realizar un procedimiento de recuperación ante desastres.

Restablecimiento a valores de fábrica realiza las siguientes acciones:

- Restablece la configuración de red, todas las contraseñas y el nombre de host.
- Borra Webmin, los archivos de configuración del dispositivo, los paquetes y los registros del sistema.
- Elimina los datos de la base de datos de ESET PROTECT.
- Restablece la contraseña del usuario de la base de datos de ESET PROTECT.

Cuando el dispositivo virtual de ESET PROTECT se reinicie, presentará el estado original que tenía cuando se implementó por primera vez, y podrá empezar a configurarlo desde cero.

Las modificaciones o ajustes personalizados no relacionados con ESET PROTECT no sufrirán cambio alguno.

Interfaz de administración Webmin

Webmin es una interfaz web de terceros que simplifica el proceso de administración de un sistema Linux. Webmin se desarrolló pensando en usuarios que tienen ciertos conocimientos de Linux pero no están familiarizados con la complejidad asociada a la administración de un sistema. Le permite realizar estas tareas desde una interfaz web muy sencilla y que actualiza automáticamente todos los archivos de configuración necesarios. Así, la tarea de administración del sistema resulta mucho más sencilla.

- Webmin está disponible a través de un navegador web. Puede iniciar sesión en esta interfaz desde cualquier sistema (ordenador cliente o dispositivo móvil) que esté conectado a la red. Es más fácil de utilizar a través de la red que utilizar de forma local otros entornos gráficos de configuración.

- Las versiones recientes de Webmin se pueden distribuir y modificar de forma gratuita para uso tanto comercial como no comercial. Puede consultar más información en las páginas web de Webmin.

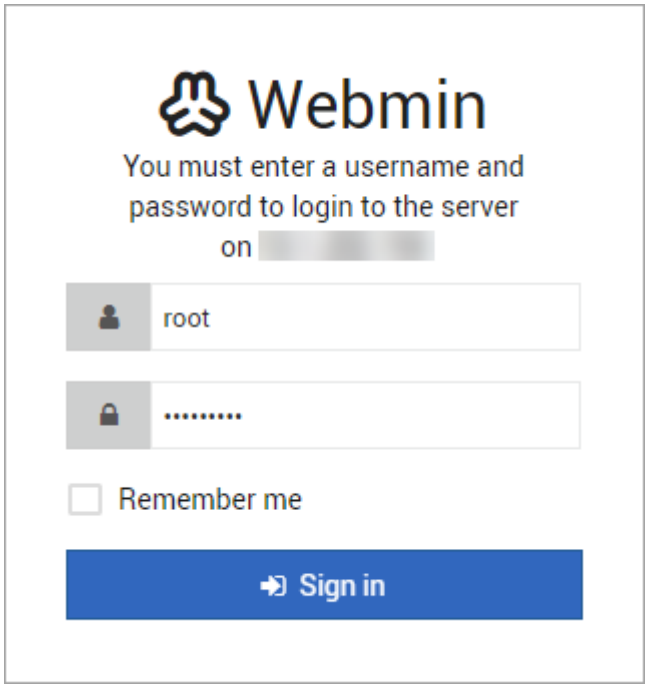
Webmin está incluido en el dispositivo virtual de ESET PROTECT. Para empezar a utilizarlo debe activarlo. Utiliza HTTPS y se ejecuta en el puerto 10000. La dirección IP de Webmin se mostrará en la pantalla de la Consola de administración del dispositivo virtual de ESET PROTECT.

Para acceder a Webmin:

Abra el navegador web e introduzca la dirección IP o el nombre de host del dispositivo virtual de ESET PROTECT implementado en la barra de direcciones. Utilice el puerto 10000 y el siguiente formato de URL: *https://<host name or IP address>:10000* por ejemplo *https://10.1.119.162:10000* o *https://esmcva:10000.*

Introduzca el nombre de usuario y la contraseña:

- El nombre de usuario es **root**
- La contraseña predeterminada es **eraadmin**, pero si la ha modificado, utilice la contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT.



Tras iniciar sesión correctamente se mostrará la Consola de Webmin.

Consola

Al iniciar sesión en Webmin, en la **Consola** se mostrará la Información del sistema de su dispositivo virtual de ESET PROTECT, con información como el nombre de host, el sistema operativo, el tiempo de actividad del sistema, el uso de memoria, las actualizaciones de paquetes, etc. También se mostrará un área de notificaciones en la parte inferior de la página en la que se mostrarán aquellos elementos que requieren su atención. Por ejemplo, podría mostrarse una notificación en la que se indica que hay una nueva versión de Webmin disponible y que le permite tomar medidas pulsando el botón **Actualizar Webmin**. Se recomienda actualizarlo. Una vez completada la actualización, aparecerá el mensaje **Instalación de Webmin finalizada**.

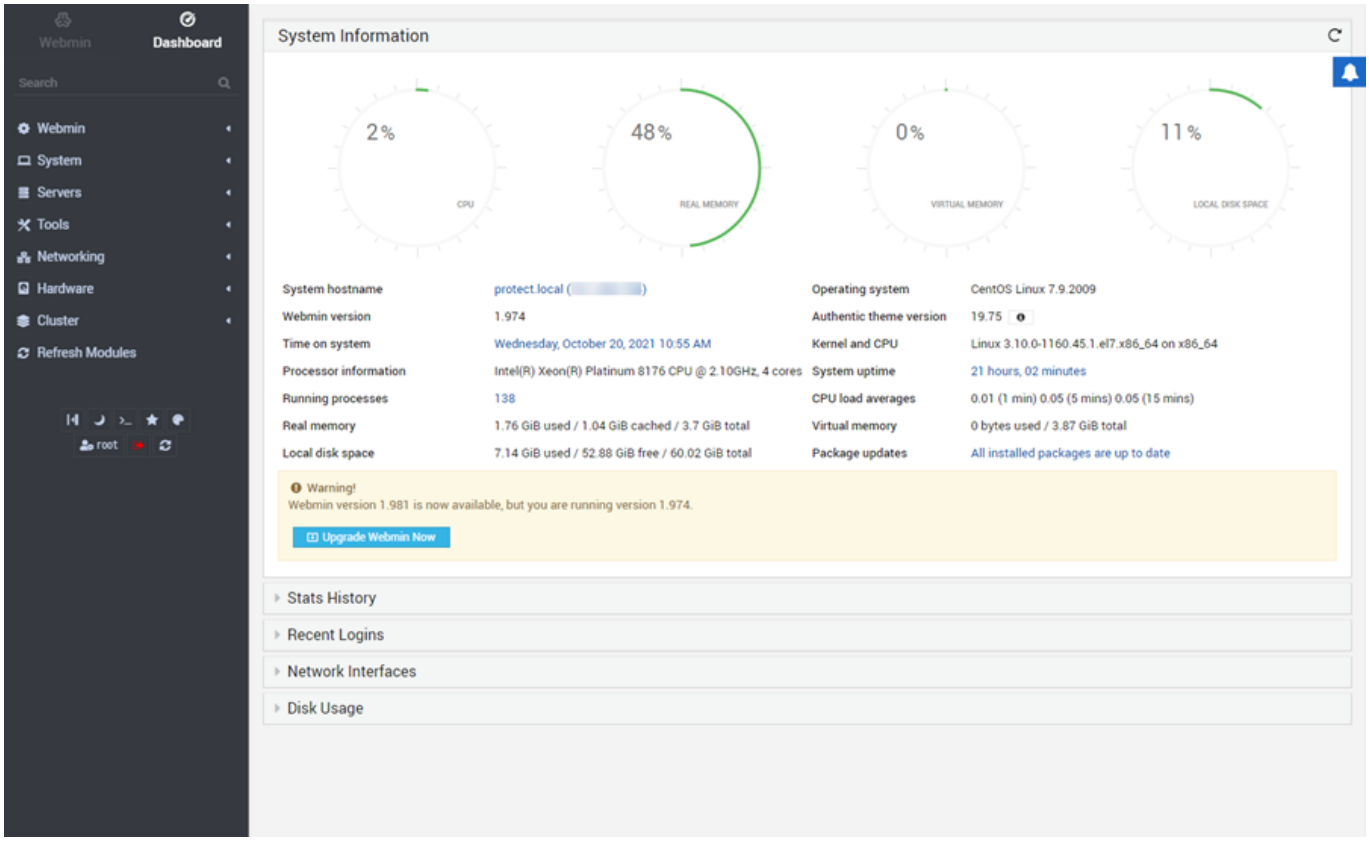
El menú principal incluye las categorías de módulos: **Webmin**, **Sistema**, **Servidores**, **Herramientas**, **Red**, **Hardware** y **Clúster**. Para obtener más información sobre los módulos, consulte las páginas Módulos de Webmin.

Webmin detecta automáticamente la configuración del dispositivo virtual y muestra los módulos correspondientes.

A la hora de administrar el dispositivo virtual de ESET PROTECT, los módulos más importantes son:

- Sistema
- Servidores
- Herramientas
- Red

Webmin funciona con **privilegios root** de Linux completos, lo que significa que puede editar cualquier archivo y ejecutar cualquier comando en el sistema. Es posible que, si comete un error, elimine todos los archivos del sistema o sea imposible arrancarlo. Por este motivo, es importante que tenga cuidado al ejecutar Webmin. Incluso a pesar de que Webmin le suele advertir antes de realizar acciones potencialmente peligrosas, no realice cambios de configuración en aquellos elementos con los que no esté familiarizado.



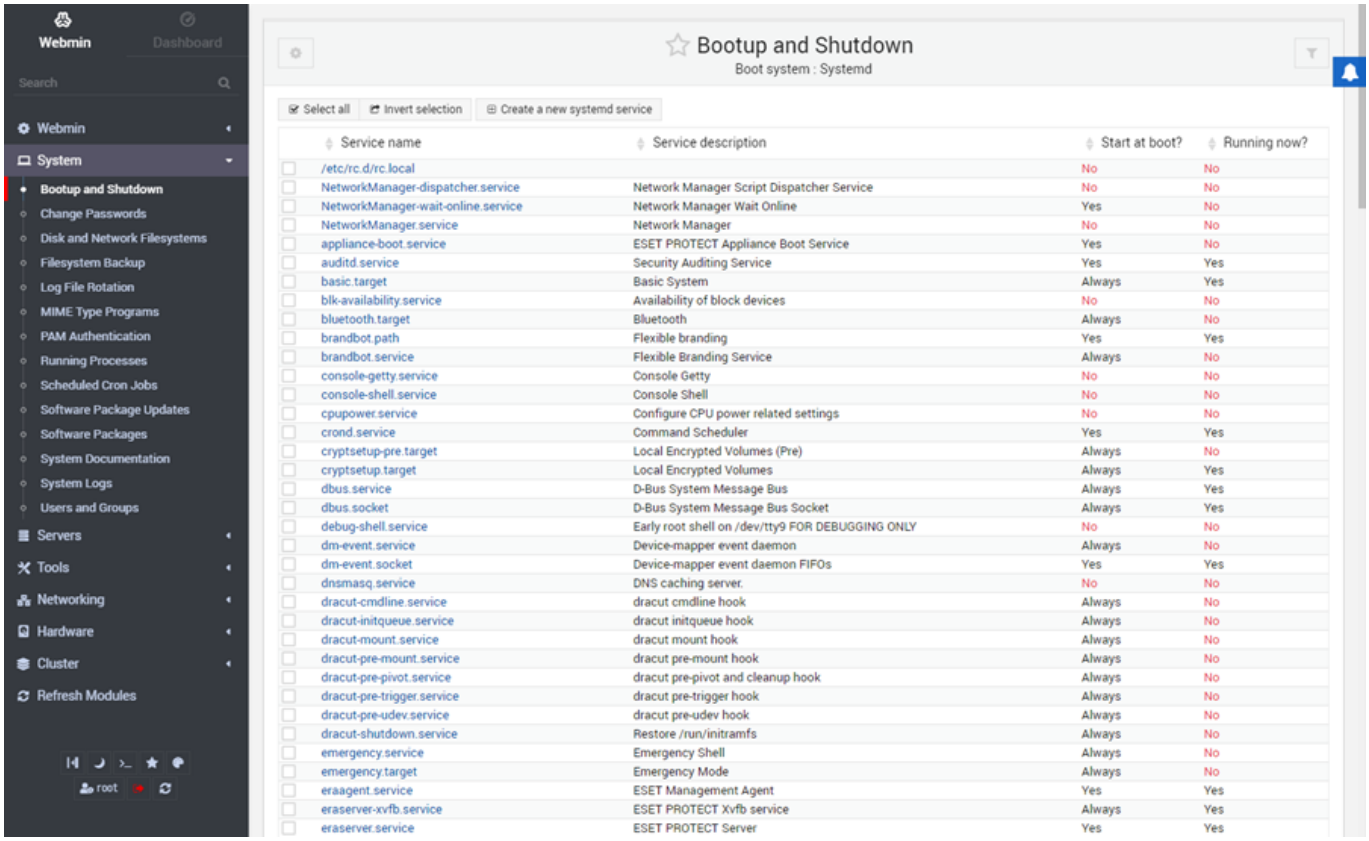
Notificación: si hay algo de lo que Webmin quiere avisarle, se mostrará una notificación en la parte inferior de la Consola.

Cerrar sesión: cuando termine de utilizar Webmin, utilice el icono de cierre de sesión del menú de la izquierda.

Sistema

Desde este apartado puede configurar algunos de los módulos del **Sistema**.

Arranque y desconexión: le permite gestionar los servicios, modificar, iniciar, detener y reiniciar un servicio o varios a la vez. También puede crear y modificar los scripts que se ejecutan en el arranque y en el apagado, etc. Puede **Reiniciar** o **Apagar** la máquina virtual de ESET PROTECT con los botones situados en la parte inferior de la página.



Cambiar contraseñas: le permite cambiar las contraseñas del usuario del sistema operativo de la máquina virtual.

> No utilice esta opción cuando quiera cambiar la contraseña del dispositivo virtual de ESET PROTECT o la base de datos de ESET PROTECT, utilice Cambiar contraseña de la máquina virtual o Cambiar contraseña de la base de datos desde la Consola de administración del dispositivo de máquina virtual de ESET PROTECT.

Procesos en ejecución: puede gestionar todos los procesos que se encuentran en ejecución en el sistema por medio de Webmin. Este módulo se puede usar para ver, cerrar, modificar la prioridad y ejecutar procesos en el sistema.

Actualizaciones del paquete de software: le muestra las actualizaciones disponibles y le permite actualizar todos los paquetes seleccionados o solo algunos.

Registros del sistema: utilice esta opción para ver los archivos de registro del sistema y, si es necesario, cambiar la ubicación en la que se almacenan los mensajes del registro.

Servidores

Desde este apartado puede configurar algunos de los módulos de **Servidores**:

Servidor web Apache: es uno de los módulos más complejos y potentes de Webmin, ya que le permite configurar casi todas y cada una de las funciones de Apache. Puede utilizarlo como servidor HTTP para suministrar archivos de instalación o actualizaciones. Tendrá que configurar el cortafuegos agregando reglas para activar los puertos correspondientes.

> No es igual que el servidor web Apache para la Consola web de ESET PROTECT, pero puede utilizar este servidor web Apache con cualquier otro fin, si es que lo necesita.

ESET PROTECT: este módulo le permite **Ejecutar la herramienta de diagnóstico**, **Restablecer la contraseña de ESET PROTECT Server Administrator**, **Reparar el certificado de ESET PROTECT Server** y la **autoridad de certificación**, **Reparar el certificado de ESET Management Agent** y la **autoridad de certificación**, **Reparar la conexión con ESET Management Agent** o **Editar el archivo Apache Tomcat server.xml** para cambiar los algoritmos de cifrado y los certificados HTTPS de Web Console.

Servidor de bases de datos MySQL: le permite gestionar los permisos de usuario, cambiar la contraseña o ver el contenido de la base de datos.

> No utilice el servidor de bases de datos MySQL para realizar copias de seguridad o restauraciones de la base de datos de ESET PROTECT, utilice la Consola de administración del dispositivo virtual de ESET PROTECT. Consulte Copia de seguridad de la base de datos para obtener información detallada.

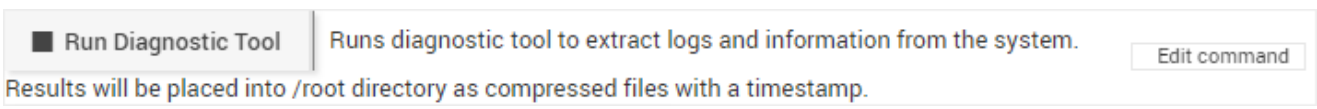
Compartir archivos en Windows con Samba: le permite especificar los directorios que desea compartir con clientes Windows mediante el protocolo SMB (Bloque de mensajes del servidor). Puede configurar Samba para que los archivos del dispositivo virtual de ESET PROTECT estén disponibles para los clientes de Windows, en caso de ser necesario. También puede configurar y unirse a un dominio de Windows. Si los recursos compartidos están activados, deberán activarse también los puertos de Samba en el cortafuegos.

Servidor SSH: este módulo se utiliza para configurar los servidores de SSH y OpenSSH, y presupone que tiene un conocimiento básico de los programas cliente a nivel usuario. Puede configurar SSH Server y los clientes en su sistema.

ESET PROTECT

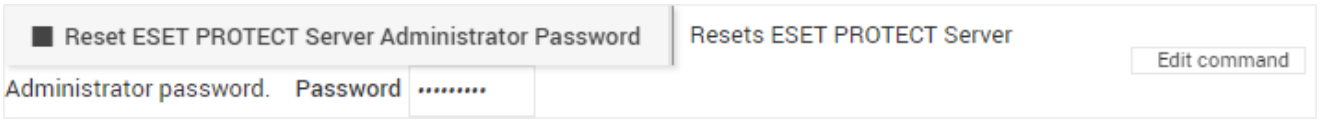
El módulo **ESET PROTECT** le permite ejecutar determinados comandos predefinidos, principalmente para reparar los certificados de ESET PROTECT, ejecutar una herramienta de diagnóstico o restablecer la contraseña de ESET PROTECT Server.

Run Diagnostic Tool: haga clic en el botón para extraer los registros y la información del sistema. Se exportarán los registros de ESET PROTECT Server y ESET Management Agent. Puede utilizar el módulo Gestor de archivos para encontrar y descargar los archivos de registro de diagnóstico exportados comprimidos en formato *.zip*.

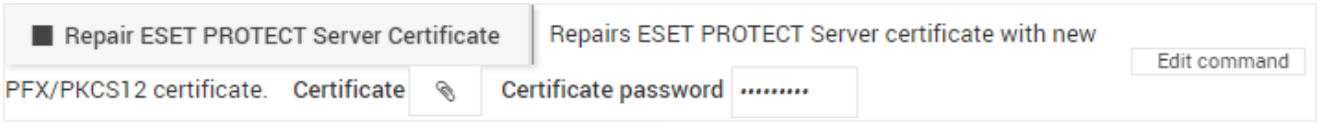


Reset ESET PROTECT Server Administrator Password : si ha olvidado la contraseña de ESET PROTECT Server o

simplemente quiere restablecer la contraseña, introduzca la nueva contraseña de la cuenta de ESET PROTECT Server Administrator y pulse el botón para ejecutar el comando.

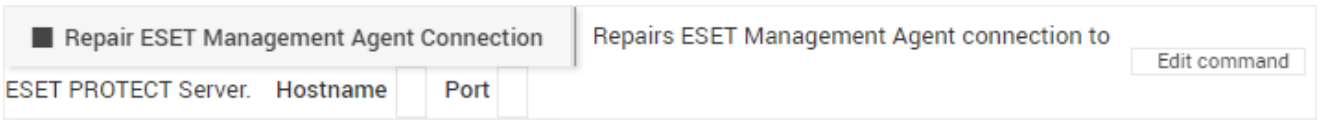


Repair ESET PROTECT Server Certificate: repara el certificado de ESET PROTECT Server con el nuevo certificado PFX/PKCS12. Haga clic en el icono del **clip de papel** y examine para acceder al archivo de certificado PFX o PKCS12 de ESET PROTECT Server y, a continuación, haga clic en **Abrir**. Introduzca la contraseña del certificado de ESET PROTECT Server y pulse el botón para ejecutar el comando.



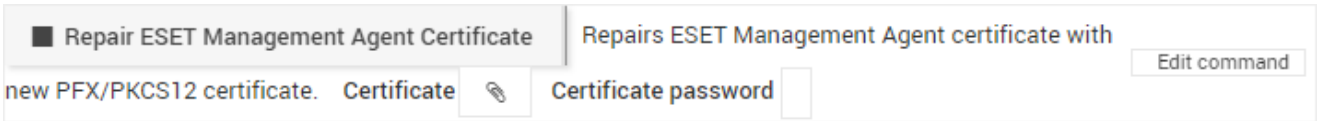
Repair ESET PROTECT Server Certification Authority: repara la autoridad de certificación de ESET PROTECT Server con el certificado DER. Haga clic en el icono del **clip de papel** y examine para acceder al archivo de certificado *.der* de la autoridad de certificación y, a continuación, haga clic en **Abrir**.

Repair ESET Management Agent Connection: repara la conexión de ESET Management Agent con ESET PROTECT Server. Escriba el **Nombre de host** y el número de **puerto** de ESET PROTECT Server y, a continuación, pulse el botón para ejecutar el comando.

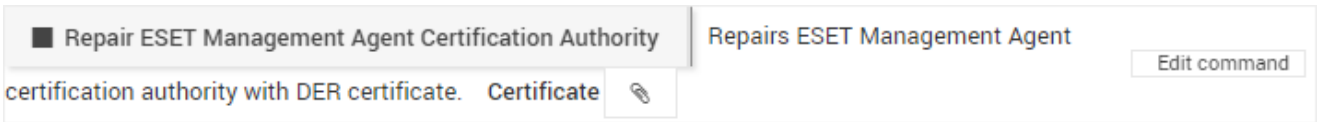


Repair ESET Management Agent Certificate: repara el certificado de ESET Management Agent con el nuevo certificado PFX/PKCS12. Haga clic en el icono del **clip de papel** y examine para acceder al archivo de certificado *PFX* o *PKCS12* de ESET Management Agent y, a continuación, haga clic en **Abrir**. Introduzca la contraseña del certificado de ESET Management Agent y pulse el botón para ejecutar el comando.

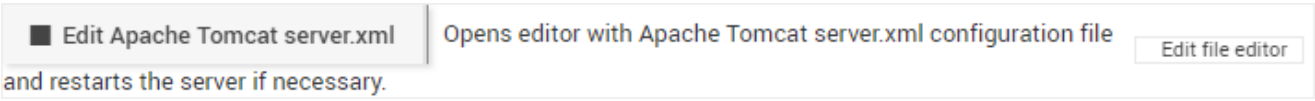
La frase de contraseña del certificado no puede contener los siguientes caracteres: " \ Estos caracteres provocan errores críticos durante la inicialización del agente.



Repair ESET Management Agent Certification Authority: repara la autoridad de certificación de ESET Management Agent con el nuevo certificado DER. Haga clic en el icono del **clip de papel** y examine para acceder al archivo de certificado *.der* de la autoridad de certificación y, a continuación, haga clic en **Abrir**.



Edit Apache Tomcat server.xml: puede modificar el archivo de configuración de Apache Tomcat server.xml para cambiar los algoritmos de cifrado y los certificados HTTPS de Web Console. Cuando pulse el botón, se abrirá un editor de texto con el que podrá modificar el archivo `/etc/tomcat/server.xml`. Haga clic en el botón **Guardar** para guardar los cambios. En caso de ser necesario reiniciar, se reiniciará automáticamente. Si no desea guardar los cambios realizados, haga clic en **Volver a los comandos**.



Herramientas

Esta categoría de Webmin contiene distintos módulos. Hay dos módulos muy útiles:

Gestor de archivos: le permite ver y manipular los archivos del servidor mediante una interfaz HTML. La primera vez que cargue el Gestor de archivos (también conocido como **Filemin**) se mostrará el contenido del directorio raíz del dispositivo virtual de ESET PROTECT, en función del usuario con el que haya iniciado sesión.

- La navegación por la estructura de directorios es muy sencilla, solo tendrá que hacer clic en el nombre del directorio o en su icono (carpeta). Verá el directorio actual en la sección superior izquierda de la ventana de Filemin ; haga clic en cualquier parte de la ruta de acceso para mostrar el contenido del directorio en cuestión.

- Filemin también puede utilizarse para buscar archivos, haga clic en **Herramientas** en la barra de herramientas (en la esquina superior derecha de la ventana de Filemin) y seleccione **Buscar**. En el campo **Consulta de búsqueda**, introduzca un patrón de búsqueda para realizar la búsqueda.

- Si desea descargar un archivo del dispositivo virtual de ESET PROTECT en el ordenador en el que se ejecuta el navegador web, haga clic en el nombre del archivo o en su icono.

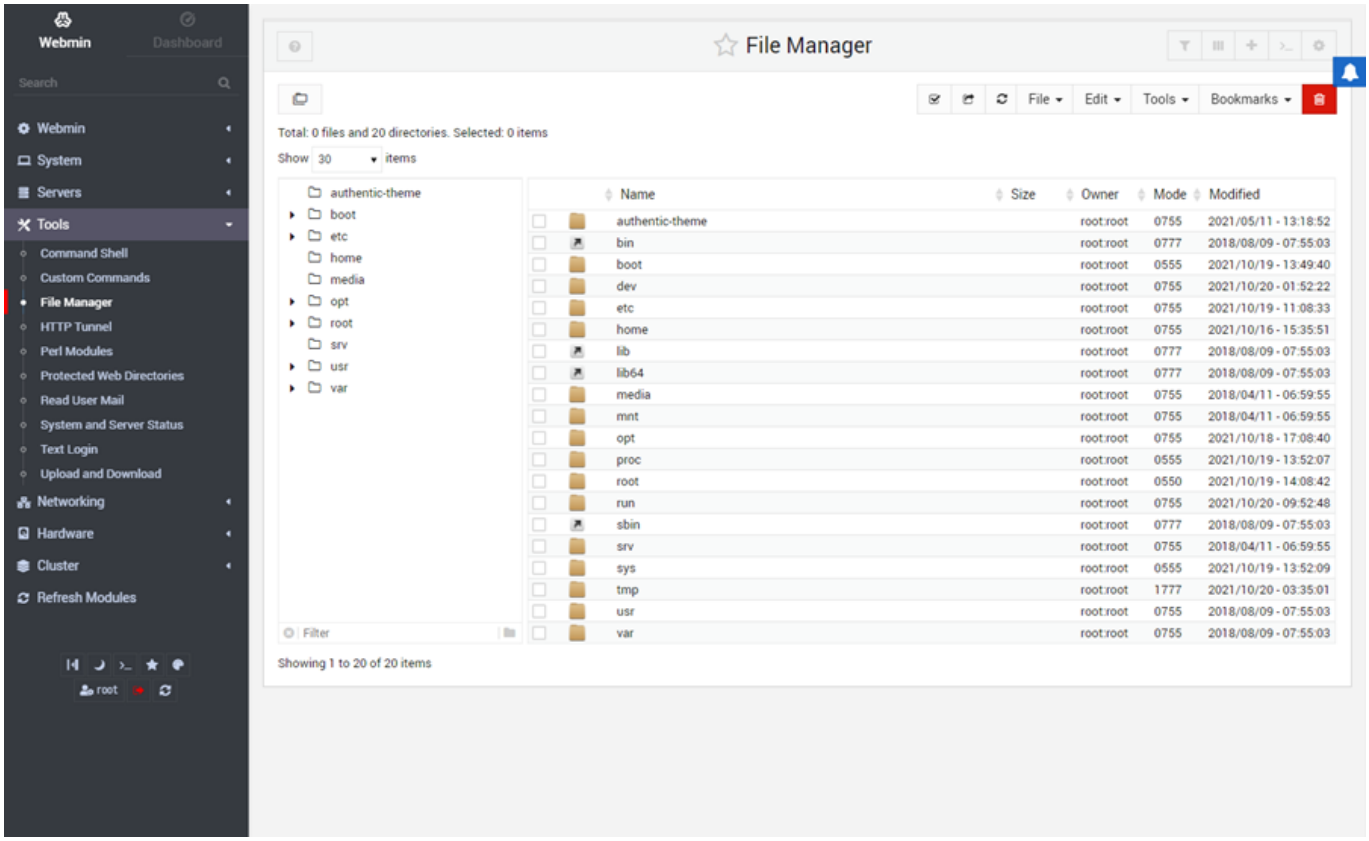
- Si desea cargar un archivo desde el ordenador en el que se está ejecutando el navegador web, haga clic en **Archivo** y, a continuación, en **Cargar en el directorio actual**. Se abrirá un cuadro de diálogo; haga clic en el icono del clip de papel para examinar los archivos que desea cargar. Puede seleccionar varios archivos y cargarlos haciendo clic en el botón **Cargar archivos**. Los archivos cargados se almacenarán en el directorio actual. Una vez completado el proceso de carga, la lista de directorios se actualizará y verá los archivos que ha cargado.

- También puede recuperar un archivo de una URL remota. Para ello, haga clic en **Archivo** y seleccione **Obtener desde URL**.

- Podrá mostrar y editar el contenido de cualquier archivo de su sistema haciendo clic en el icono **Editar** de la columna **Acciones**.

- Para crear un archivo de texto vacío nuevo, haga clic en **Archivo**, **Crear nuevo archivo** y escriba el nombre del archivo nuevo.

- Para cambiar el nombre de un archivo o un directorio, haga clic en el icono de **Cambiar nombre** del menú contextual que aparece al hacer clic con el botón derecho del ratón.



Cargar y descargar: es otro módulo útil de Webmin en la categoría **Herramientas**. Le permite realizar tres acciones con archivos distintas:

- **Descargar de Internet**: introduzca las URL de los archivos que desea descargar de Internet en el dispositivo virtual de ESET PROTECT y especifique la ubicación en la que desea almacenar los archivos.
- **Cargar en el servidor**: haga clic en el icono del clip de papel para examinar los archivos que desea cargar; puede cargar hasta cuatro archivos a la vez. Especifique la ubicación en la que desea almacenar los archivos.
- **Descargar del servidor**: especifique la ruta de acceso, incluido el nombre del archivo, en el campo de texto **Archivo para descargar**, o haga clic en el icono que aparece junto a él para examinar el sistema de archivos del dispositivo virtual de ESET PROTECT y elegir el archivo que desea descargar en el ordenador en el que se está ejecutando el navegador web. Haga clic en el botón **Descargar** para empezar a descargar el archivo; puede descargar los archivos de uno en uno.

Red

En la mayoría de las ocasiones no tendrá que modificar la configuración de la red, pero si se ve obligado a hacerlo, puede hacerlo desde la categoría **Red**. Desde este apartado puede configurar algunos de los módulos útiles:

Configuración de Kerberos5: es necesario tener los partes de Kerberos correctamente configurados para que se produzca la sincronización con Active Directory. Puede ejecutar Unirse de nuevo al dominio cuando los partes de Kerberos estén configurados.

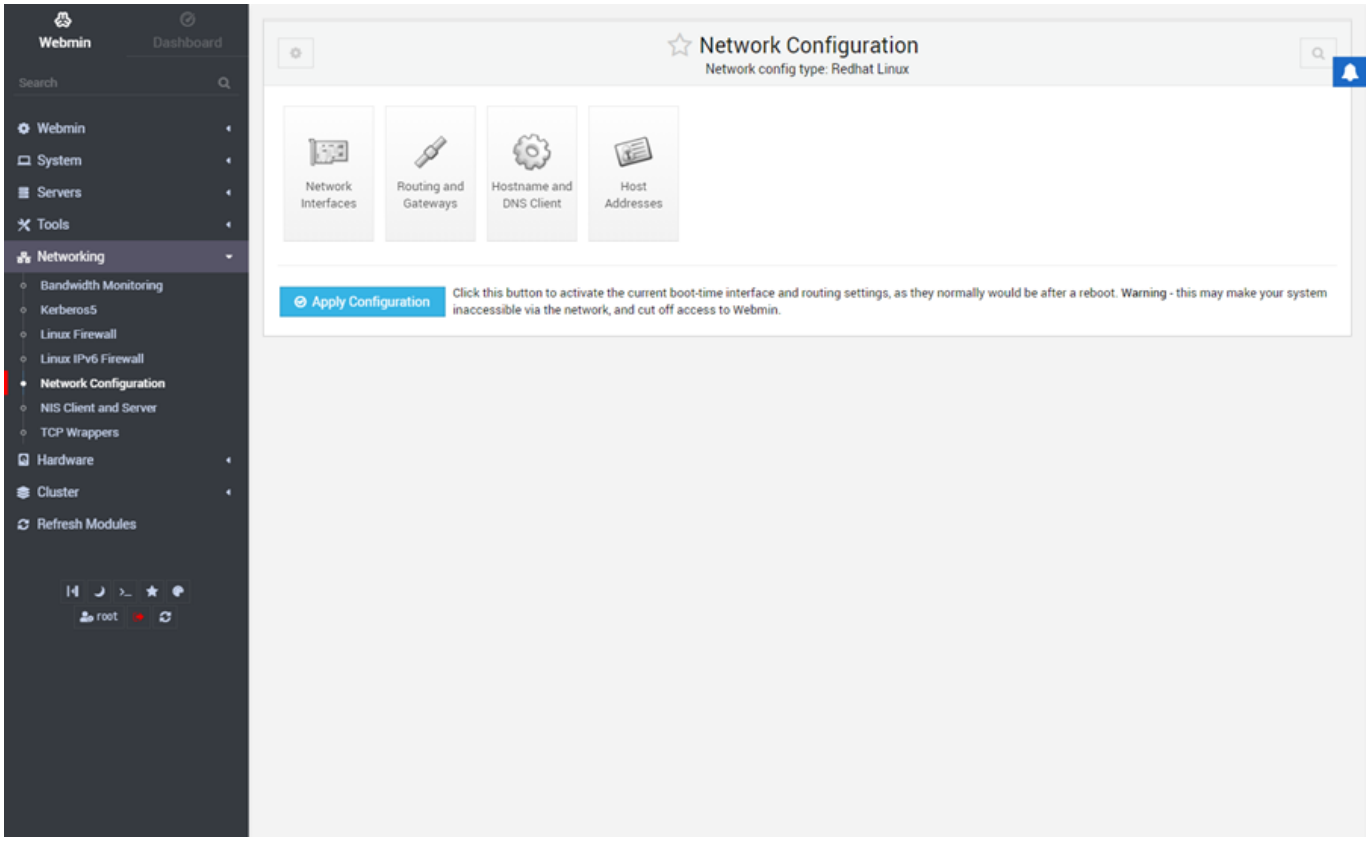
Cortafuegos Linux: cortafuegos basado en IPtables. Si necesita permitir puertos, puede hacerlo aquí agregando algunas reglas o modificando las ya existentes.

Configuración de la red: permite configurar el adaptador de red, cambiar la dirección IP, el nombre de host, el

DNS y otros ajustes de la red.

Cuando haya terminado de configurar el sistema, pulse el botón **Aplicar configuración** para que los cambios entren en vigor.

Estas opciones están destinadas exclusivamente a administradores avanzados. Si la configuración de red no es correcta, puede que el sistema quede inaccesible a través de la red e impedir el acceso a Webmin. Sin embargo, podrá acceder a la Consola de administración del dispositivo virtual de ESET PROTECT desde la ventana de terminal de la máquina virtual.



Certificados de ESET PROTECT

Los certificados de ESET PROTECT son necesarios para implementar los tipos de dispositivo ESET PROTECT MDM ESET PROTECT.

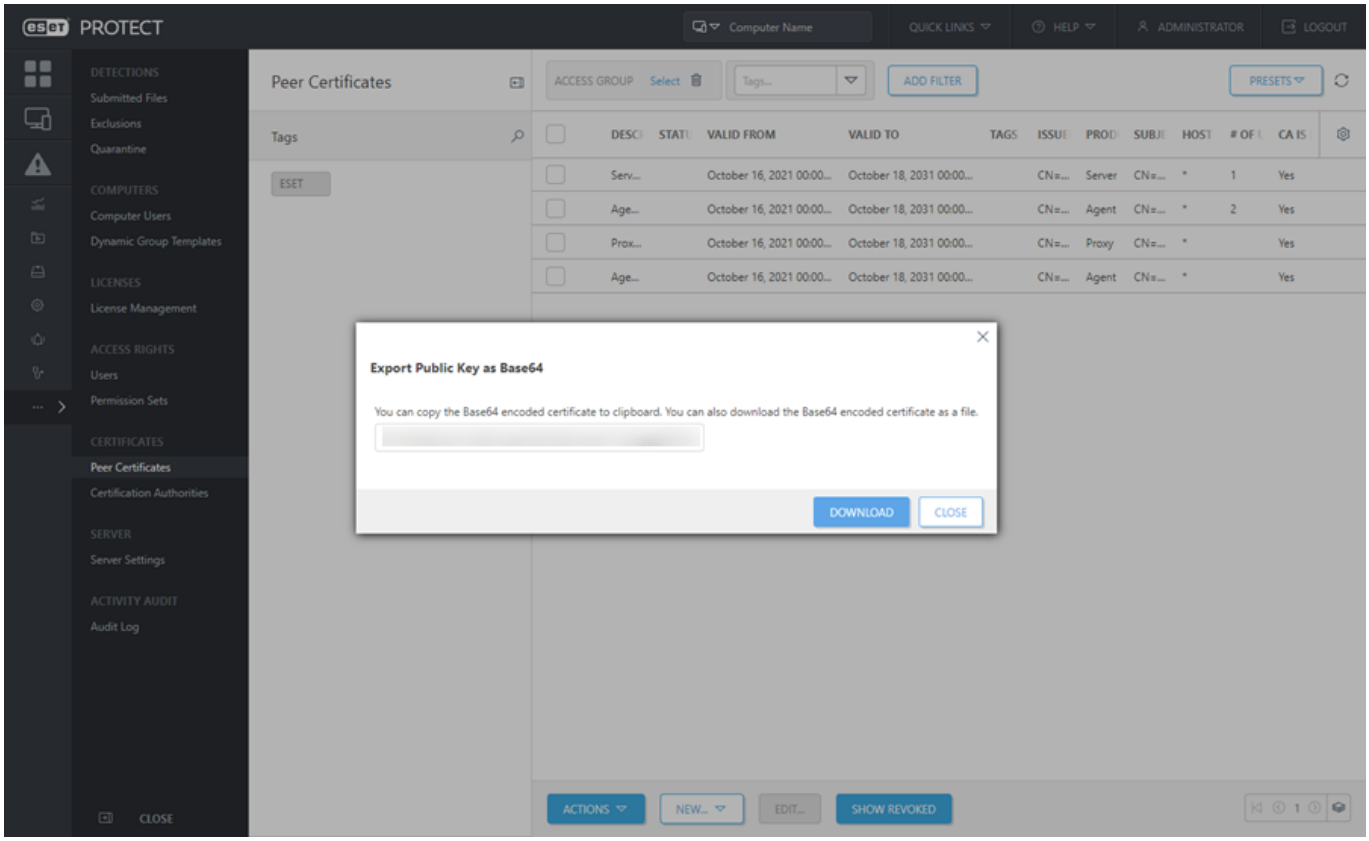
Los certificados de los componentes de ESET PROTECT están disponibles en Web Console.

Para copiar el contenido de un certificado en formato Base64:

1. Haga clic en **Más** > **Certificados de iguales**.

2. Seleccione un certificado y, a continuación, seleccione Exportar como Base64. Puede descargar también el certificado con codificación Base64 como un archivo.

Repita este paso con los certificados de otros componentes, y con su autoridad certificadora.



Para exportar un certificado, un usuario debe tener derechos de **Uso** de **Certificados**. Consulte la lista completa de derechos de acceso para obtener más información.

Actualización o migración del dispositivo virtual de ESET PROTECT

Para actualizar o migrar el dispositivo virtual, puede realizar las siguientes acciones:

- **Actualizar**: instala una versión más reciente de los componentes de ESET PROTECT.
- **Migración**: mueve el dispositivo virtual de ESET PROTECT a otra instancia de la misma versión.
- **Migración y actualización**: mueve el dispositivo virtual de ESET PROTECT a otra instancia de una versión superior.

Una nueva implementación del dispositivo virtual de ESET PROTECT 8.1 y versiones posteriores tiene la seguridad avanzada activada de forma predeterminada. Si utiliza ESMC o el dispositivo virtual de ESET PROTECT 8.0 con la seguridad avanzada desactivada y actualiza al dispositivo virtual de ESET PROTECT 8.1 y versiones posteriores, la seguridad avanzada permanecerá desactivada.

Antes de la actualización o migración

Realice una copia de seguridad de su base de datos y exporte la autoridad certificadora y los certificados de igual del dispositivo virtual de ESMC/ESET PROTECT antiguo antes de migrar o actualizar la instancia de ESET PROTECT.

Recuperación de la base de datos frente a la actualización de componentes

Hay dos formas principales de actualizar el dispositivo virtual:

- Usar la recuperación de la base de datos: actualiza todo el dispositivo (el sistema operativo subyacente), no solo ESET PROTECT Server. El proceso es más complicado y requiere tener dos dispositivos simultáneos durante el periodo de transición. Se recomienda utilizar la recuperación de la base de datos para actualizar a las versiones principales o como método de resolución de problemas.

- Actualización mediante la tarea actualización Ade componentes en Web Console: el proceso es más sencillo y no requiere acceso al dispositivo, sino solo a Web Console. Recomendamos este procedimiento para actualizaciones leves y de correcciones de errores.

Proceso de migración y actualización (método de actualización recomendado)

Utilice las siguientes instrucciones para migrar y actualizar el dispositivo virtual de ESET PROTECT.

1.Descargue la versión más reciente de *protect_appliance.ova (*o `protect_appliance.vhd.zip` si usa Microsoft Hyper-V).

2.Implemente el nuevo dispositivo virtual de ESET PROTECT. Consulte Proceso de implementación del dispositivo de ESET PROTECT para ver las instrucciones. **No configure** aún el nuevo dispositivo virtual de ESET PROTECT a través de su interfaz web.

3.Recupere la base de datos del dispositivo virtual antiguo. Consulte Recuperar la base de datos de otro servidor para ver una guía paso a paso completa.

No desinstale ni quite aún su antiguo VA Server.

4.Configure su nuevo dispositivo virtual de ESET PROTECT a través de su interfaz web.

5.Verificar de que el nuevo dispositivo virtual de ESET PROTECT se comporta de la misma forma que el antiguo,

oSi el nuevo dispositivo virtual de ESET PROTECT tiene una **dirección IP distinta**:

a)Cree una nueva política en su dispositivo virtual para establecer una nueva dirección IP para ESET PROTECT Server y asignarla a todos los ordenadores.

b)Espere a que la política se distribuya a todas las instancias de ESET Management Agent.

c)Asegúrese de que todos los ordenadores estén conectados al nuevo dispositivo virtual de ESET PROTECT.

d)Apague y retire el dispositivo virtual antiguo.

Le recomendamos encarecidamente que no desinstale el antiguo dispositivo virtual de ESET PROTECT Server mediante un script de desinstalación. Este procedimiento de desinstalación disociará (quitará) todas las licencias de la nueva base de datos del dispositivo virtual de ESET PROTECT Server. Para evitar este comportamiento, elimine la base de datos del antiguo dispositivo virtual de ESET PROTECT Server (`DROP DATABASE`) antes de desinstalar.

oSi el nuevo dispositivo virtual de ESET PROTECT tiene la **misma dirección IP**:

Asegúrese de que la configuración de red de su nuevo ESET PROTECT Server (dirección IP, FQDN, nombre del ordenador, registro SRV de DNS) coincida con la de su antiguo VA Server. También puede usar el nombre de cliente si cambia el registro de DNS para que apunte al servidor nuevo.

a)Apague el dispositivo virtual antiguo.

b)Encienda el dispositivo virtual de ESET PROTECT nuevo.

c)Asegúrese de que todos los ordenadores estén conectados al nuevo dispositivo virtual de ESET PROTECT.

d)Retire el dispositivo virtual antiguo.

Le recomendamos encarecidamente que no desinstale el antiguo dispositivo virtual de ESET PROTECT Server mediante un script de desinstalación. Este procedimiento de desinstalación disociará (quitará) todas las licencias de la nueva base de datos del dispositivo virtual de ESET PROTECT Server. Para evitar este comportamiento, elimine la base de datos del antiguo dispositivo virtual de ESET PROTECT Server (`DROP DATABASE`) antes de desinstalar.

6.Actualice un grupo de ejemplo de ESET Management Agent mediante una ESET PROTECTtarea de Actualización de componentes.

7.Si la actualización del grupo de ejemplo se realiza correctamente y los agentes siguen conectándose, continúe con el resto de agentes.

Proceso de actualización (método de actualización alternativo)

La actualización de ESMC o versiones antiguas de ESET PROTECT a la versión más reciente de ESET PROTECT en el mismo dispositivo virtual no actualiza otro software del dispositivo virtual (sistema operativo, paquetes necesarios para el correcto funcionamiento de ESET PROTECT Server). Se recomienda migrar el servidor tras realizar la tarea de actualización en sí.

Actualice el dispositivo virtual mediante una tarea de Actualización de componentes:

1.Actualice primero el ESET PROTECT Server.

2.Actualice un grupo de ejemplo de ESET Management Agent.

3.Si la actualización del grupo de ejemplo se realiza correctamente y los agentes siguen conectándose, continúe con el resto de agentes.

Recuperación ante desastres del dispositivo virtual de ESET PROTECT

Si se produce la desafortunada situación de que el dispositivo virtual de ESET PROTECT resulta dañado y no puede iniciarlo de nuevo, o incluso se elimina del almacenamiento o se destruye por cualquier otro motivo, puede seguir

el procedimiento de recuperación ante desastres.

> Es necesario tener una copia de seguridad de la base de datos del dispositivo virtual de ESET PROTECT para que la recuperación se realice correctamente.

1. **Descargue** la versión más reciente de *protect_appliance.ova* o `protect_appliance.vhd.zip` si usa Microsoft Hyper-V. La ventaja de este procedimiento de recuperación es que su dispositivo virtual de ESET PROTECT estará actualizado.

2. **Implemente un dispositivo virtual de ESET PROTECTnuevo**, pero no lo configure todavía. Consulte Proceso de implementación del dispositivo de ESET PROTECT para ver las instrucciones.

3. **Active Webmin** para poder cargar el archivo de copia de seguridad de MySQL; para obtener información de activación detallada, consulte el apartado Activar o desactivar el acceso remoto.

4. **Restaure la base de datos** a partir del archivo de copia de seguridad más reciente que tenga; siga los pasos descritos en el apartado Restaurar la base de datos.

5. **Configure** el dispositivo virtual de ESET PROTECT que acaba de implementar con la base de datos restaurada de la misma forma que el dispositivo virtual anterior; consulte Configuración del dispositivo virtual de ESET PROTECT para obtener más información.

Resolución de problemas

Los siguientes archivos de registro se pueden utilizar para resolver los problemas del dispositivo virtual de ESET PROTECT. También es posible que el personal de soporte técnico de ESET le solicite registros de diagnóstico. Estos son los archivos de registro que puede enviar para su análisis:

Nombre del registro	Ubicación	Descripción
Configuración del dispositivo virtual de ESET PROTECT	*/root/appliance-configuration-log.txt*	Si la implementación del dispositivo virtual de ESET PROTECT falla, no reinicie el dispositivo y revise el archivo de registro de configuración.
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log* */var/log/eset/RogueDetectionSensor/RDSensorInstaller.log*	Archivo de registro de instalación de ESET PROTECT Server Otros componentes de ESET PROTECT utilizan una ruta de acceso similar y el nombre de archivo correspondiente.
Registro de seguimiento de ESET PROTECT Server Registro de seguimiento de ESET Management Agent	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/Agent/*	Revise los registros de seguimiento: *trace.log* *status.html* *last-error.html* Otros componentes de ESET PROTECT utilizan una ruta de acceso y nombres de archivo similares.

Nombre del registro	Ubicación	Descripción
Proxy HTTP Apache	*/opt/apache/logs/* */var/log/httpd*	Archivo de registro de versiones anteriores del dispositivo virtual de ESET PROTECT Archivo de registro de versiones posteriores del dispositivo virtual de ESET PROTECT
Volcados de memoria de ESET PROTECT Server	*/var/opt/eset/RemoteAdministrator/Server/Dumps/*	
Herramienta de diagnóstico de ejecución de ESET PROTECT Server o ESET Management Agent	*/root/RemoteAdministratorAgentDiagnostic.zip*	Si tiene problemas con el dispositivo virtual de ESET PROTECT, puede **Ejecutar la herramienta de diagnóstico**. Consulte el módulo Webmin de ESET PROTECT para obtener más información.

Si el servidor o el agente se bloquean y no puede cambiar el nivel de detalle del registro a través de la Consola web, puede activar el registro de seguimiento completo creando el archivo vacío:

Para el agente:

```
touch /var/log/eset/RemoteAdministrator/Agent/traceAll
```

Para el servidor:

```
touch /var/log/eset/RemoteAdministrator/Server/traceAll
```

Se recomienda utilizar el gestor de archivos de Webmin, con el que podrá buscar archivos fácilmente y descargar los registros en caso de ser necesario.

Preguntas frecuentes sobre el dispositivo virtual de ESET PROTECT

Este capítulo abarca algunas de las preguntas más frecuentes y los problemas encontrados. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- Cómo saber qué componentes de ESET PROTECT hay instalados
- Cómo activar el ping en el dispositivo virtual de ESET PROTECT
- ¿Tengo que añadir otros componentes al dispositivo virtual de ESET PROTECT?
- Cómo activar el proxy HTTP Apache en mi dispositivo virtual de ESET PROTECT después de la configuración inicial

- Cómo configurar LDAP para que permita la sincronización del grupo estático en el dispositivo virtual de ESET PROTECT
- Configurar la conexión LDAPS con un dominio
- Cómo recuperar una contraseña olvidada del dispositivo virtual de ESET PROTECT
- Cómo cambiar la cadena de conexión a la base de datos de ESET PROTECT
- Cómo configurar Hyper-V Server para el Sensor RD
- Cómo cambiar los números de puerto del dispositivo virtual de ESET PROTECT
- Cómo aumentar el tamaño de la memoria para MySQL Server
- Error con ESET PROTECT al ejecutarlo en Hyper-V Server 2012 R2
- Cómo mejorar el rendimiento de Oracle VirtualBox
- Cómo activar el comando YUM en el servidor proxy HTTP
- Cómo actualizar el sistema operativo de un ordenador que ejecute el servidor del dispositivo virtual de ESET PROTECT
- Cómo desactivar SELinux de forma permanente
- Cómo reiniciar la consola de administración del dispositivo virtual
- Cómo utilizar el proxy para las conexiones de los agentes
- Cómo activar SSH

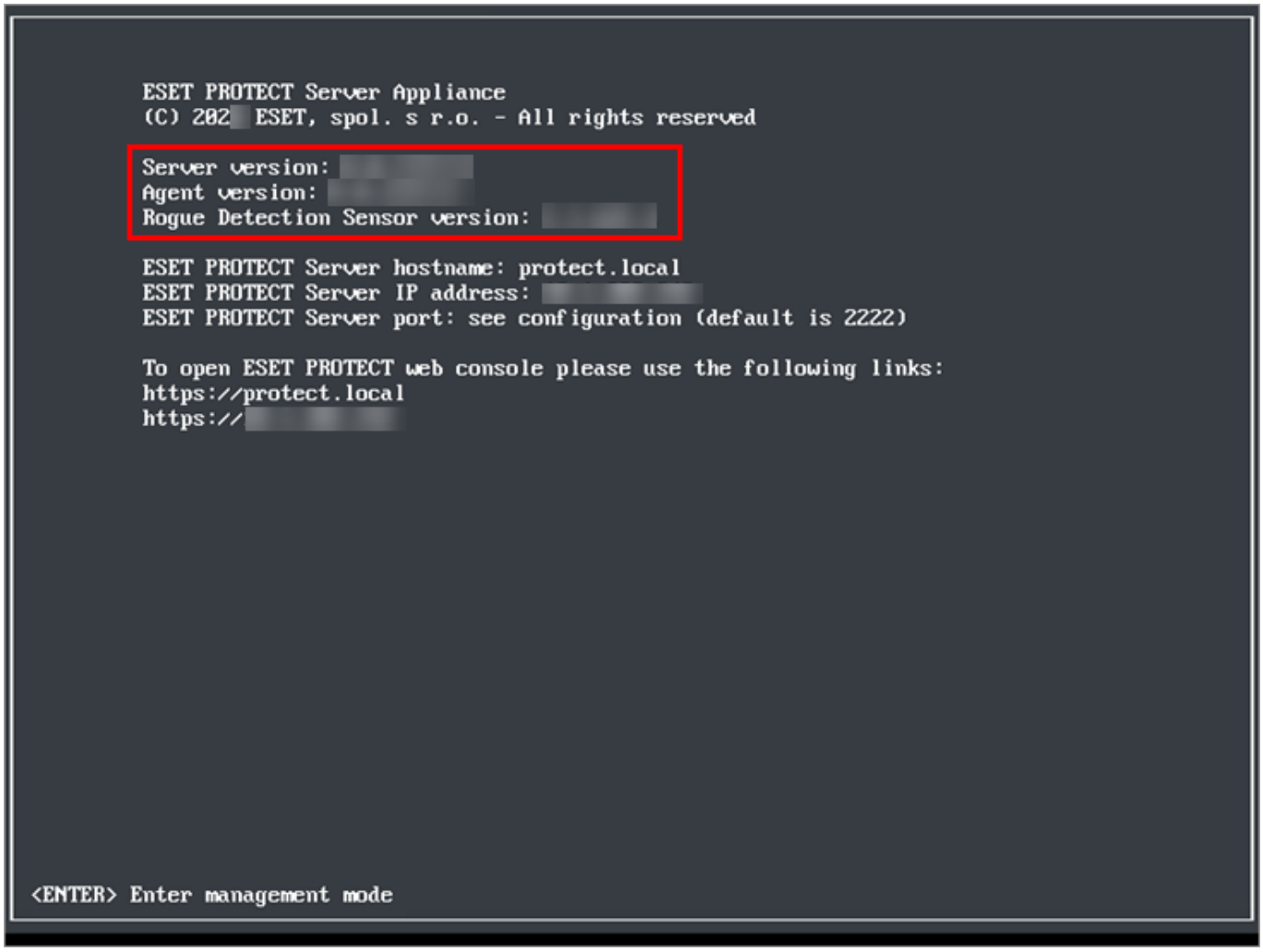
Si no encuentra su problema en las páginas de ayuda anteriores, utilice una palabra clave o frase que describa el problema para realizar la búsqueda en las páginas de ayuda de ESET PROTECT.

Si no encuentra la solución a su problema o consulta en las páginas de ayuda, puede probar con nuestra base de datos de conocimientos en línea, que se actualiza periódicamente.

Si es necesario, puede ponerse en contacto directamente con nuestro centro de soporte técnico en línea para comunicarle sus consultas o problemas. Puede acceder al formulario de contacto desde Web Console de ESET PROTECT > **Ayuda** > **Contactar con el servicio de atención al cliente**.

Cómo saber qué componentes de ESET PROTECT hay instalados

Encontrará una lista de los componentes de ESET PROTECT y sus versiones en la ventana de la consola de su dispositivo virtual de ESET PROTECT. Si desea actualizar este cuadro de diálogo tras la actualización del componente, puede reiniciar el dispositivo virtual. Otra opción es acceder al modo de administración y seleccionar **Exit to terminal**, para después salir de la ventana de terminal y volver a la pantalla de bloqueo.



Cómo activar el ping en el dispositivo virtual de ESET PROTECT

Abra una ventana de terminal y ejecute los siguientes comandos como usuario root para permitir realizar ping en un equipo dispositivo virtual de ESET PROTECT.

Antes de comenzar, compruebe qué versión de CentOS se está ejecutando en el sistema con el comando `hostnamectl`. A continuación, ejecute los siguientes comandos en función de su versión del sistema operativo.

Para CentOS 7

1. Llame al comando iptables:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

2. Guarde iptables:

```
service iptables save
```

Ahora se puede hacer ping al dispositivo virtual de ESET PROTECT desde otros ordenadores situados en la misma subred.

¿Tengo que añadir otros componentes al dispositivo virtual de ESET PROTECT?

No, el dispositivo virtual de ESET PROTECT funciona con la configuración predeterminada. Solo tendrá que implementar el dispositivo y configurarlo. Es, con mucha diferencia, la forma más sencilla de implementar ESET PROTECT, siempre que utilice un hipervisor compatible.

Cómo activar el proxy HTTP Apache en mi dispositivo virtual de ESET PROTECT después de la configuración inicial

El proxy HTTP Apache se utiliza principalmente para almacenar en caché los archivos de actualización del motor de detección e información de ESET LiveGrid®. Abra una ventana del terminal y, según la versión de su sistema operativo, ejecute los siguientes comandos como usuario root para activar el proxy HTTP Apache:

i
- La ubicación de `apachectl` y `htcacheclean` variará dependiendo de su sistema: compruébelo antes de ejecutar el script.
- El parámetro `/var/cache/httpd/proxy` determina la ubicación de la carpeta de almacenamiento en caché; esta ubicación se define en `/etc/httpd/conf.d/proxy.conf`, en `CacheRoot`.

Para CentOS 7

```
1.  systemctl enable httpd

2.  sudo mkdir -p /etc/systemd/system/httpd.service.requires

3.  sudo ln -
s /usr/lib/systemd/system/htcacheclean.service /etc/systemd/system/httpd.service.req
uires

4.  systemctl start httpd

5.  htcacheclean -d60 -t -i -p/var/cache/httpd/proxy -l10000M
```

i Puede ajustar parámetros para la desinfección de la memoria caché del proxy HTTP Apache: `-d` define el intervalo de desinfección en minutos, `-p` especifica la ruta como directorio raíz de la memoria caché del disco, `-t` elimina todos los directorios vacíos, `-i` elimina de forma inteligente la memoria caché solo cuando se modificó la memoria caché del disco, mientras que `-l` define el límite del tamaño total de la memoria caché del disco.

```
6.  iptables -A INPUT -p tcp --dport 3128 -j ACCEPT

7.  ip6tables -A INPUT -p tcp --dport 3128 -j ACCEPT

8.  service iptables save

9.  service ip6tables save
```

Así se iniciará el proxy HTTP Apache y se activará el puerto 3128 en un cortafuegos. Tendrá que crear políticas

para que todos los productos de ESET o componentes de ESET PROTECT se comuniquen a través del proxy HTTP Apache y permitir el almacenamiento en caché de los archivos de instalación o actualización de los productos de ESET. Asegúrese de que la configuración de Apache contiene el segmento ProxyMatch del host del servidor. Para obtener más información, consulte el artículo de nuestra base de conocimientos, parte **II. Configurar los ajustes de políticas de los ordenadores cliente**.

Cómo configurar LDAP para que permita la sincronización del grupo estático en el dispositivo virtual de ESET PROTECT

Si la operación de unión al dominio falla, el problema suele ser una configuración incorrecta del dispositivo virtual de ESET PROTECT; para obtener más información, consulte el artículo de nuestra base de conocimiento.

Configurar la conexión LDAPS con un dominio

ESET PROTECT Server en Windows utiliza el protocolo cifrado LDAPS (LDAP a través de SSL) de forma predeterminada para todas las conexiones de Active Directory.

Siga los pasos indicados a continuación para configurar el dispositivo virtual de ESET PROTECT para que se conecte a Active Directory a través de LDAPS.

Requisitos previos

- Configurar LDAPS en el controlador de dominio: asegúrese de exportar la clave pública de la autoridad certificadora de DC.
- Asegúrese de que Kerberos esté correctamente configurado en el dispositivo virtual de ESET PROTECT.

Activar LDAPS en el dispositivo virtual de ESET PROTECT

1. Abra la ventana de terminal de la máquina virtual que contiene el dispositivo virtual de ESET PROTECT.
2. Escriba la contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT y pulse **Entrar** dos veces.
3. Seleccione **Salir a terminal** y pulse **Entrar**.
4. Detenga el servicio ESET PROTECT Server.

```
systemctl stop eraserver
```

5. Escribir el siguiente comando:

```
nano /etc/systemd/system/eraserver.service
```

6. Añada la siguiente línea a la sección **[Service]**:

```
Environment="ESMC_ENABLE_LDAPS=1"
```

7. Pulse **CTRL + X** y escriba **Y** para guardar los cambios realizados en el archivo. Pulse **Entrar** para salir del editor.

8. Ejecute el siguiente comando para volver a cargar la configuración:

```
systemctl daemon-reload
```

9. Iniciar el servicio ESET PROTECT Server.

```
systemctl start eraserver
```

10. Copie el archivo del certificado generado en el controlador de dominio en la siguiente ubicación del dispositivo virtual de ESET PROTECT Server:

```
/etc/pki/ca-trust/source/anchors/
```

11. Ejecute el siguiente comando:

```
update-ca-trust
```

Cómo recuperar una contraseña olvidada del dispositivo virtual de ESET PROTECT

Inicie su dispositivo virtual de ESET PROTECT en el Modo de un solo usuario. Para obtener instrucciones, consulte la documentación de CentOS 7. Cuando esté en el shell del Modo de un solo usuario, cambie la contraseña del usuario root utilizando el comando `passwd`.

Si se muestra el mensaje `"passwd: Authentication token manipulation error"` (contraseña: Error de manipulación del token de autenticación), siga estos pasos de resolución de problemas.

Cómo cambiar la cadena de conexión a la base de datos de ESET PROTECT

Puede cambiar la cadena de conexión a la base de datos de ESET PROTECT del dispositivo virtual de ESET PROTECT modificando el archivo `StartupConfiguration.ini`.

Para cambiar la cadena de conexión a la base de datos de ESET PROTECT, siga las instrucciones indicadas a continuación:

1. Acceda al **modo de administración** escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Exit to terminal** con las teclas de flecha y, a continuación, pulse **Entrar**.

2. Tipo:

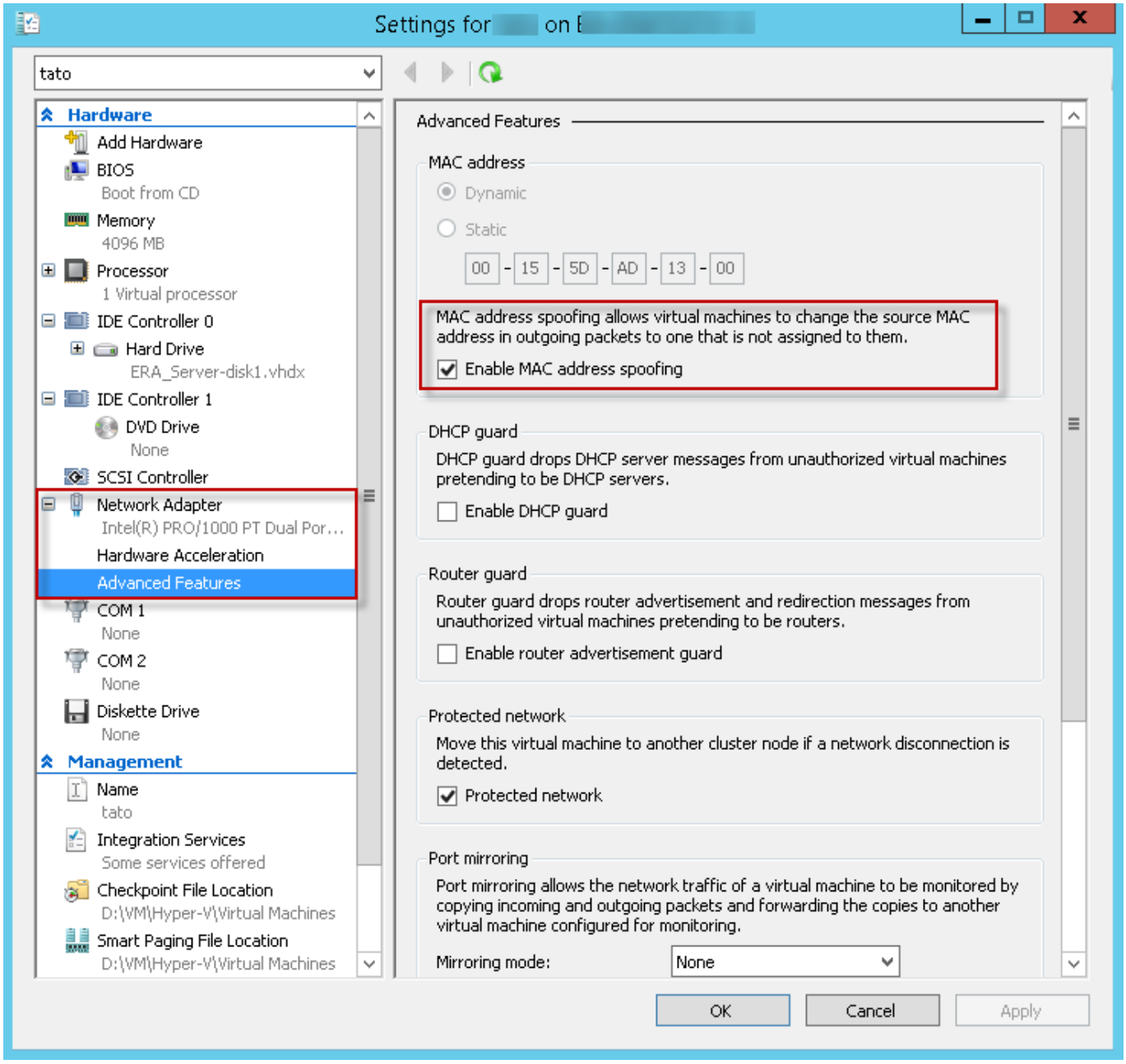
```
nano /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

3. Cambie los datos de la cadena de conexión a la base de datos de ESET PROTECT.

4. Pulse `Ctrl+X` y `y` para guardar los cambios.

Cómo configurar Hyper-V Server para el Sensor RD

Asegúrese de que la falsificación de direcciones MAC esté activada en la configuración de Hyper-V Manager (ver a continuación).



Cómo cambiar los números de puerto del dispositivo virtual de ESET PROTECT

Para cambiar un número de puerto, realice los siguientes cambios en el componente de ESET PROTECT en cuestión:

Puerto de Web Console de ESET PROTECT (predeterminado 8443)

1.Abra Webmin, diríjase a **Servidores** > **ESET PROTECT** > **Editar** *Apache Tomcat server.xml* y modifique la línea `<Connector port="8443"`

2.Edite */var/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* y establezca `server_port=` en su valor.

3.Reinicie el servicio Tomcat: `systemctl restart tomcat`

Puertos de ESET PROTECT Server (predeterminados: 2222, 2223): inicie sesión en ESET PROTECT Web Console, diríjase a **Más** > **Configuración del servidor** > **Conexión** y cambie los ajustes que resulten necesarios.

Si ha cambiado alguno de los puertos anteriores, tendrá que modificar también la configuración del cortafuegos. Abra Webmin, diríjase a **Redes** > **Cortafuegos de Linux** y cambie los números de puerto de las reglas existentes. Otra opción es agregar reglas nuevas.

Cómo aumentar el tamaño de la memoria para MySQL Server

Siga estos pasos para aumentar el tamaño de la memoria destinada a MySQL Server:

1. Acceda al **modo de administración** escribiendo la contraseña y pulsando Entrar dos veces. Seleccione **Salir a terminal** con las teclas de flecha y, a continuación, pulse **Entrar**.

2. Tipo:
`nano /etc/my.cnf`

3. Busque la línea `innodb_buffer_pool_size = 1024M` y cambie la cifra a 50 % de la RAM de la máquina virtual. `1024M` equivale a 1024 megabytes.

4. Pulse `Ctrl+X` para salir del editor de texto y, a continuación, pulse `Y` para guardar.

5. Reinicie el dispositivo con la opción **Reiniciar el sistema** del **modo de administración**.

Error con ESET PROTECT al ejecutarlo en Hyper-V Server 2012 R2

Tras iniciar sesión en ESET PROTECT Web Console, aparece el mensaje de error "Unable to handle Kernel NULL pointer dereference at (null)".

Desactive la memoria dinámica en la configuración del ordenador virtual para resolver este problema.

Cómo mejorar el rendimiento de Oracle VirtualBox

Puede cambiar el número de procesadores (núcleos de la CPU) en los **ajustes** del dispositivo virtual de ESET PROTECT. Diríjase a la pestaña **Sistema** > **Procesador**. Reduzca el número de procesadores del dispositivo virtual. Por ejemplo, si tiene cuatro CPU físicas, cambie el ajuste para que el dispositivo virtual utilice solo dos procesadores.

Cómo activar el comando YUM en el servidor proxy HTTP

Si tiene una red local en la que se usa un servidor proxy como intermediario para el acceso a Internet, el comando `yum` puede no estar configurado correctamente y no funcionar.

Para configurar `yum` de forma que funcione con un proxy:

1. Acceda al modo de administración escribiendo la contraseña y pulsando **Entrar** dos veces. Seleccione **Salir** a terminal con las teclas de flecha y, a continuación, pulse **Entrar**.

2. Tipo:
```
nano /etc/yum.conf
```

3. Añada una línea con información sobre su proxy. Por ejemplo:
```
proxy=http://proxysvr.yourdom.com:3128
```

4. Si el proxy necesita nombre de usuario y contraseña, agregue estos ajustes. Por ejemplo:
```
proxy=http://proxysvr.yourdom.com:3128
proxy_username=YourProxyUsername
proxy_password=YourProxyPassword
```

5. Pulse `Ctrl+X` y `y` para guardar los cambios.

> Tenga en cuenta que `/etc/yum.conf` debe ser legible para todos los que trabajen con el comando `yum`. Por lo tanto, el resto de usuarios podrán leer la contraseña de su proxy. No utilice la misma contraseña en ningún otro sitio.

Para obtener más información, lea la documentación oficial del proveedor.

Cómo actualizar el sistema operativo de un ordenador que ejecute el servidor del dispositivo virtual de ESET PROTECT

Si Web Console de ESET PROTECT muestra una advertencia que indica que en el servidor del dispositivo virtual de ESET PROTECT **El sistema operativo no está actualizado**, debe actualizar el sistema operativo del servidor del dispositivo virtual de ESET PROTECT. Ejecute la tarea Actualización del sistema operativo desde ESET PROTECTWeb Console de . Una vez finalizada la actualización, el mensaje de advertencia desaparecerá.

Si la actualización del sistema operativo se realiza desde la interfaz de Webmin, desde el terminal o con una herramienta de terceros, el mensaje de advertencia no desaparecerá una vez actualizado el sistema operativo. En este caso, le recomendamos ejecutar la tarea **Actualización del sistema operativo** desde Web Console de ESET PROTECT.

Cómo desactivar SELinux de forma permanente

SELinux está activado de forma predeterminada en el dispositivo virtual. Para desactivarlo de forma permanente, siga estos pasos:

1. Seleccione **Exit to Terminal** en la Consola de administración del dispositivo virtual.

2. Ejecute el comando:
```
nano /etc/selinux/config
```

3. Cambie la línea:
```
SELINUX=permisive
```
hasta
```
SELINUX=disabled
```

4. Guarde los cambios y salga del editor.

5. Reinicie el ordenador con el siguiente comando para aplicar la nueva configuración.
```
reboot
```

Cómo reiniciar la consola de administración del dispositivo virtual

Es posible reiniciar la interfaz gráfica del dispositivo virtual sin reiniciar la máquina virtual. Esto forzará la actualización de todos los datos de la consola. (Por ejemplo, si una configuración cambiada no se está aplicando en la consola de administración del dispositivo virtual).

1. Seleccione **Exit to Terminal** en la Consola de administración del dispositivo virtual.

2. Ejecute el comando:
```
./appliance-gui restart
```

Cómo utilizar el proxy para las conexiones de los agentes

Uso del proxy para reenviar el agente de ESET Management: las conexiones del servidor de ESET PROTECT de ESET PROTECT son posibles a través del proxy HTTP Apache. Siga las Instrucciones para Linux para la instalación de Apache HTTP Proxy.

Cómo activar SSH

Para activar el dispositivo virtual de ESET PROTECT (o dispositivo virtual de ESMC): consulte Activar o desactivar el acceso remoto.

Resolución de problemas de SSH

Abra una ventana de terminal y ejecute el siguiente comando:

- `sudo service sshd status`: compruebe que SSH se está ejecutando. Si SSH no se está ejecutando, puede iniciarlo con `service sshd start`.

- `sudo iptables -S`: si el puerto 22 está abierto, verá la línea `-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`. Para agregar el puerto 22 a iptables, ejecute el siguiente comando: `sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`.

Acuerdo de licencia para el usuario final

Fecha de entrada en vigor: 19 de octubre de 2021.

IMPORTANTE: Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo y acepta la Política de Privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de Privacidad, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo

electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo ("Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. **Instalación, Ordenador y una Clave de licencia**. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (“un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíqueselo inmediatamente al Proveedor.

c) **Home Edition o Business Edition.** La versión Home Edition del Software se utilizará exclusivamente en entornos privados o no comerciales para uso doméstico y familiar. Debe obtener una versión Business Edition del Software para poder utilizarlo en entornos comerciales y en servidores de correo, relays de correo, puertas de enlace de correo o puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El Software clasificado como "OEM" solo se puede utilizar en el equipo con el que lo haya obtenido. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la Licencia, Usted debe eliminar, destruir o devolver (a sus expensas) el Software y todas las copias de seguridad del mismo a ESET o a la tienda donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos aplicable son necesarias para el funcionamiento del Software y para actualizar dicho Software. El Proveedor podrá publicar actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para proporcionar Actualizaciones, es necesario verificar la autenticidad de la licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La Política de final de la vida útil ("Política de final de la vida útil"), disponible en https://go.eset.com/eol_business, puede regir la forma de proporcionar las Actualizaciones. No se proporcionarán Actualizaciones después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador.

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.

5. **Ejercicio de los derechos de usuario final**. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes ni crear versiones derivadas

del software. El uso del software está sujeto a las siguientes restricciones:

a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.

c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.

d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. **Copyright**. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. **Reserva de derechos**. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. **Versiones en varios idiomas, software en soporte dual, varias copias**. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar,

alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. **Comienzo y rescisión del Acuerdo.** Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Su derecho a usar el Software y sus funciones puede estar sujeto a la Política de final de la vida útil. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil, dejará de tener derecho a utilizar el Software. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. **Ninguna obligación adicional**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. **Soporte técnico**. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. No se proporcionará soporte técnico después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de

soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. **Transferencia de la licencia**. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. **Licencia para organismos públicos y gubernamentales de EE.UU.**. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. **Cumplimiento de las normas de control comercial**.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo ("Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen.

(los actos jurídicos a los que se hace referencia en los puntos i e ii. anteriores se denominan, conjuntamente, "Leyes de control comercial").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es

probable que incumpla lo dispuesto en el Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. **Avisos**. Los avisos y las devoluciones del Software y la Documentación deben enviarse a ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle los cambios que se produzcan en este Acuerdo, en las Políticas de privacidad, en la Política de final de la vida útil y en la Documentación de conformidad con el art. 22 del Acuerdo. ESET puede enviarle correos electrónicos y notificaciones en la aplicación a través del Software o publicar la comunicación en su sitio web. Acepta recibir comunicaciones legales de ESET en formato electrónico, lo que incluye cualquier comunicación sobre cambios en los Términos, los Términos especiales o las Políticas de privacidad, cualquier propuesta o aceptación de contrato o invitación para negociar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. **Legislación aplicable**. Este acuerdo se regirá e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

ESET se reserva el derecho a realizar cambios en el Software y a modificar los términos de este Acuerdo, sus Anexos, la Política de Privacidad, la Política de final de la vida útil y la Documentación, o de cualquier parte de lo anterior, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar los cambios del Software o en la forma en la que ESET desarrolla su actividad, (ii) por motivos legales, de legislación o de seguridad, o (iii) para evitar un uso inadecuado o perjuicios. Se le notificará cualquier modificación del Acuerdo por correo electrónico, mediante una notificación en la aplicación o a través de otros medios electrónicos. Si no está de acuerdo con los cambios propuestos para el Acuerdo, puede rescindirlo de acuerdo con el art. 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios propuestos se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

ANEXO AL ACUERDO

Envío de información al proveedor. Al envío de información al proveedor se le aplican las siguientes disposiciones

adicionales:

El Software incluye funciones que recogen datos sobre el proceso de instalación, el Ordenador o la plataforma en la que está instalado el Software, información sobre las operaciones y la funcionalidad del Software e información sobre dispositivos administrados (en adelante, “Información”) y posteriormente los envían al Proveedor. La Información puede contener datos (incluidos datos personales obtenidos aleatoria o accidentalmente) relativos a dispositivos administrados. Si se activa esta función del Software, el Proveedor podrá recopilar la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante.

El Software necesita que haya un componente instalado en el ordenador administrado, que permite transferir información entre el ordenador administrado y el software de administración remota. La información que se puede transferir contiene datos de administración como información sobre hardware y software del ordenador administrado e instrucciones de administración del software de administración remota. El resto del contenido de los datos transferidos desde el ordenador administrado lo determinará la configuración del software instalado en el ordenador administrado. El contenido de las instrucciones del software de administración lo determinará la configuración del software de administración remota.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, número de registro de la empresa 31333532, como controlador de datos («ESET» o «Nosotros»), quiere ser transparente en cuanto al procesamiento de datos personales y la privacidad de sus clientes. Para alcanzar este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes («Usuario final» o «Usted») sobre los siguientes temas:

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

Los servicios prestados por ESET implementados en el producto se prestan de acuerdo con los términos del Acuerdo de licencia para el usuario final ("EULA"), pero algunos pueden requerir atención específica. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos diferentes servicios descritos en el EULA y en la documentación de producto, como el servicio de actualización, ESET LiveGrid®, protección contra mal uso de datos, soporte, etc. Para que todo funcione, debemos recopilar la siguiente información:

- La administración de los productos de seguridad de ESET requiere y almacena de manera local información como el ID y el nombre del puesto, el nombre del producto, información sobre la licencia, información de activación y caducidad, información de hardware y software relativa al ordenador administrado con el producto de seguridad de ESET instalado. Se recopilan registros relacionados con las actividades de los productos y de seguridad de ESET y los dispositivos administrados, y están disponibles para facilitar las funciones y los servicios de administración sin envío automatizado a ESET.
- Información relativa al proceso de instalación, incluida la plataforma en la que se instala nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como la huella digital de hardware,

los ID de instalación, los volcados de bloqueo, los ID de licencia, la dirección IP, la dirección MAC, los ajustes de configuración del producto, lo que también podría incluir los dispositivos administrados.

• La información sobre licencias, como el ID de licencia, y datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de las licencias y la prestación de nuestros servicios.

• La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica, como los archivos de registro generados.

• Los datos relativos al uso de nuestros servicios son totalmente anónimos al finalizar la sesión. Una vez concluida la sesión, no se guarda ningún tipo de información personal.

Confidencialidad de los datos

ESET es una empresa que opera en todo el mundo a través de filiales o socios que forman parte de su red de distribución, servicio y asistencia. La información procesada por ESET puede transferirse a y de filiales o socios para cumplir el CLUF en aspectos como la prestación de servicios, la asistencia o la facturación. Según su ubicación y el servicio que decida utilizar, podemos vernos obligados a transferir sus datos a un país para el que no exista una decisión de adecuación de la Comisión Europea. Incluso en este caso, todas las transferencias de información cumplen la legislación sobre protección de datos y solo se realizan si es necesario. Deben implementarse sin excepción las cláusulas contractuales tipo, las reglas corporativas vinculantes u otra medida de seguridad adecuada.

Hacemos todo lo posible para evitar que los datos se almacenen más tiempo del necesario durante la prestación de servicios de acuerdo con el EULA. Nuestro período de retención puede ser mayor que el período de validez de su licencia para que tenga tiempo de renovarla de forma sencilla y cómoda. Pueden continuar tratándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar en todo momento la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y los servicios de tratamiento. Sin embargo, en caso de filtración de información que ponga en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora y a los interesados. Como titular de los datos, tiene derecho a presentar una reclamación ante una autoridad supervisora.

Derechos del titular de los datos.

ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. Sin perjuicio de las condiciones establecidas por las leyes de protección de datos aplicables, en su calidad de interesado, tiene los siguientes derechos:

• derecho a solicitar a ESET acceso a sus datos personales;

• derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a completarlos en caso de que estén incompletos);

• derecho a solicitar la eliminación de sus datos personales;

• derecho a solicitar la restricción del procesamiento de sus datos personales;

• derecho a oponerse al procesamiento;

- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk